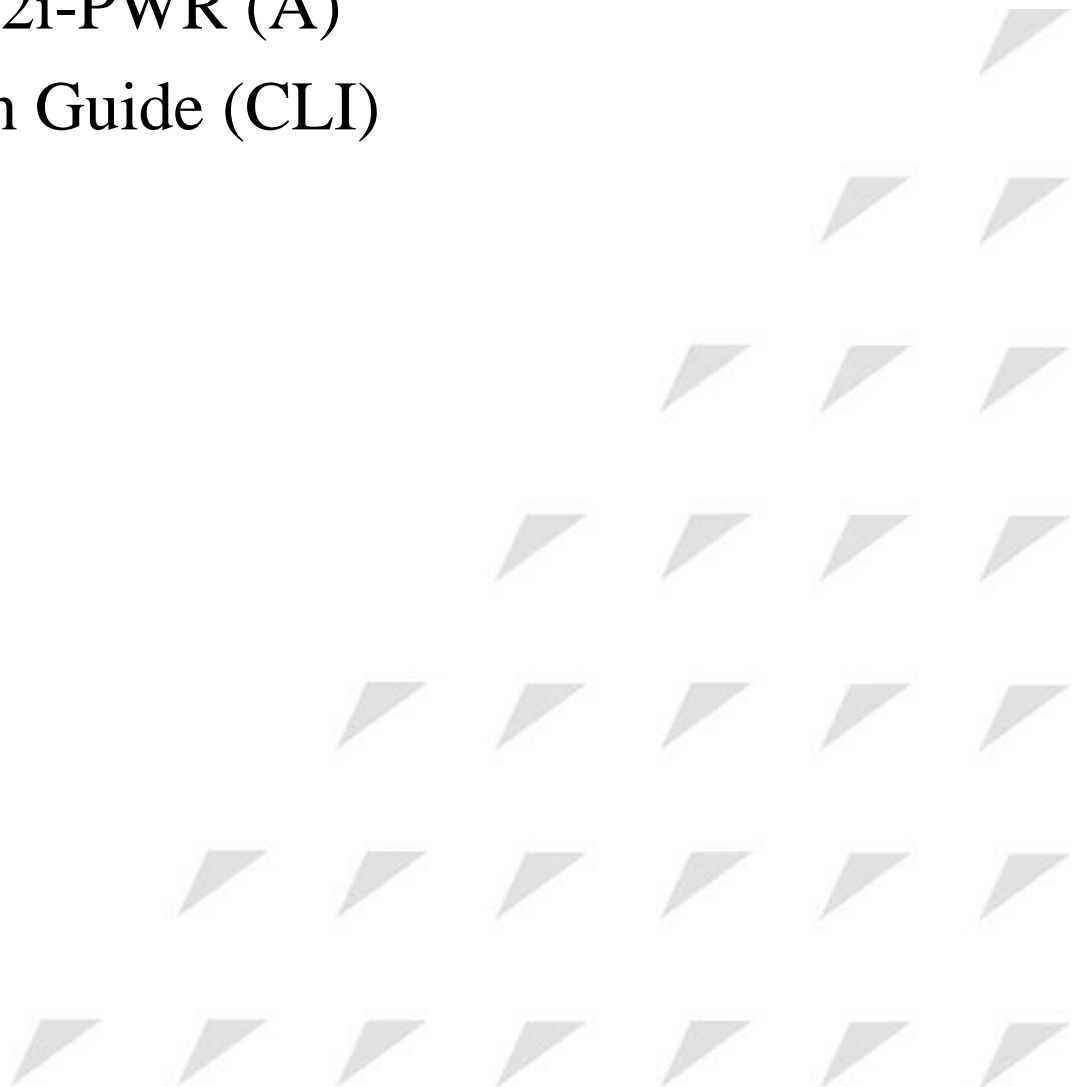


www.raisecom.com

**Gazelle S1512i-PWR (A)
Configuration Guide (CLI)
(Rel_02)**



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

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

Tel: 8610-82883305

Fax: 8610-82883056

Email: export@raisecom.com

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

Postal code: 100094

Notice

Copyright ©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 Gazelle S1512i-PWR, and related configurations, including basic configurations, basic principles and configuration procedures of Ethernet, ring network protection, IP routing, 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 Gazelle S1512i-PWR, and how to network with the Gazelle S1512i-PWR.

Versions



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



Product name	Product version	Software version	Hardware version
Gazelle S1512i-PWR	P100R001	V3.41.10 or later	A.00 or later

Conventions

Symbol conventions

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

Symbol	Description
 Warning	Indicate a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
 Caution	Indicate a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.

Symbol	Description
 Note	Provide additional information to emphasize or supplement important points of the main text.
 Tip	Indicate a tip that may help you solve a problem or save time.

General conventions

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

Command conventions

Convention	Description
Boldface	The keywords of a command line are in boldface .
<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.

Interface type and value range

Format	Description
<i>interface-type</i>	It indicates the interface type with values shown below: <ul style="list-style-type: none">• vlan: VLAN interface• loopback: loopback interface• gigaethernet: 1000 Mbit/s physical interface• port-channel: LAG interface
<i>interface-number</i>	It indicates the interface ID, which varies with the interface type and device model, as shown below: <ul style="list-style-type: none">• vlan: 1–4094• loopback: 1• gigaethernet <i>unit/slot/port</i>: 1/1/1–1/1/12 (1000 Mbit/s physical interface)• port-channel: 1–32



Note

In configuration steps of features in this document, the interface configuration mode and maximum number of interfaces are subject to the actual device.

Change history

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

Issue 02 (2018-05-30)

Second commercial release

- Fixed known bugs.

Issue 01 (2018-02-24)

Initial commercial release

Contents

1 Basic configurations	1
1.1 Accessing device	1
1.1.1 Introduction.....	1
1.1.2 Accessing through Console interface	2
1.1.3 Accessing through Telnet	3
1.1.4 Accessing through SSH.....	5
1.1.5 Configuring Banner.....	7
1.1.6 Checking configurations	7
1.1.7 Configuring console.....	8
1.1.8 Example for configuring SSH login.....	9
1.2 CLI	11
1.2.1 Introduction.....	11
1.2.2 Privileges	12
1.2.3 Modes.....	12
1.2.4 Shortcut keys.....	15
1.2.5 Acquiring help.....	16
1.2.6 Display information	19
1.2.7 Command history	20
1.2.8 Restoring default value of command line	20
1.2.9 Logging commands.....	20
1.3 User management.....	21
1.3.1 Introduction.....	21
1.3.2 Preparing for configurations	22
1.3.3 Default configurations of user management	22
1.3.4 Configuring basic information about user.....	22
1.3.5 Managing user login.....	23
1.3.6 Managing user commands	23
1.3.7 Checking configurations	23
1.3.8 Example for configuring user management	24
1.4 File management	26
1.4.1 Introduction.....	26
1.4.2 Managing BootROM files.....	27

1.4.3 Managing system files	27
1.4.4 Managing configuration files	28
1.4.5 Checking configurations	28
1.4.6 Maintenance	29
1.5 Upgrading BootROM	29
1.5.1 Introduction	29
1.5.2 Upgrading BootROM file through BootROM	30
1.5.3 Upgrading BootROM file through CLI	30
1.5.4 Configuring BootROM password	31
1.5.5 Checking configurations	32
1.5.6 Maintenance	32
1.6 Upgrading system software	33
1.6.1 Introduction	33
1.6.2 Upgrading system software through BootROM	33
1.6.3 Upgrading system software through CLI	35
1.6.4 Checking configurations	36
1.7 Time management	36
1.7.1 Configuring time and time zone	36
1.7.2 Configuring DST	37
1.7.3 Configuring NTP	37
1.7.4 Configuring SNTP	39
1.7.5 Checking configurations	39
1.8 Interface management	40
1.8.1 Introduction	40
1.8.2 Default configurations of interface management	40
1.8.3 Configuring basic attributes of interfaces	41
1.8.4 Configuring interface rate statistics	41
1.8.5 Configuring flow control on interfaces	42
1.8.6 Shutting down/Restarting interface	42
1.8.7 Configuring L2Protocol Peer STP	42
1.8.8 Configuring Console interface	43
1.8.9 Checking configurations	43
1.9 Configuring basic information	44
1.10 Task scheduling	45
1.10.1 Introduction	45
1.10.2 Configuring task scheduling	45
1.10.3 Checking configurations	45
1.11 Watchdog	46
1.11.1 Introduction	46
1.11.2 Preparing for configurations	46
1.11.3 Default configurations of Watchdog	46
1.11.4 Configuring Watchdog	46

1.11.5 Checking configurations	46
2 Ethernet	47
2.1 MAC address table	47
2.1.1 Introduction.....	47
2.1.2 Preparing for configurations	49
2.1.3 Default configurations of MAC address table.....	50
2.1.4 Configuring static MAC address.....	50
2.1.5 Configuring blackhole MAC address.....	50
2.1.6 Filtering unknown multicast packets.....	51
2.1.7 Configuring MAC address learning	51
2.1.8 Configuring MAC address limit.....	51
2.1.9 Configuring aging time of MAC addresses.....	51
2.1.10 Enabling suppression of MAC address flapping	52
2.1.11 Checking configurations	52
2.1.12 Maintenance	52
2.1.13 Example for configuring MAC address table.....	53
2.2 VLAN.....	54
2.2.1 Introduction.....	54
2.2.2 Preparing for configurations	57
2.2.3 Default configurations of VLAN	57
2.2.4 Configuring VLAN attributes	58
2.2.5 Configuring interface mode	58
2.2.6 Configuring VLAN on Access interface	58
2.2.7 Configuring VLAN on Trunk interface.....	59
2.2.8 Configuring VLAN partitions by MAC address	60
2.2.9 Configuring VLAN partitions by IP subnet	60
2.2.10 Checking configurations	61
2.2.11 Example for configuring VLAN	61
2.3 QinQ.....	64
2.3.1 Introduction.....	64
2.3.2 Preparing for configurations	65
2.3.3 Default configurations of QinQ	66
2.3.4 Configuring basic QinQ	66
2.3.5 Configuring selective QinQ	67
2.3.6 Configuring network-side interface to Trunk mode	67
2.3.7 Configuring TPID	68
2.3.8 Checking configurations	68
2.3.9 Example for configuring basic QinQ	68
2.3.10 Example for configuring selective QinQ	70
2.4 VLAN mapping.....	71
2.4.1 Introduction.....	71

2.4.2	Preparing for configurations	72
2.4.3	Default configurations of VLAN mapping	72
2.4.4	Configuring VLAN mapping	73
2.4.5	Checking configurations	74
2.4.6	Example for configuring VLAN mapping	74
2.5	STP/RSTP	76
2.5.1	Introduction.....	76
2.5.2	Preparing for configurations	79
2.5.3	Default configurations of STP	79
2.5.4	Enabling STP	80
2.5.5	Configuring STP parameters.....	80
2.5.6	(Optional) configuring edge interface	81
2.5.7	(Optional) configuring link type	81
2.5.8	Checking configurations	82
2.5.9	Example for configuring STP	82
2.6	MSTP	85
2.6.1	Introduction.....	85
2.6.2	Preparing for configurations	88
2.6.3	Default configurations of MSTP.....	88
2.6.4	Enabling MSTP.....	89
2.6.5	Configuring MST region and its maximum number of hops	89
2.6.6	Configuring root/backup bridge.....	90
2.6.7	Configuring interface priority and system priority.....	91
2.6.8	Configuring network diameter for switch network	92
2.6.9	Configuring internal path cost of interface	92
2.6.10	Configuring external path cost of interface.....	93
2.6.11	Configuring maximum transmission rate on interface	93
2.6.12	Configuring MSTP timer	93
2.6.13	Configuring edge interface.....	94
2.6.14	Configuring BPDU filtering.....	95
2.6.15	Configuring BPDU Guard.....	95
2.6.16	Configuring STP/RSTP/MSTP mode switching	96
2.6.17	Configuring link type	96
2.6.18	Configuring root interface protection.....	97
2.6.19	Configuring interface loopguard	97
2.6.20	Configuring TC packet suppression.....	98
2.6.21	Checking configurations	98
2.6.22	Maintenance	99
2.6.23	Example for configuring MSTP.....	99
2.7	MRSTP.....	104
2.7.1	Introduction.....	104
2.7.2	Preparing for configurations	104

2.7.3 Default configurations of MRSTP	104
2.7.4 Enabling MRSTP	105
2.7.5 Configuring MRSTP parameters.....	105
2.7.6 Checking configurations	106
2.8 Loop detection.....	106
2.8.1 Introduction.....	106
2.8.2 Preparing for configurations	108
2.8.3 Default configurations of loop detection.....	108
2.8.4 Configuring loop detection	108
2.8.5 Checking configurations	109
2.8.6 Maintenance.....	109
2.8.7 Example for configuring inner loop detection	109
2.9 Interface protection	111
2.9.1 Introduction.....	111
2.9.2 Preparing for configurations	111
2.9.3 Default configurations of interface protection	112
2.9.4 Configuring interface protection	112
2.9.5 Checking configurations	112
2.9.6 Example for configuring interface protection	112
2.10 Port mirroring.....	114
2.10.1 Introduction.....	114
2.10.2 Preparing for configurations	115
2.10.3 Default configurations of port mirroring.....	115
2.10.4 Configuring port mirroring	115
2.10.5 Checking configurations	116
2.10.6 Example for configuring port mirroring.....	116
2.11 L2CP	118
2.11.1 Introduction.....	118
2.11.2 Preparing for configurations.....	118
2.11.3 Default configurations of L2CP	118
2.11.4 Configuring global L2CP	118
2.11.5 Configuring L2CP profile	119
2.11.6 Configuring L2CP profile on interface.....	119
2.11.7 Checking configurations	120
2.11.8 Maintenance	120
2.11.9 Example for configuring L2CP.....	120
3 PoE.....	124
3.1 Introduction.....	124
3.1.1 Principles of PoE.....	124
3.1.2 PoE modules	124
3.1.3 PoE advantages	125

3.1.4 PoE concepts	125
3.2 Configuring PoE.....	126
3.2.1 Preparing for configurations	126
3.2.2 Default configurations of PoE.....	126
3.2.3 Enabling interface PoE.....	126
3.2.4 Configuring maximum output power of PoE.....	126
3.2.5 Configuring priority of PoE	127
3.2.6 Configuring PSE power utilization rate threshold	127
3.2.7 Configuring identification of non-standard PDs	127
3.2.8 Enabling forcible power supply on interface	128
3.2.9 Enabling overtemperature protection.....	128
3.2.10 Enabling global Trap.....	128
3.2.11 Checking configurations	129
3.3 Example for configuring PoE power supply	129
4 Ring network protection.....	132
4.1 G.8032.....	132
4.1.1 Introduction.....	132
4.1.2 Preparing for configurations	132
4.1.3 Default configurations of G.8032	133
4.1.4 Creating G.8032 ring.....	133
4.1.5 (Optional) creating G.8032 tributary ring	135
4.1.6 (Optional) configuring G.8032 switching control.....	137
4.1.7 Configuring ERPS fault detection mode.....	138
4.1.8 Checking configurations	138
4.1.9 Maintenance.....	138
5 IP services	139
5.1 IP basis	139
5.1.1 Introduction.....	139
5.1.2 Preparing for configurations	139
5.1.3 Default configurations of Layer 3 interface	139
5.1.4 Configuring IPv4 address of VLAN interface	140
5.1.5 Configuring IPv6 address of VLAN interface	140
5.1.6 Checking configurations	140
5.1.7 Example for configuring VLAN interface to interconnect with host	141
5.2 Loopback interface.....	142
5.2.1 Introduction.....	142
5.2.2 Preparing for configurations	142
5.2.3 Default configurations of loopback interface.....	143
5.2.4 Configuring IP address of loopback interface	143
5.2.5 Checking configurations	143
5.3 ARP.....	143

5.3.1 Introduction.....	143
5.3.2 Preparing for configurations	144
5.3.3 Default configurations of ARP	144
5.3.4 Configuring static ARP entries.....	145
5.3.5 Configuring dynamic ARP entries	145
5.3.6 Configuring gratuitous ARP packet learning	145
5.3.7 Configuring local proxy ARP.....	146
5.3.8 Configuring ARP anti-attack.....	146
5.3.9 Checking configurations	146
5.3.10 Maintenance.....	146
5.3.11 Example for configuring ARP	147
5.4 NDP.....	148
5.4.1 Introduction.....	148
5.4.2 Preparing for configurations	149
5.4.3 Default configurations of NDP	149
5.4.4 Configuring static neighbor entries.....	149
5.4.5 Configuring times of sending NS messages for detecting duplicated addresses.....	149
5.4.6 Configuring maximum number of NDPs allowed to be learnt on Layer 3 interface.....	150
5.4.7 Checking configurations	150
5.4.8 Maintenance.....	151
6 IP routing.....	152
6.1 Introduction.....	152
6.1.1 Route management.....	152
6.1.2 Default route	152
6.1.3 Routing policy.....	153
6.1.4 OSPF.....	154
6.1.5 RIP.....	160
6.2 Configuring route management.....	162
6.2.1 Configuring route management.....	162
6.2.2 Checking configurations	162
6.3 Configuring static route.....	163
6.3.1 Preparing for configurations	163
6.3.2 Configuring static route	163
6.3.3 Checking configurations	164
6.3.4 Example for configuring static route.....	164
6.4 Configuring routing policy.....	165
6.4.1 Configuring IP prefix-list.....	165
6.4.2 Configuring route mapping table	166
6.4.3 Checking configurations	167
6.5 Configuring OSPFv2.....	168
6.5.1 Configuring basic functions of OSPF	168

6.5.2 Configuring OSPF route attributes.....	168
6.5.3 Configuring OSPF network	170
6.5.4 Configuring OSPF NBMA network neighbor.....	171
6.5.5 Optimizing OSPF network.....	172
6.5.6 Configuring OSPF authentication mode	174
6.5.7 Configuring Stub area	175
6.5.8 Controlling OSPF routing information	176
6.5.9 Configuring NSSA.....	178
6.5.10 Controlling OSPF routing information	178
6.5.11 Configuring OSPF routing policy	180
6.5.12 Checking configurations	183
6.5.13 Maintenance	183
6.6 Configuring RIP	184
6.6.1 Configuring basic RIP functions	184
6.6.2 Configuring RIP version	184
6.6.3 Configuring redistribution of external routes.....	185
6.6.4 Configuring RIP timer.....	186
6.6.5 Configuring loop suppression	186
6.6.6 Configuring authentication	186
6.6.7 Configuring routing policy.....	187
6.6.8 Configuring route calculation	187
6.6.9 Checking configurations	188
6.6.10 Maintenance	188
7 DHCP.....	189
7.1 DHCP Client	189
7.1.1 Introduction.....	189
7.1.2 Preparing for configurations	192
7.1.3 Default configurations of DHCP Client	192
7.1.4 Configuring DHCP Client.....	193
7.1.5 Configuring DHCPv6 Client.....	193
7.1.6 Checking configurations	194
7.1.7 Example for configuring DHCP Client	194
7.2 DHCP Snooping	196
7.2.1 Introduction.....	196
7.2.2 Preparing for configurations	197
7.2.3 Default configurations of DHCP Snooping.....	198
7.2.4 Configuring DHCP Snooping	198
7.2.5 Configuring DHCPv6 Snooping	199
7.2.6 Checking configurations	199
7.2.7 Example for configuring DHCP Snooping.....	200
7.3 DHCP Options.....	201

7.3.1 Introduction.....	201
7.3.2 Preparing for configurations	203
7.3.3 Default configurations of DHCP Option.....	203
7.3.4 Configuring DHCP Option fields.....	203
7.3.5 Configuring DHCP Option 18 over IPv6.....	204
7.3.6 Configuring DHCP Option 37 over IPv6.....	205
7.3.7 Configuring user-defined DHCP Option over IPv6	205
7.3.8 Checking configurations	206
7.4 DHCP Server.....	206
7.4.1 Introduction.....	206
7.4.2 Preparing for configurations	208
7.4.3 Creating and configuring IPv4 address pool	209
7.4.4 Enabling DHCPv4 Server	209
7.4.5 Checking configurations	209
7.4.6 Example for configuring DHCPv4 Server	210
7.5 DHCP Relay.....	211
7.5.1 Introduction.....	211
7.5.2 Preparing for configurations	212
7.5.3 Default configurations of DHCP Relay.....	212
7.5.4 Configuring global DHCP Relay	212
7.5.5 Configuring destination IP address for forwarding packets	213
7.5.6 Configuring IP address of DHCP relay device.....	213
7.5.7 (Optional) configuring DHCP Relay to support Option 82.....	213
7.5.8 Checking configurations	214
7.5.9 Example for configuring DHCPv4 Relay	214
8 QoS.....	216
8.1 Introduction.....	216
8.1.1 Service model.....	216
8.1.2 Priority trust	217
8.1.3 Traffic classification.....	217
8.1.4 Traffic policy.....	219
8.1.5 Priority mapping	220
8.1.6 Queue scheduling.....	220
8.1.7 Congestion avoidance	222
8.1.8 Rate limiting based on interface and VLAN	223
8.1.9 QoS enhancement	223
8.2 Configuring priority	224
8.2.1 Preparing for configurations	224
8.2.2 Default configurations of basic QoS	224
8.2.3 Configuring types of priorities trusted by interface	225
8.2.4 Configuring mapping from CoS to local priority and color	225

8.2.5 Configuring mapping from DSCP to local priority and color	226
8.2.6 Configuring DSCP mutation	226
8.2.7 Configuring CoS remarking	227
8.2.8 Checking configurations	227
8.3 Configuring congestion management	228
8.3.1 Preparing for configurations	228
8.3.2 Default configurations of congestion management	228
8.3.3 Configuring SP queue scheduling	228
8.3.4 Configuring WRR or SP+WRR queue scheduling	229
8.3.5 Configuring DRR or SP+DRR queue scheduling	229
8.3.6 Configuring queue bandwidth guarantee	229
8.3.7 Checking configurations	230
8.4 Configuring congestion avoidance	230
8.4.1 Preparing for configurations	230
8.4.2 Default configurations of congestion avoidance	230
8.4.3 Configuring SRED	231
8.4.4 Checking configurations	231
8.5 Configuring traffic classification and traffic policy	231
8.5.1 Preparing for configurations	231
8.5.2 Default configurations of traffic classification and traffic policy	232
8.5.3 Creating traffic class	232
8.5.4 Configuring traffic classification rules	232
8.5.5 Creating rate limiting rule and shapping rule	233
8.5.6 Creating traffic policy	234
8.5.7 Defining traffic policy mapping	234
8.5.8 Defining traffic policy operation	235
8.5.9 Applying traffic policy to interface	236
8.5.10 Checking configurations	236
8.5.11 Maintenance	237
8.6 Configuring rate limiting	237
8.6.1 Preparing for configurations	237
8.6.2 Configuring rate limiting based on interface	237
8.6.3 Checking configurations	238
8.7 Configuration examples	238
8.7.1 Example for configuring congestion management	238
8.7.2 Example for configuring rate limiting based on traffic policy	240
8.7.3 Example for configuring rate limiting based on interface	243
9 Multicast	246
9.1 Introduction	246
9.2 Basic functions of Layer 2 multicast	251
9.2.1 Introduction	251

9.2.2	Preparing for configurations	253
9.2.3	Default configurations of basic functions of Layer 2 multicast	253
9.2.4	Configuring basic functions of Layer 2 multicast	253
9.2.5	Checking configurations	254
9.2.6	Maintenance	254
9.3	IGMP Snooping.....	254
9.3.1	Introduction.....	254
9.3.2	Preparing for configurations	255
9.3.3	Default configurations of IGMP Snooping	255
9.3.4	Configuring IGMP Snooping	255
9.3.5	Checking configurations	256
9.3.6	Example for applying multicast on ring network	256
9.4	IGMP MVR.....	259
9.4.1	Introduction.....	259
9.4.2	Preparing for configurations	259
9.4.3	Default configurations of IGMP MVR	260
9.4.4	Configuring IGMP MVR	260
9.4.5	Checking configurations	261
9.4.6	Example for configuring IGMP MVR	261
9.5	IGMP filtering	263
9.5.1	Introduction.....	263
9.5.2	Preparing for configurations	264
9.5.3	Default configurations of IGMP filtering.....	264
9.5.4	Enabling global IGMP filtering.....	265
9.5.5	Configuring IGMP filtering profile	265
9.5.6	Configuring maximum number of multicast groups	266
9.5.7	Checking configurations	266
9.5.8	Example for applying IGMP filtering on interface	267
9.6	MLD.....	269
9.6.1	Preparing for configurations	269
9.6.2	Configuring basic functions of MLD	269
9.6.3	Checking configurations	270
9.6.4	Maintenance.....	270
9.7	IGMP Querier.....	270
9.7.1	Introduction.....	270
9.7.2	Preparing for configurations	272
9.7.3	Default configurations of IGMP Querier	272
9.7.4	Configuring IGMP Querier	272
9.7.5	Checking configurations	273
9.8	Multicast VLAN copy	273
9.8.1	Introduction.....	273
9.8.2	Preparing for configurations	275

9.8.3 Default configurations of multicast VLAN copy	276
9.8.4 Configuring multicast VLAN copy	276
9.8.5 Configuring static multicast members of VLAN copy	277
9.8.6 Checking configurations	277
10 Security.....	279
10.1 ACL.....	279
10.1.1 Introduction.....	279
10.1.2 Preparing for configurations	279
10.1.3 Configuring MAC ACL	280
10.1.4 Configuring filter	284
10.1.5 Checking configurations	284
10.1.6 Maintenance.....	285
10.1.7 Example for configuring ACL	285
10.2 Port security MAC	286
10.2.1 Introduction.....	286
10.2.2 Preparing for configurations	288
10.2.3 Default configurations of secure MAC address	288
10.2.4 Configuring basic functions of port security MAC.....	288
10.2.5 Configuring static secure MAC address.....	289
10.2.6 Configuring dynamic secure MAC address	290
10.2.7 Configuring sticky secure MAC address	290
10.2.8 Checking configurations	291
10.2.9 Maintenance.....	291
10.2.10 Example for configuring port security MAC	291
10.3 Dynamic ARP inspection	294
10.3.1 Introduction.....	294
10.3.2 Preparing for configurations	295
10.3.3 Default configurations of dynamic ARP inspection	295
10.3.4 Configuring trusted interfaces of dynamic ARP inspection	296
10.3.5 Configuring static binding of dynamic ARP inspection	296
10.3.6 Configuring dynamic binding of dynamic ARP inspection.....	296
10.3.7 Configuring protection VLAN of dynamic ARP inspection	297
10.3.8 Configuring rate limiting on ARP packets on interface	297
10.3.9 Checking configurations	297
10.3.10 Example for configuring dynamic ARP inspection.....	297
10.4 RADIUS.....	300
10.4.1 Introduction.....	300
10.4.2 Preparing for configurations	301
10.4.3 Default configurations of RADIUS	301
10.4.4 Configuring RADIUS authentication.....	301
10.4.5 Configuring RADIUS accounting.....	302

10.4.6	Checking configurations	302
10.4.7	Example for configuring RADIUS	303
10.5	TACACS+	304
10.5.1	Introduction.....	304
10.5.2	Preparing for configurations	305
10.5.3	Default configurations of TACACS+.....	305
10.5.4	Configuring TACACS+ authentication	305
10.5.5	Configuring TACACS+ accounting	306
10.5.6	Checking configurations	306
10.5.7	Maintenance.....	306
10.5.8	Example for configuring TACACS+.....	307
10.6	Storm control.....	308
10.6.1	Introduction.....	308
10.6.2	Preparing for configurations	309
10.6.3	Default configurations of storm control	309
10.6.4	Configuring storm control.....	309
10.6.5	Configuring DLF packet forwarding.....	310
10.6.6	Checking configurations	310
10.6.7	Example for configuring storm control.....	310
10.7	IP Source Guard	311
10.7.1	Introduction.....	311
10.7.2	Preparing for configurations	313
10.7.3	Default configurations of IP Source Guard	313
10.7.4	Configuring interface trusted status of IP Source Guard.....	313
10.7.5	Configuring IP Source Guard binding.....	314
10.7.6	Checking configurations	315
10.7.7	Example for configuring IP Source Guard.....	315
10.8	PPPoE+	317
10.8.1	Introduction.....	317
10.8.2	Preparing for configurations	318
10.8.3	Default configurations of PPPoE+	318
10.8.4	Configuring basic functions of PPPoE+	319
10.8.5	Configuring PPPoE+ packet information.....	320
10.8.6	Checking configurations	322
10.8.7	Maintenance	322
10.8.8	Example for configuring PPPoE+	322
10.9	Configuring CPU protection	324
10.9.1	Preparing for configurations	324
10.9.2	Configuring global CPU CAR	324
10.9.3	Checking configurations	325
10.9.4	Maintenance	325
10.10	Configuring anti-ARP attack	325

10.10.1 Preparing for configurations	325
10.10.2 Configuring ARP	326
10.10.3 Checking configurations	326
11 Reliability	327
11.1 Link aggregation.....	327
11.1.1 Introduction.....	327
11.1.2 Preparing for configurations.....	328
11.1.3 Configuring manual link aggregation.....	328
11.1.4 Configuring static LACP link aggregation.....	329
11.1.5 Configuring manual master/slave link aggregation.....	330
11.1.6 Checking configurations	331
11.1.7 Example for configuring static LACP link aggregation	332
11.2 Interface backup	334
11.2.1 Introduction.....	334
11.2.2 Preparing for configurations.....	336
11.2.3 Default configurations of interface backup	336
11.2.4 Configuring basic functions of interface backup.....	336
11.2.5 (Optional) configuring FS on interfaces.....	337
11.2.6 Checking configurations	338
11.2.7 Example for configuring interface backup	338
11.3 Link-state tracking.....	340
11.3.1 Introduction.....	340
11.3.2 Preparing for configurations.....	341
11.3.3 Default configurations of link-state tracking.....	341
11.3.4 Configuring link-state tracking	341
11.3.5 Checking configurations	342
12 OAM	343
12.1 Introduction.....	343
12.2 Configuring EFM	344
12.2.1 Preparing for configurations	344
12.2.2 Configuring basic functions of EFM.....	345
12.2.3 Configuring active functions of EFM	345
12.2.4 Configuring passive functions of EFM	347
12.2.5 Configuring link monitoring and fault indication	347
12.2.6 Checking configurations	349
12.2.7 Maintenance.....	350
13 System management.....	351
13.1 SNMP.....	351
13.1.1 Introduction.....	351
13.1.2 Preparing for configurations	353
13.1.3 Default configurations of SNMP	353

13.1.4	Configuring basic functions of SNMPv1/SNMPv2c	354
13.1.5	Configuring basic functions of SNMPv3	355
13.1.6	Configuring IP address authentication by SNMP server	356
13.1.7	Configuring other information about SNMP	356
13.1.8	Configuring Trap.....	357
13.1.9	Checking configurations	357
13.1.10	Example for configuring SNMPv1/SNMPv2c and Trap.....	358
13.1.11	Example for configuring SNMPv3 and Trap.....	360
13.2	KeepAlive	362
13.2.1	Introduction.....	362
13.2.2	Preparing for configurations	363
13.2.3	Default configurations of KeepAlive	363
13.2.4	Configuring KeepAlive.....	363
13.2.5	Checking configurations	364
13.2.6	Example for configuring KeepAlive	364
13.3	RMON.....	365
13.3.1	Introduction.....	365
13.3.2	Preparing for configurations	366
13.3.3	Default configurations of RMON	366
13.3.4	Configuring RMON statistics	367
13.3.5	Configuring RMON historical statistics.....	367
13.3.6	Configuring RMON alarm group.....	367
13.3.7	Configuring RMON event group	368
13.3.8	Checking configurations	368
13.3.9	Maintenance	369
13.3.10	Example for configuring RMON alarm group	369
13.4	LLDP.....	370
13.4.1	Introduction.....	370
13.4.2	Preparing for configurations	372
13.4.3	Default configurations of LLDP	372
13.4.4	Enabling global LLDP	373
13.4.5	Enabling interface LLDP	373
13.4.6	Configuring basic functions of LLDP	374
13.4.7	Configuring LLDP Trap.....	374
13.4.8	Checking configurations	374
13.4.9	Maintenance	375
13.4.10	Example for configuring LLDP	375
13.5	Optical module DDM.....	378
13.5.1	Introduction.....	378
13.5.2	Preparing for configurations	379
13.5.3	Default configurations of optical module DDM	379
13.5.4	Enabling optical module DDM	379

13.5.5 Enabling optical module DDM Trap.....	380
13.5.6 Checking configurations	380
13.6 System log	381
13.6.1 Introduction.....	381
13.6.2 Preparing for configurations	382
13.6.3 Default configurations of system log	382
13.6.4 Configuring basic information of system log.....	382
13.6.5 Configuring system log output.....	383
13.6.6 Checking configurations	384
13.6.7 Maintenance.....	385
13.6.8 Example for configuring outputting system logs to log host	385
13.7 Alarm management	386
13.7.1 Introduction.....	386
13.7.2 Preparing for configurations	390
13.7.3 Default configurations of alarm management	391
13.7.4 Configuring basic functions of alarm management	391
13.7.5 Checking configurations	393
13.8 Hardware environment monitoring	393
13.8.1 Introduction.....	393
13.8.2 Preparing for configurations	396
13.8.3 Default configurations of hardware environment monitoring	396
13.8.4 Enabling global hardware environment monitoring.....	397
13.8.5 Configuring temperature monitoring alarm	397
13.8.6 Configuring power supply alarm	398
13.8.7 Clearing all hardware environment monitoring alarms manually	398
13.8.8 Checking configurations	398
13.9 CPU monitoring	399
13.9.1 Introduction.....	399
13.9.2 Preparing for configurations	399
13.9.3 Default configurations of CPU monitoring	400
13.9.4 Showing CPU monitoring information	400
13.9.5 Configuring CPU monitoring alarm.....	400
13.9.6 Checking configurations	400
13.10 Cable diagnosis	401
13.10.1 Introduction.....	401
13.10.2 Preparing for configurations	401
13.10.3 Configuring cable diagnosis.....	401
13.10.4 Checking configurations	401
13.11 Memory monitoring	402
13.11.1 Preparing for configurations.....	402
13.11.2 Configuring memory monitoring	402
13.11.3 Checking configurations	402

13.12 Ping	403
13.12.1 Introduction.....	403
13.12.2 Configuring Ping.....	403
13.13 Traceroute.....	404
13.13.1 Introduction.....	404
13.13.2 Configuring Traceroute.....	404
14 Appendix	406
14.1 Terms.....	406
14.2 Acronyms and abbreviations	411

Figures

Figure 1-1 Accessing device through PC connected with RJ45 Console interface	2
Figure 1-2 Configuring communication parameters in Hyper Terminal	3
Figure 1-3 Networking with device as Telnet server	4
Figure 1-4 Networking with device as Telnet client.....	5
Figure 1-5 Configuring SSH login	9
Figure 1-6 User management networking	24
Figure 2-1 Forwarding packets according to the MAC address table	48
Figure 2-2 MAC networking	53
Figure 2-3 VLAN partitions	55
Figure 2-4 VLAN and interface protection networking	62
Figure 2-5 Principles of basic QinQ	65
Figure 2-6 Basic QinQ networking	69
Figure 2-7 Selective QinQ networking	70
Figure 2-8 Principles of VLAN mapping	72
Figure 2-9 VLAN mapping networking	75
Figure 2-10 Network storm due to loopback.....	77
Figure 2-11 Loop networking with STP.....	78
Figure 2-12 Failure in forwarding VLAN packets due to RSTP	79
Figure 2-13 STP networking	82
Figure 2-14 Basic concepts of the MSTI network.....	86
Figure 2-15 MSTI concepts.....	87
Figure 2-16 Networking with multiple spanning trees instances in MST region	88
Figure 2-17 MSTP networking.....	100
Figure 2-18 Configuring MRSTP for specifying root bridge	104
Figure 2-19 Loop detection networking	107
Figure 2-20 Loop detection networking	110

Figure 2-21 Interface protection networking.....	113
Figure 2-22 Principles of port mirroring	114
Figure 2-23 Port mirroring networking.....	117
Figure 2-24 L2CP networking.....	120
Figure 3-1 Principles of PoE.....	124
Figure 3-2 PoE switch power supply networking	129
Figure 5-1 VLAN interface networking	141
Figure 5-2 Configuring ARP networking	147
Figure 5-3 Principles of NDP address resolution	148
Figure 6-1 Roles of broadcast interface.....	156
Figure 6-2 OSPF area and router type.....	158
Figure 6-3 NSSA area	159
Figure 6-4 Configuring static route	164
Figure 7-1 DHCP typical networking.....	190
Figure 7-2 Structure of a DHCP packet	190
Figure 7-3 DHCP Client networking.....	192
Figure 7-4 DHCP Client networking.....	195
Figure 7-5 DHCP Snooping	197
Figure 7-6 DHCP Snooping networking	200
Figure 7-7 DHCP Server and Client networking.....	207
Figure 7-8 Structure of a DHCP packet	207
Figure 7-9 DHCP Server networking	210
Figure 7-10 Typical application of DHCP Relay.....	212
Figure 7-11 DHCP Relay networking	214
Figure 8-1 Traffic classification	218
Figure 8-2 Structure of the IP packet header.....	218
Figure 8-3 Structures of ToS priority and DSCP.....	218
Figure 8-4 Structure of a VLAN packet	218
Figure 8-5 Structure of CoS	219
Figure 8-6 SP scheduling	221
Figure 8-7 WRR scheduling.....	221
Figure 8-8 DRR scheduling.....	222
Figure 8-9 Queue scheduling networking	238

Figure 8-10 Rate limiting based on traffic policy.....	241
Figure 8-11 Rate limiting based on interface	244
Figure 9-1 Multicast transmission networking.....	247
Figure 9-2 Basic concepts in multicast.....	249
Figure 9-3 Mapping between IPv4 multicast address and multicast MAC address	250
Figure 9-4 Operating positions of IGMP and Layer 2 multicast features.....	250
Figure 9-5 IGMP Snooping networking.....	255
Figure 9-6 Ring network multicast networking.....	257
Figure 9-7 IGMP MVR networking	260
Figure 9-8 MVR networking.....	262
Figure 9-9 Applying IGMP filtering on interface.....	267
Figure 9-10 Data transmission of IGMP MVR	274
Figure 9-11 Data transmission of multicast VLAN copy	275
Figure 9-12 Multicast VLAN copy networking	276
Figure 10-1 ACL networking	285
Figure 10-2 Port security MAC networking.....	292
Figure 10-3 Principles of dynamic ARP inspection	294
Figure 10-4 Configuring dynamic ARP inspection	298
Figure 10-5 RADIUS networking	303
Figure 10-6 TACACS+ networking	307
Figure 10-7 Storm control networking.....	311
Figure 10-8 Principles of IP Source Guard	312
Figure 10-9 Configuring IP Source Guard	316
Figure 10-10 Accessing the network through PPPoE authentication	318
Figure 10-11 PPPoE+ networking.....	323
Figure 11-1 Static LACP mode link aggregation networking	332
Figure 11-2 Principles of interface backup.....	334
Figure 11-3 Networking with interface backup in different VLANs.....	335
Figure 11-4 Interface backup networking	339
Figure 12-1 OAM classification.....	344
Figure 13-1 Principles of SNMP	352
Figure 13-2 Principles of SNMPv3 authentication	355
Figure 13-3 SNMPv1/SNMPv2c networking	358

Figure 13-4 SNMPv3 and Trap networking	360
Figure 13-5 KeepAlive networking.....	364
Figure 13-6 RMON networking	366
Figure 13-7 RMON networking	369
Figure 13-8 Structure of a LLDPDU.....	371
Figure 13-9 Structure of a TLV packet.....	371
Figure 13-10 LLDP networking	376
Figure 13-11 Networking of outputting system log to log host.....	385
Figure 13-12 Principles of Ping	403
Figure 13-13 Principles of Traceroute.....	404

Tables

Table 1-1 Shortcut keys for display features	19
Table 2-1 Interface mode and packet processing.....	56
Table 7-1 Fields of a DHCP packet.....	190
Table 7-2 Common DHCP options.....	202
Table 7-3 Fields of a DHCP packet.....	207
Table 8-1 Mapping from DSCP or CoS to local priority.....	220
Table 8-2 Mapping between local priority and queue	220
Table 8-3 Default mapping from CoS to local priority	224
Table 8-4 Default mapping from DSCP to local priority.....	225
Table 8-5 Default mapping from ToS to local priority and color	225
Table 13-1 TLV types	371
Table 13-2 Log levels.....	381
Table 13-3 Alarm fields	388
Table 13-4 Alarm levels.....	388
Table 13-5 Trap information	395
Table 13-6 Syslog information	396

1 Basic configurations

This chapter describes basic configurations and configuration procedures of the Gazelle S1512i-PWR, and provides related configuration examples, including the following sections:

- Accessing device
- CLI
- User management
- File management
- Upgrading BootROM
- Upgrading system software
- Time management
- Interface management
- Configuring basic information
- Task scheduling
- Watchdog

1.1 Accessing device

1.1.1 Introduction

The Gazelle S1512i-PWR can be configured and managed in Command Line Interface (CLI) mode or NView NNM network management mode.

The Gazelle S1512i-PWR 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 conduct remote Telnet configuration.
- SSH mode: before accessing the Gazelle S1512i-PWR through SSH, you need to log in to the Gazelle S1512i-PWR and start the SSH service through the Console interface.

When configuring the Gazelle S1512i-PWR in network management mode, you must first configure the IP address of the VLAN interface on CLI, and then configure the Gazelle S1512i-PWR through the NView NNM system.

1.1.2 Accessing through Console interface

Introduction

The Console interface is an interface which is commonly used to connect the network device with a PC running the terminal emulation program. 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 configure and manage the Gazelle S1512i-PWR through the Console interface when the network fails.

In the following two conditions, you can only log in to the Gazelle S1512i-PWR and configure it through the Console interface:

- The Gazelle S1512i-PWR is powered on to start for the first time.
- Accessing the Gazelle S1512i-PWR through Telnet fails.

Accessing device from RJ45 Console interface

If you want to access the Gazelle S1512i-PWR through RJ45 Console interface from a PC, 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 on a PC, to configure communication parameters as shown in Figure 1-2, and then log in to the Gazelle S1512i-PWR.

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

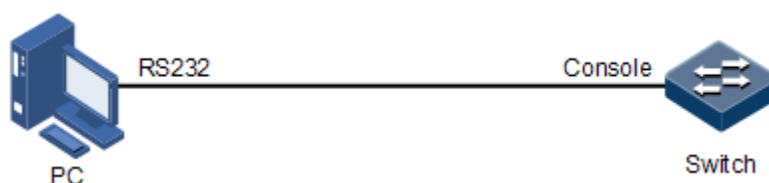
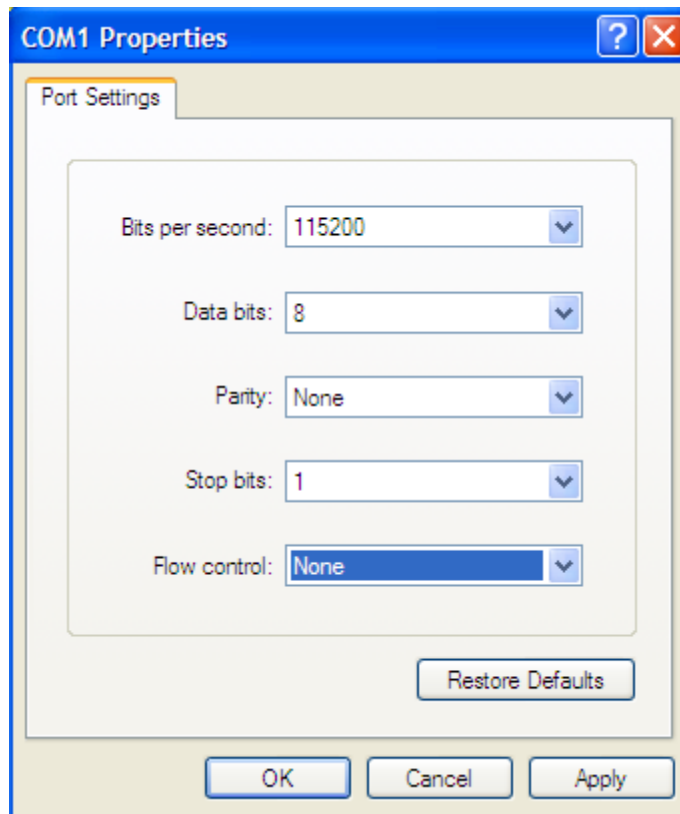


Figure 1-2 Configuring communication parameters in Hyper Terminal



The Gazelle S1512i-PWR supports logging in from the Console interface by using the password only instead of the user name and password.

Step	Command	Description
1	Raisecom#line password password	Configure the password for logging in from the Console interface. The password should have at least 8 characters including lowercase letters, uppercase letters, and numbers.
2	Raisecom#console login line	Configure the mode for logging in from the Console interface to the password only instead of the user name and password.

1.1.3 Accessing through Telnet

Telnet enables you to log in to the Gazelle S1512i-PWR remotely from a PC. Log in to the Gazelle S1512i-PWR from the PC, and then Telnet other Gazelle S1512i-PWR devices on the network. You do not need to connect a PC to each Gazelle S1512i-PWR. In Telnet connection status, if you enter the password incorrectly for three 3 times, the Telnet connection will be automatically disconnected.

Telnet services provided by the Gazelle S1512i-PWR are as below:

- Telnet Server: run the Telnet Client program on a PC to log in to the Gazelle S1512i-PWR, and conduct configuration and management. As shown in Figure 1-3, Gazelle S1512i-PWR is providing Telnet Server service at this time.

Figure 1-3 Networking with device as Telnet server



 **Note**

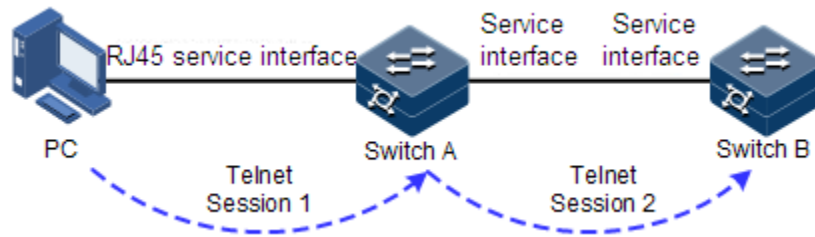
The Gazelle S1512i-PWR supports up to 10 Telnet users.

Before accessing the Gazelle S1512i-PWR through Telnet, you need to log in to the Gazelle S1512i-PWR through the Console interface and start the Telnet service. Configure the Telnet service for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface vlan 1</code>	Enter VLAN interface 1.
3	<code>Raisecom(config-vlan1)#ip address ip-address [ip- mask] [sub] Raisecom(config-vlan1)#ipv6 address ipv6-address/ipv6- mask link-local</code>	Configure the IP address of VLAN interface 1.
4	<code>Raisecom(config-vlan1)#exit</code>	Return to global configuration mode.
5	<code>Raisecom(config)#telnet- server accept interface-type interface-list</code>	(Optional) configure the interface that supports the Telnet function.
6	<code>Raisecom(config)#telnet- server access-list { ip access-list number ipv6 access-list number }</code>	(Optional) configure the Telnet ACL.
7	<code>Raisecom(config)#telnet- server close terminal-telnet session-number</code>	(Optional) release the specified Telnet session.
8	<code>Raisecom(config)#telnet- server max-session session- number</code>	(Optional) configure the maximum number of Telnet sessions supported by the Gazelle S1512i-PWR. By default, it is 10.

- Telnet Client: when you connect to the Gazelle S1512i-PWR through the terminal emulation program or Telnet Client program on a PC, then telnet another Gazelle S1512i-PWR and configure/manage them. As shown in Figure 1-4, Switch A not only works as the Telnet server but also provides the Telnet Client service.

Figure 1-4 Networking with device as Telnet client



Configure Telnet Client as below.

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

1.1.4 Accessing through SSH

Telnet is lack of security authentication and it transports messages through Transmission Control Protocol (TCP) which poses a 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 commands. SSHv2 is a network security protocol, which can effectively prevent information disclosure 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 establishes a secure channel over TCP. Moreover, SSHv2 supports other service ports besides standard port 22, avoiding illegal attacks from the network.

Before accessing the Gazelle S1512i-PWR through SSHv2, you must log in to the Gazelle S1512i-PWR through the Console interface and start SSH service.

Default configurations for accessing the Gazelle S1512i-PWR 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
SSH authentication timeout	600s
Number of SSHv2 authentication failures allowed by the device	20
SSH snooping port number	22
SSH session status	Disable
SSH version	v2

Configure SSH service for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#generate ssh-key length</code>	Generate local SSHv2 key pair and designate its length. By default, it is 512 bits.
3	<code>Raisecom(config)#ssh2 server</code>	Start the SSH server. By default, it is not started. Use the no ssh2 server command to shut down the SSH server. (Optional) configure SSH key renegotiation period.
4	<code>Raisecom(config)#ssh2 server authentication { password rsa-key }</code>	(Optional) configure SSHv2 authentication mode. By default, it is password.
5	<code>Raisecom(config)#ssh2 server authentication public-key public key</code>	(Optional) record the public key of the client on the Gazelle S1512i-PWR in rsa-key authentication mode.
6	<code>Raisecom(config)#ssh2 server authentication-timeout period</code>	(Optional) configure the SSHv2 authentication timeout. The Gazelle S1512i-PWR 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	<code>Raisecom(config)#ssh2 server authentication-retries times</code>	(Optional) configure the allowable failure times for SSHv2 authentication. The Gazelle S1512i-PWR 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.
8	<code>Raisecom(config)#ssh2 server port port-number</code>	(Optional) configure SSHv2 snooping port number. By default, it is 22.  Note 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 Telnet sessions supported by the Gazelle S1512i-PWR. By default, it is 10.

Step	Command	Description
10	<code>Raisecom(config)#ssh2 access-list { ip access-list number ipv6 access-list number }</code>	(Optional) configure the SSH ACL number.
11	<code>Raisecom(config)#ssh2 server close session session-number</code>	(Optional) close the specified SSHv2 session.

1.1.5 Configuring Banner

By using a Banner, you can configure welcome information and prompt, such as the influence on modifying configurations, precautions, or disclaimer. The Banner appears when you log in to or exit the Gazelle S1512i-PWR.

Configure the Banner for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#b anner login char message</code>	Configure the prompt for logging in to the Gazelle S1512i-PWR. <ul style="list-style-type: none"> <i>char</i>: information separator, 1 byte. You can enter any characters except "&", "<", ">", "(", ")", "[", "]", " ", "\", """, and """, and the start and end characters must be the same. <i>message</i>: contents of the Banner. You can enter up to 2560 characters.
3	<code>Raisecom(config)#b anner enable</code>	Enable Banner.

1.1.6 Checking configurations

Use the following commands to check the configuration results.

No.	Command	Description
1	<code>Raisecom#show telnet-server</code>	Show configurations of Telnet Server.
2	<code>Raisecom#show ssh public- key [authentication]</code>	Show the public key for SSH authentication on the device and client.
3	<code>Raisecom#show ssh { server session }</code>	Show information about the SSH server and session.
4	<code>Raisecom#show banner login</code>	Show configurations of the Banner.

1.1.7 Configuring console

Introduction

If you enter the incorrect login password over three times, the console will deny your further login. You have to wait until the silent time for login failure expires.

The Gazelle S1512i-PWR supports logging off users after expiration; in other words, if you perform no operations within the specified time, you will be logged off. Then you will have to log in to the console again.

Configurations of the console are basic configurations for operating the Gazelle S1512i-PWR. You can configure the console as required.

Default configurations

Default configurations of the console are as below.

Function	Default value
Logoff time for terminal expiration	600s
Silent time for login failure	3s

Configuring console

Configure the console for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#terminal time-out <i>period</i></code>	Configure the logoff time for the console expiration.
2	<code>Raisecom#logout</code>	Log off the Gazelle S1512i-PWR.

Checking configurations

Use the following commands to check the configuration results.

No.	Command	Description
1	<code>Raisecom#show terminal</code>	Show configurations of the console.

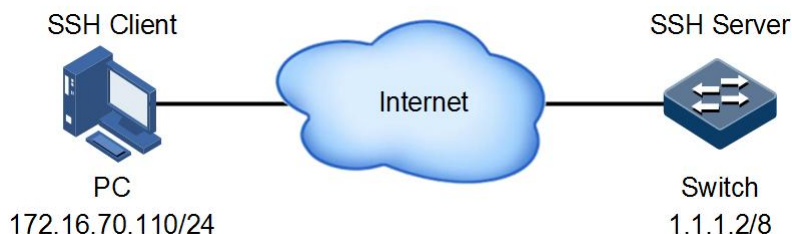
1.1.8 Example for configuring SSH login

Networking requirements

As shown in Figure 1-5, when a user logs in to the switch remotely from a PC through an insecure network, you must configure SSH Server and RSA authentication on the Switch to guarantee security of data exchange, with detailed requirements as below:

- Configure the SSH authentication timeout to 400s and allowed authentication failure times to 3.
- Disable SSH sessions 1, 3, and 4.
- Configure the public key name of SSH authentication to raisecom and mode to rsa-key.
- Configure the default name for SSH login to raisecom.

Figure 1-5 Configuring SSH login



Configuration steps

- Step 1 Configure a routing protocol to make the route between the Gazelle S1512i-PWR and PC available. Detailed configurations are omitted.
- Step 2 Generate a local SSH key pair, and enable SSH Server.

```
Raisecom#config  
Raisecom(config)#generate ssh-key  
Raisecom(config)#ssh2 server
```

- Step 3 Configure the SSH authentication timeout to 400s and allowed authentication failure times to 3. Disable SSH sessions 1, 3, and 4.

```
Raisecom(config)#ssh2 server authentication-timeout 400  
Raisecom(config)#ssh2 server authentication-retries 3  
Raisecom(config)#ssh2 server close session 1  
Raisecom(config)#ssh2 server close session 3  
Raisecom(config)#ssh2 server close session 4
```

- Step 4 Generate a SSH public key, and save the SSH private key on the SSH client. This step is done in a terminal emulation program.

- Step 5 Write the client public key to the Gazelle S1512i-PWR. Copy the SSH public key generated in step 4, paste it in the terminal emulation program, and press **Ctrl+S** to save the public key.

```
Raisecom(config)#ssh server authentication raisecom public-key
(Ctrl+s) for save input and return
(Ctrl+z) for discard input and return.
-----
AAAAB3NzaC1yc2EAAAADAQABAAQgQCpVAVIDgyYBrKnVlrioF54MTodZR6Ah5I
MwgBb+z10QDrLpppY1EBYiad5z6AUNFizjB9xk/kRffBPXB+znMl9QStkEYZVrXT
R93pv0JihlSsurj2g1HjnJnNFRqpaIPNZTCBDeWANke3AGYdNyYlvtwbZuwQlOk0
/gJbiaYAFw==
```

- Step 6 Configure the SSH authentication mode to rsa-key.

```
Raisecom(config)#ssh server authentication rsa-key
```

- Step 7 Establish a SSH session. Log in to the Gazelle S1512i-PWR in SSH mode.

Checking results

Use the following command to view configurations of the SSH server.

```
Raisecom#show ssh server
SSH server information:
-----
State: Enable
Version: sshv2
Authentication method(default:local user-password ): rsa-key
Authentication timeout(default 600): 400s
Authentication retries(default 20): 3
Rekey interval time(default 0): 0h
Max client count(default 5): 2
Current client count: 0
Current channel count: 0
Listen port on (default 22): 22
```

Use the following command to view the SSH public key.

```
Raisecom#show ssh public-key
RSA public key :
---- BEGIN SSH PUBLIC KEY ----
Comment: "rsa-key"
AAAAB3NzaC1yc2EAAAADAQABAAQnr5LEevdxWU1urIwrkMVsfDSb/8IbsQ
qbbEA/J73JKJkyawhakluZVddiCDV8fKcuCKmg8fyem1X+pLRWRjoZlQ+Q==
Fingerprint: md5 e3:85:68:d3:31:52:f1:de:28:2b:de:68:af:42:69:c0
---- END SSH PUBLIC KEY ----
```

```
Authentication public key :
---- BEGIN SSH PUBLIC KEY ----
Comment: "rsa-key"

Public-key name: raisecom
Public-key:
AAAAB3NzaC1yc2EAAAADAQABAAQGCpVAVIDgyYBrKnVlrioFx54MTodZR6
Ah5IMWgBb+z10QDrLpppY1EBYiad5z6AUNFizjB9xk/kRffBPXB+znM19QSt
KEYZVrXTR93pv0Jih1sSURj2g1HjnJnNFRqpaIPNZTCBDeWANke3AGYdNyYl
vtwbZuwQ1ok0/gJbiaYAFw==

---- END SSH PUBLIC KEY ----
```

Use the following command to view information about the SSH session. Session 2 is established while sessions 1, 3, and 4 are disabled.

```
Raisecom#show ssh session
ID Ver Cipher(IN/OUT) Con-Time State UserId Ip
-----
1 -- --/-- -- Disable -- --
*2 2.0 aes/aes 0h:6m:21s OK(1channels) raisecom 172.16.70.110
3 -- --/-- -- Disable -- --
4 -- --/-- -- Disable -- --
5 -- --/-- -- Closed -- --
```

1.2 CLI

1.2.1 Introduction

The Command Line Interface (CLI) is a medium for you to communicate with the Gazelle S1512i-PWR. You can configure, monitor, and manage the Gazelle S1512i-PWR through the CLI.

You can log in to the Gazelle S1512i-PWR 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 Gazelle S1512i-PWR locally through the Console interface.
- Configure the Gazelle S1512i-PWR locally or remotely through Telnet/Secure Shell v2 (SSHv2).
- Commands are classified into different privileges. You can execute the commands that correspond to your privilege 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 Gazelle S1512i-PWR.

- Enter a question mark (?) at the system prompt to obtain online help.
- Support multiple intelligent analysis methods, such as fuzzy match and context association.

1.2.2 Privileges

The Gazelle S1512i-PWR 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.

1.2.3 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.

If the Gazelle S1512i-PWR is in default configuration, a "login" prompt will appear. After you enter the user name raisecom and password raisecom, it will enter user EXEC mode, and the screen will display:

```
Raisecom#
```



Note

Users under privilege 11 do not need to enter the password when entering privileged EXEC mode.

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

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



Note

- Command line prompt "Raisecom" is the default host name. You can use the **hostname** *string* command to modify the host name in privileged EXEC mode.
- 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 previous command mode.

- You can use the **end** command to return to privileged EXEC mode from any modes except privileged EXEC mode.

The Gazelle S1512i-PWR supports the following command line modes:

Mode	Enter method	Description
Privileged EXEC	After login, enter the user name and password at the prompt of login.	Raisecom#
Global configuration	In privileged EXEC mode, use the config terminal command.	Raisecom(config)#
Physical layer interface configuration	In global configuration mode, use the interface gigaethernet <i>unit/slot/interface</i> command.	Raisecom(config-gigaethernetunit/solt/port)#
Loopback interface configuration	In global configuration mode, use the interface loopback <i>lb-number</i> command.	Raisecom(config-loopback)#
VLAN configuration	In global configuration mode, use the vlan <i>vlan-id</i> command.	Raisecom(config-vlan)#
VLAN interface configuration	In global configuration mode, use the interface vlan <i>vlan-id</i> command.	Raisecom(config-vlanif)#
Aggregation group interface configuration	In global configuration mode, use the interface port-channel <i>channel-number</i> command.	Raisecom(config-port-channel)#
Route mapping configuration	In global configuration mode, use the route-map <i>map-name</i> { permit deny } <i>number</i> command.	Raisecom(config-route-map)#
OSPF configuration	In global configuration mode, use the router ospf <i>process-id</i> [router-id <i>router-id</i>] command.	Raisecom(config-router-ospf)#
Traffic classification configuration	In global configuration mode, use the class-map <i>class-map-name</i> command.	Raisecom(config-cmap)#
Traffic policy configuration	In global configuration mode, use the policy-map <i>policy-map-name</i> command.	Raisecom(config-pmap)#
Traffic policy configuration bound with traffic classification	In traffic policy configuration mode, use the class-map <i>class-map-name</i> command.	Raisecom(config-pmap-c)#
Basic IP ACL configuration	In global configuration mode, use the access-list <i>acl-number</i> command. In the command, <i>acl-number</i> ranges from 1000 to 1999.	Raisecom(config-acl-ipv4-std)#

Mode	Enter method	Description
Extended IP ACL configuration	In global configuration mode, use the access-list <i>acl-number</i> command. In the command, <i>acl-number</i> ranges from 2000 to 2999.	Raisecom(config-acl-ipv4-ext)#
MAC ACL configuration	In global configuration mode, use the access-list <i>acl-number</i> command. In the command, <i>acl-number</i> ranges from 3000 to 3999.	Raisecom(config-acl-mac)#
User ACL configuration	In global configuration mode, use the access-list <i>acl-number</i> command. In the command, <i>acl-number</i> ranges from 5000 to 5999.	Raisecom(config-acl-udf)#
MST region configuration	In global configuration mode, use the spanning-tree region-configuration command.	Raisecom(config-region)#
Profile configuration	In global configuration mode, use the igmp filter profile <i>profile-number</i> command.	Raisecom(config-igmp-profile)#
cos-remark configuration	In global configuration mode, use the mls qos mapping cos-remark <i>profile-id</i> command.	Raisecom(cos-remark)#
cos-to-pri configuration	In global configuration mode, use the mls qos mapping cos-to-local-priority <i>profile-id</i> command.	Raisecom(cos-to-pri)#
dscp-mutation configuration	In global configuration mode, use the mls qos mapping dscp-mutation <i>profile-id</i> command.	Raisecom(dscp-mutation)#
dscp-to-pri configuration	In global configuration mode, use the mls qos mapping dscp-to-local-priority <i>profile-id</i> command.	Raisecom(dscp-to-pri)#
SRED profile configuration	In global configuration mode, use the mls qos sred profile <i>profile-id</i> command.	Raisecom(sred)#
CMAF profile configuration	In global configuration mode, use the class-map <i>class-map-name</i> command.	Raisecom(config-cmap)#
Traffic monitoring profile configuration	In global configuration mode, enter the mls qos policer-profile <i>policer-name</i> [single] command.	Raisecom(traffic-policer)#
PMAP configuration	In global configuration mode, use the policy-map <i>policy-map-name</i> command.	Raisecom(config-pmap)

Mode	Enter method	Description
Traffic policy configuration bound with traffic classification	In PMAP configuration mode, use the class-map <i>class-map-name</i> command.	Raisecom(config-pmap-c)#
Chinese prompt	In any configuration mode, use the language chinese command.	Raisecom#
English prompt	In any configuration mode, use the language english command.	Raisecom#

1.2.4 Shortcut keys

The Gazelle S1512i-PWR supports the following shortcut keys.

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

Shortcut key	Description
Ctrl+A	Move the cursor to the beginning of the command.
Ctrl+B	Identical to the Left Arrow key.
Ctrl+C	Interrupt the ongoing command, such as ping and traceroute .
Ctrl+D or Delete	Delete the character at the cursor.
Ctrl+E	Move the cursor to the end of the command.
Ctrl+F	Identical to the Right Arrow key
Ctrl+K	Delete all characters from the cursor to the end of the command.
Ctrl+L	Clear screen information.
Ctrl+S	Identical to the Down Arrow key
Ctrl+W	Identical to the Up Arrow key
Ctrl+X	Delete all characters before the cursor (except the cursor location).
Ctrl+Y	Show history commands.
Ctrl+Z	Return to privileged EXEC mode from the current mode (except user EXEC mode).
Space bar or Y	Scroll down one screen.
Enter	Scroll down one line.

1.2.5 Acquiring help

Complete help

You can acquire complete help under following three conditions:

- You can enter a question mark (?) at the system prompt to view 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.

vlan1	
<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
cluster        cluster configuration
cluster-autoactive Cluster autoactive function
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 li?
```

The command output is as below.

```
link-state-tracking  Fault tracking
```

- 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 Gazelle S1512i-PWR 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 with "^" is invalid.
Ambiguous input in the position marked by '^'	The keyword marked with "^" is not clear.



Note

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

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

Filtering displayed information

The Gazelle S1512i-PWR 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 Gazelle S1512i-PWR 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 with the assigned string, in case-sensitive mode.
- | **include string**: show all lines only matching with 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# terminal page-break enable	Enable terminal page-break.

1.2.7 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 Gazelle S1512i-PWR as below.

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

1.2.8 Restoring default value of command line

The default value of command line can be restored by the **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 a feature while the **disable** parameter is used to disable the feature.

For example:

- In physical layer interface configuration mode, the **description text** command is used to modify descriptions of an interface while the **no description** command is used to delete descriptions of the interface and restore to the default values.
- In physical layer interface configuration mode, the **shutdown** command is used to shut down an interface while the **no shutdown** command is used to restart the 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 are often restored by the **no** form.

1.2.9 Logging commands

Configure command logging for the Gazelle S1512i-PWR as below.

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

1.3 User management

1.3.1 Introduction

When you start the Gazelle S1512i-PWR for the first time, connect the PC through Console interface to the Gazelle S1512i-PWR, enter the default user name and password in Hyper Terminal to access and configure the Gazelle S1512i-PWR.

If there is no privilege restriction, any remote user can log in to the Gazelle S1512i-PWR through Telnet or access network by building Point to Point Protocol (PPP) connection when service interfaces are configured with IP addresses. This is unsecure to the Gazelle S1512i-PWR and network. Creating users for the Gazelle S1512i-PWR and configuring password and privilege helps manage login users and ensures network and device security.

Authenticating users

Users can log in to the Gazelle S1512i-PWR after authentication. The authentication and authorization information is saved in the remote RADIUS server, remote TACACS+ server, and Network Access Server (NAS), namely, the local device.

- Users saved in the database of the local device are called local users.
- Users saved in the database of the remote RADIUS server or remote TACACS+ server are called remote authentication users.

Classifying user privileges

Command lines are protected by different authorities. Users of different privileges can execute commands of the corresponding privilege. User privileges are also user priorities, which are classified into 15 privileges corresponding to command levels, and four types:

- Privileges 1–4: users can execute visitor commands.
- Privileges 5–10: users can execute monitor or below commands.
- Privileges 11–14: users can execute operator or below commands.
- Privilege 15: users can execute administrator or below commands.

Managing user commands

Generally, users cannot execute a command that is above their privileges. You can modify this restriction by managing user commands, allowing them to execute some commands above their privileges, or prohibit them from executing some commands below their privileges.

1.3.2 Preparing for configurations

Scenario

To prevent malicious users from accessing the Gazelle S1512i-PWR through different modes, such as Telnet, and to eliminate risks on the Gazelle S1512i-PWR, you must effectively manage users in terms of basic information, login, and user commands.

Prerequisite

N/A

1.3.3 Default configurations of user management

Default configurations of user management are as below.

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

1.3.4 Configuring basic information about user

Create user basic information for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#user name user-name password [cipher simple] password</code>	Create a local user account, or modify the password of the specified user.
2	<code>Raisecom#user name user-name privilege privilege</code>	(Optional) configure the user priority.
3	<code>Raisecom#user user-name service-type { lan-access ssh telnet web console all }</code>	Configure the service type supported by the user.
4	<code>Raisecom#user name user-name state { active inactive }</code>	Configure the user activation status.
5	<code>Raisecom#password check { complex simple }</code>	(Optional) configure the strength for checking the user to configure or modify the password.



Note

- Besides the default user raisecom, up to 9 local user accounts can be created.
- The login password is a string of 8–16 characters, composed of digits, uppercase letters, and lowercase letters.

1.3.5 Managing user login

Manage user login for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# enable password [<i>cipher password</i>]	Modify the password entered for modify the user privilege.
2	Raisecom# enable [<i>privilege</i>]	Configure the user privilege.
3	Raisecom# user login { local-radius local-user radius-local radius-user local-tacacs tacacs-local tacacs-user }	Configure authentication mode for user login.
4	Raisecom# logout	Log off the device.



Note

Users under privilege 11 do not need to enter the password for entering privileged EXEC mode.

1.3.6 Managing user commands

Manage user commands for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# user <i>user-name</i> { allow-exec disallow-exec } <i>first-keyword</i> [<i>second-keyword</i>]	(Optional) configure the priority rule for login users to perform the command line. <ul style="list-style-type: none"> • Specifying the allow-exec parameter allows you to perform commands higher than the current priority. • Specifying the disallow-exec parameter disallows you to perform commands lower than the current priority only.



Note

- You cannot modify privilege of level 15 user through this command.
- Up to 15 management command rules can be configured for a user.

1.3.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show user table [detail]</code>	Show information about users of the Gazelle S1512i-PWR.
2	<code>Raisecom#show user active</code>	Show information about online users of the Gazelle S1512i-PWR.

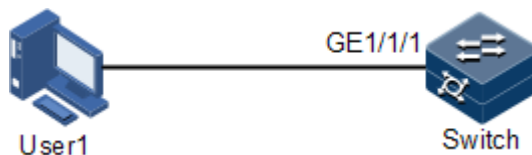
1.3.8 Example for configuring user management

Networking requirements

As shown in Figure 1-6, to prevent malicious users from logging in to the Gazelle S1512i-PWR and to eliminate risks on the Gazelle S1512i-PWR, configure user management as below:

- Configure the user login mode to local-user.
- Create a local user user1 with plain password of aaAA123@.
- Configure user1 privilege to privilege 10.
- Configure user1 service type to Telnet.
- Allow user 1 to execute commands starting with **mirror**.

Figure 1-6 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 user's service type.

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

Step 5 Configure user command management.

```
Raisecom#user user1 allow-exec mirror  
If the first key-word exist, please input 'yes' to confirm:yes
```

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 :0.0.0.0  
Login :telnet-1  
Status :online  
Service type:console telnet ssh web lan-access  
User State :active  
  
Username :user1  
Priority :10  
Server :0.0.0.0  
Login :--  
Status :offline  
Service type:telnet  
User State :active  
User command control config:  
-----  
Type:allow  
First keyword :mirror  
Second keyword :(null)  
-----
```

Use the newly-created user name user1 and password aaAA123@ to log in to the Gazelle S1512i-PWR, and check whether the user privilege is correctly configured.

```
Login:user1
```

```
Password:  
Raisecom#config  
Raisecom(config)#mirror remote-vlan 1  
Set successfully.
```

As you can see above, user 1 of privilege 10 can execute the command beginning with the **mirror** parameter successfully after you configure user command management.

1.4 File management

1.4.1 Introduction

System Bootrom file

The system Bootrom file (BootROM software) is used to initialize the Gazelle S1512i-PWR. After the Gazelle S1512i-PWR is powered on, the BootROM software is running to initialize the Gazelle S1512i-PWR. You can upgrade the BootROM software if a new version is available.

System startup file

The system startup file is used to start and operate the Gazelle S1512i-PWR. It supports the normal operation and implements functions of the Gazelle S1512i-PWR. You can upgrade the system startup file if a new version is available. In addition, to avoid a system fault, you can back up the system startup file. The Gazelle S1512i-PWR supports 2 sets of system startup software simultaneously, providing master-to-slave switching of dual systems.

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 Gazelle S1512i-PWR 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 Notepad 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 Gazelle S1512i-PWR 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 Gazelle S1512i-PWR uses default parameters for initialization.

The configuration that is currently used by the Gazelle S1512i-PWR is called the running configuration.

You can modify the running configuration of Gazelle S1512i-PWR 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.

1.4.2 Managing BootROM files

In Boot mode, you can do the following operations.

Operation	Description
t	Upgrade the system software to the Gazelle S1512i-PWR.
m	Update the boot file to the Gazelle S1512i-PWR.
b	Read the system software from the Gazelle S1512i-PWR and load it.
s	Specify the sequence for loading the system software upon device startup.
e	Clear environment variables.
r	Restart the Gazelle S1512i-PWR.
p	Configure the BootROM password.
?/h	Show information about help and system files.

Manage BootROM files for the Gazelle S1512i-PWR 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.

1.4.3 Managing system files

Manage system files for the Gazelle S1512i-PWR as below.

All the following steps are optional and in any sequence.

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

Step	Command	Description
3	Raisecom# upload system-boot { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> } { system1.z system2.z }	(Optional) upload the system boot file through FTP, SFTP, or TFTP.

1.4.4 Managing configuration files

Manage configuration files for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# download startup-config { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> } [<i>dir</i>]	(Optional) download the startup configuration file through FTP or TFTP.
2	Raisecom# download backup-config { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> } [<i>dir</i>]	(Optional) download the backup configuration file through FTP or TFTP.
3	Raisecom# erase [<i>file-name</i>]	(Optional) delete files saved in the Flash.
4	Raisecom# upload startup-config { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> } [<i>dir</i>]	(Optional) upload the startup configuration file through FTP or TFTP.
5	Raisecom# upload backup-config { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> } [<i>dir</i>]	(Optional) upload the backup configuration file through FTP or TFTP.
6	Raisecom# switch startup-config backup-config	(Optional) load the backup configuration file upon device startup.
7	Raisecom# upload command-log { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> } [<i>dir</i>]	(Optional) upload the command line logging file and system logs through FTP or TFTP.
8	Raisecom# upload logging-file { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> } [<i>dir</i>]	(Optional) upload the system log file through FTP or TFTP.
9	Raisecom# write	(Optional) save the running configuration file in the Flash.



1.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show startup-config	Show configurations loaded upon device startup.
2	Raisecom# show running-config	Show the running configurations.

1.4.6 Maintenance

Maintain the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# write [backup-config]	Save running configurations as a startup configuration file which can take effect upon next startup.  Caution 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# dir	Show names of system files.
3	Raisecom# erase [<i>file-name</i> backup-config]	Delete a specified system file. If the file-name parameter is not configured, this configuration will delete the startup configuration file.  Caution After a file is deleted through this command, it cannot be restored. Use this command with care.

1.5 Upgrading BootROM

1.5.1 Introduction

The BootROM file is used to initialize the Gazelle S1512i-PWR. You can upgrade the BootROM file through FTP or TFTP.



Note

Before upgrading system software, you should upgrade the BootROM file which is used to start system software.

1.5.2 Upgrading BootROM file through BootROM

Before upgrading the BootROM file through BootROM, you should establish an FTP environment, and use a PC as the FTP server and the Gazelle S1512i-PWR as the client. Basic requirements are as below.

- Configure the FTP server. Ensure that the FTP server is available.
- Configure the IP address of the FTP server; keep it in the same network segment with that of the Gazelle S1512i-PWR.

Upgrade the BootROM file through BootROM for the Gazelle S1512i-PWR as below.

Step	Operation
1	<p>Log in to the Gazelle S1512i-PWR through serial interface as the administrator, enter privileged EXEC mode, and restart the Gazelle S1512i-PWR through the reboot command.</p> <pre>Raisecom#reboot</pre>
2	<p>When the system successfully loads the big BootROM, and it displays "Press space to enter boot menu", press Space bar to enter the Raisecom interface. 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>
3	<p>Type "m" to upgrade the Boot software to the Gazelle S1512i-PWR.</p> <pre> [Raisecom]:m ipaddr: 192.168.5.100 serverip: 192.168.5.1 filename: gazelles1512i_BOOT_1.9.0_20171013 press y to confirm: y </pre>
4	<p>Type "r" to rapidly execute the big BootROM file. The Gazelle S1512i-PWR is restarted and will load the downloaded BootROM file.</p>

1.5.3 Upgrading BootROM file through CLI

Upgrade system software through CLI for the Gazelle S1512i-PWR as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Raisecom# upload bootstrap { ftp ip-address user-name password file-name tftp ip-address file-name }[dir]	(Optional) upload the BootROM file through FTP or TFTP.
2	Raisecom# download bootstrap { ftp ip-address user-name password file-name tftp ip-address file-name }[dir]	Download the BootROM file through FTP or TFTP.
3	Raisecom# reboot [now]	Restart the Gazelle S1512i-PWR.

1.5.4 Configuring BootROM password

When you enter BootROM command mode, the system will check whether the enter password and configured password are consistent. In this case, you can modify the BootROM password.

Configure the BootROM password for the Gazelle S1512i-PWR as below.

Step	Description
1	Log in to the Gazelle S1512i-PWR through serial interface as the administrator, enter privileged EXEC mode, and restart the Gazelle S1512i-PWR through the reboot command. Raisecom# reboot
2	When the system successfully loads the BootROM file, and it displays "Press space to enter boot menu", press Space bar to enter the Boot interface. The command list is displayed as below: <pre style="text-align: center;"> 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. [Boot]: </pre>

Step	Description
3	Type "p" to configure the password for entering the boot menu. [Boot]: p No password! Please input new password: **** Please input new password again: **** Saving Environment to SPI Flash... Erasing SPI flash...writing to SPI flash...done Password setting OK!
4	To delete the password, return to the Boot menu, type "e", enter the configured password, type "y", and press Enter . [Boot]: e Please input password for entering(3 tries):**** Password OK! press y to confirm: y SF: Detected MX66L51235F with page size 256 Bytes, erase size 64 KiB, total 64 MiB Done Please reboot to apply these changes!
5	Type "r" to rapidly execute the BootROM file. The Gazelle S1512i-PWR will be restarted



1.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show version	Show the current version of system software.

1.5.6 Maintenance

Maintain the Gazelle S1512i-PWR as below.

No.	Command	Description
1	<pre>Raisecom# write [backup- config]</pre>	<p>Write running configurations in the Flash, and save them as the startup configuration file. The startup configuration file will take effect upon next startup.</p> <p> Caution</p> <p>When you save running configurations as the new configuration file in the Flash, the file will overwrite the original startup configuration file. In this case, back up the original one in advance.</p>
2	<pre>Raisecom# dir</pre>	<p>Show information about the system file in the Flash.</p>
3	<pre>Raisecom# erase [file- name backup- config]</pre>	<p>Delete a specified system file. If the <i>file-name</i> parameter is not configured, this configuration will delete the startup configuration file.</p> <p> Caution</p> <p>After a file is deleted through this command, it cannot be restored. Use this command with care.</p>

1.6 Upgrading system software

1.6.1 Introduction

The Gazelle S1512i-PWR needs to be upgraded if you wish to add new features, optimize functions, or fix bugs in the current software version.

The Gazelle S1512i-PWR supports the following two upgrade modes:

- Upgrade through BootROM
- Upgrade through CLI

1.6.2 Upgrading system software through BootROM

You need to upgrade system software through BootROM in 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 an FTP environment, and use a PC as the FTP server and the Gazelle S1512i-PWR as the client. Basic requirements are as below.

- Configure the FTP server. Ensure that the FTP server is available.
- Configure the IP address of the FTP server; keep it in the same network segment with that of the Gazelle S1512i-PWR.

Upgrade system software through BootROM for the Gazelle S1512i-PWR as below.

Step	Operation
1	<p>Log in to the Gazelle S1512i-PWR through serial interface as the administrator, enter Privileged EXEC mode, and restart the Gazelle S1512i-PWR through the reboot command.</p> <p>Raisecom#reboot</p>
2	<p>When the system successfully loads the big BootROM, and it displays "Press space to enter boot menu", press Ctrl+B to enter the interface. The command list is displayed as below:</p> <pre style="text-align: center;"> 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>
3	<p>Type "t" to upgrade system software to the Gazelle S1512i-PWR.</p> <pre> [Raisecom]:t ipaddr: 192.168.1.1 serverip: 192.168.5.1 filename: SYSTEM_3.41.10 Current system partiton info: Partition number Name Size ----- 1 SYSTEM_3.41.10 18133504 2 None 0 Please input system partition number for upgrading(1-2):2 </pre>
4	<p>Type "r" to rapidly execute the BootROM file. The Gazelle S1512i-PWR is restarted and will load the downloaded BootROM file.</p>

Step	Operation									
5	<p>For dual systems, type "s" at the Boot prompt to configure the sequence for starting systems:</p> <pre>[Boot]:s</pre> <p>Current system partiton info:</p> <table border="1"> <thead> <tr> <th>Partition number</th> <th>Name</th> <th>Size</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>SYSTEM_3.41.10</td> <td>18133504</td> </tr> <tr> <td>2</td> <td>SYSTEM_3.41.9</td> <td>18133504</td> </tr> </tbody> </table> <p>Current boot sequence: 1,2</p> <p>Please input new boot sequence: 1-2</p> <p>Saving Environment to SPI Flash...</p> <p>Erasing has completed: 100%</p> <p>writing has completed: 100%</p> <p>done</p>	Partition number	Name	Size	1	SYSTEM_3.41.10	18133504	2	SYSTEM_3.41.9	18133504
Partition number	Name	Size								
1	SYSTEM_3.41.10	18133504								
2	SYSTEM_3.41.9	18133504								

1.6.3 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 Gazelle S1512i-PWR as the client. Basic requirements are as below.

- Connect the Gazelle S1512i-PWR to the FTP/SFTP/TFTP server.
- Configure the FTP/TFTP server, and ensure that the server is available.
- Configure the IP address of the FTP/TFTP server; the Gazelle S1512i-PWR can access the FTP/TFTP server.

Upgrade system software through CLI for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#download system-boot { ftp ip-address user-name password file-name tftp ip-address file-name } { system1.z system2.z }</code>	Download the system boot file through FTP/TFTP.
2	<code>Raisecom#boot sequence</code>	(Optional) configure the sequence for loading system software.

Step	Command	Description
3	Raisecom# reboot [now]	Restart the Gazelle S1512i-PWR, and it will automatically load the downloaded system BootROM file.

1.6.4 Checking configurations

Use the following commands to check configuration results.

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

1.7 Time management

1.7.1 Configuring time and time zone

To make the Gazelle S1512i-PWR work coordinately with other devices, you must configure the system time and local time zone accurately.

The Gazelle S1512i-PWR supports 3 system time modes, which are time stamp mode, auxiliary time mode, and default mode from high to low according to timing unit accuracy. You need to select the most suitable system time mode manually in accordance with actual application environment.

Default configurations of time and time zone are as below.

Function	Default value
Local time zone	+08:00
Time zone offset	+08:00
DST status	Disable
System clock display mode	Default

Configure time and time zone for the Gazelle S1512i-PWR as below.


Step	Command	Description
1	Raisecom# clock set <i>hour minute second year month day</i>	Configure system time.

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

1.7.2 Configuring DST

Daylight Saving Time (DST) is a kind of artificial regulation local time system for saving energy. At present, there are nearly 110 countries running DST every summer around the world, but different countries has different stipulations for DST; so you should use local condition when configuring DST.

Configure DST for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# clock summer-time enable	Enable DST.
2	Raisecom# clock summer-time recurring { <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> } { <u><i>fri</i></u> <u><i>mon</i></u> <u><i>sat</i></u> <u><i>sun</i></u> <u><i>thu</i></u> <u><i>tue</i></u> <u><i>wed</i></u> } <i>month hour minute offset-mm</i>	Configure calculation period for system DST.  Note 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 configuration 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. That is to say, the summer time is from the start time this year to the ending time of next year.

1.7.3 Configuring NTP

Network Time Protocol (NTP) is a time synchronization protocol defined by RFC1305. It is used to perform time synchronization between the distributed time server and clients. NTP transmits data based on UDP, using UDP port 123.

NTP is used to perform time synchronization on all devices with clocks on the network. Therefore, these devices can provide various applications based on the uniformed time. In addition, NTP can ensure a very high accuracy with an error about 10ms.

Devices, which support NTP, can both be synchronized by other clock sources and can synchronize other devices as the clock source.

The Gazelle S1512i-PWR adopts multiple NTP working modes for time synchronization:

- Client/Server mode

In this mode, the client sends clock synchronization message to different servers. The servers work in server mode automatically after receiving the synchronization message and send 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.

- Symmetric mode

In this mode, 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 response message back. By exchanging messages, the two peers build up the symmetric mode. The active and passive peers in this mode can synchronize each other.

Default configurations of NTP are as below.

Function	Default value
Whether the Gazelle S1512i-PWR is NTP master clock	No
Global NTP server	Inexistent
Global NTP equity	Inexistent
Reference clock source	0.0.0.0



Caution

NTP and SNTP are mutually exclusive, so they cannot be enabled concurrently.

Configure NTP for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ntp server ip-address [version [v1 v2 v3 v4]]</code>	(Optional) configure NTP server address for the client working in server/client mode.
3	<code>Raisecom(config)#ntp peer ip-address [version [v1 v2 v3 v4]]</code>	(Optional) configure the IP address of the NTP peer for the Gazelle S1512i-PWR working in symmetric mode.
4	<code>Raisecom(config)#ntp refclock-master [ip-address] [stratum]</code>	Configure the clock of the Gazelle S1512i-PWR as the NTP reference clock source for the Gazelle S1512i-PWR.



Note

If the Gazelle S1512i-PWR is configured as the NTP reference clock source, it cannot be configured as the NTP server or NTP symmetric peer; vice versa.

1.7.4 Configuring SNTP

Simple Network Time Protocol (SNTP) is used to synchronize the system time of the Gazelle S1512i-PWR with the time of the SNTP device on the network. The time synchronized by SNTP is Greenwich Mean Time (GMT), which can be translated into the local time according to system configurations of time zone.

Default configurations of SNTP are as below.

Function	Default value
IP address of the SNTP server	Inexistent

Configuring unicast feature of SNTP client

Configure unicast feature of SNTP client for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#sntp server ip-address</code>	Configure the IP address of the SNTP unicast server. After the SNTP server is configured with an IP address, the Gazelle S1512i-PWR tries to obtain clock signals from the SNTP server every 10s. In addition, the maximum timeout is 60s.

1.7.5 Checking configurations

Use the following commands to check configuration results.

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

1.8 Interface management

1.8.1 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 Gazelle S1512i-PWR 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. When 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 Gazelle S1512i-PWR supports auto-MDI/MDIX.

1.8.2 Default configurations of interface management

Default configurations of interface management are as below.

Function	Default value
Interface MTU	12288 bytes
Duplex mode of the interface	Auto-negotiation
Interface rate	Auto-negotiation
Interval for monitoring the interface rate	5s
Interface rate statistics status	Disable
Interval for interface dynamic statistics	2s
Interface flow control status	Disable
Interface status	Enable
L2protocol peer STP status	Disable

1.8.3 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 thus 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. When 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 basic attributes of the interface for the Gazelle S1512i-PWR 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)#duplex { auto full half }</code>	Configure the duplex mode of the interface.
4	<code>Raisecom(config- gigaethernet1/1/port)#speed { auto 10 100 1000 }</code>	Configure the interface rate. It depends on specifications of the optical module for the optical interface.
5	<code>Raisecom(config- gigaethernet1/1/port)#tpid { 8100 9100 88a8 }</code>	(Optional) configure the interface TPID. By default, it is 0x8100.
6	<code>Raisecom(config- gigaethernet1/1/port)#jumbofra me frame-size</code>	Configure the MTU on the interface. It ranges from 1518 to 10240 bytes.
7	<code>Raisecom(config- gigaethernet1/1/port)#mdi { xover auto normal }</code>	(Optional) configure the MDI/MDIX mode of the electrical interface.
8	<code>Raisecom(config- gigaethernet1/1/port)#vibratio n-suppress peroid second</code>	(Optional) configure the period for interface vibration suppression.

1.8.4 Configuring interface rate statistics

Configure interface rate statistics for the Gazelle S1512i-PWR as below.

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

Step	Command	Description
2	<code>Raisecom(config)#dynamic statistics time <i>time</i></code>	Configure the period for dynamic statistics.
3	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
4	<code>Raisecom(config-gigaethernet1/1/port)#clear interface statistics</code>	(Optional) clear statistics on the interface rate.

1.8.5 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 Gazelle S1512i-PWR as below.

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

1.8.6 Shutting down/Restarting interface

Shut down/Restart an interface for the Gazelle S1512i-PWR as below.

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

1.8.7 Configuring L2Protocol Peer STP


To interconnect with the device that sends STP packets with the destination MAC address of 0180.C200.0008, configure L2Protocol Peer STP. When this function is enabled, the destination MAC address of STP BPDUs is 0180.C200.0008; otherwise, it is 0180.C200.0000.

Configure L2Protocol Peer STP for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/port)# l2protocol peer stp	Enable L2Protocol Peer STP.

1.8.8 Configuring Console interface

Configure the Console interface for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# console open	(Optional) enable the Console interface. Use this command in non-Console command lines only.  Caution If you use the console close command to disable the Console interface, this will cause the Gazelle S1512i-PWR to be out of control. Use it with caution.
3	Raisecom(config)# login-trap enable	(Optional) enable sending Trap upon user login or exit.
4	Raisecom# line password <i>password</i>	(Optional) configure the plaintext password for logging in from the serial interface.
5	Raisecom# line encrypt-password <i>password</i>	(Optional) configure the ciphertext password for logging in from the serial interface. The encryption algorithm is 3dex.
6	Raisecom# console login line	(Optional) configure the mode for logging in from the serial interface to password only, instead of the user name and password.

1.8.9 Checking configurations


Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show interface [<i>interface-type interface-number</i>]	Show interface status.

No.	Command	Description
2	Raisecom# show interface <i>interface-type interface-number</i> statistics [dynamic] [detail]	Show interface statistics.
3	Raisecom# show l2protocol peer stp [<i>interface-type interface-number</i>]	Show the L2protocol Peer STP status.

1.9 Configuring basic information

Configure basic information for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# host name <i>name</i>	(Optional) configure the host name. By default, the host name is Raisecom. The system supports changing the host name to make users distinguish different hosts on the network. When the host name changes, it can be seen in terminal prompt.
2	Raisecom# language { chinese english }	(Optional) configure language mode. By default, the language is English.
3	Raisecom# write	Save configurations. Save configurations to the Gazelle S1512i-PWR after configurations are complete, and new configurations will overwrite the original configurations. Without saving, new configurations will be lost after restart, and the Gazelle S1512i-PWR will continue to work with original configurations.  Caution Use the erase file-name command to delete the configuration file. This operation cannot be rolled back, so use this command with caution.
4	Raisecom# reboot [now]	(Optional) configure restart options. When the Gazelle S1512i-PWR fails, restart it to try to solve the problem according to actual condition.

Caution

- Restarting the Gazelle S1512i-PWR interrupts services, so use the command with caution.
- Save configurations before restarting to avoid loss of configurations.

1.10 Task scheduling

1.10.1 Introduction

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

The Gazelle S1512i-PWR supports task scheduling by combining the program list with commands. 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 periodically execute commands.

1.10.2 Configuring task scheduling

Configure task scheduling for the Gazelle S1512i-PWR as below.

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

1.10.3 Checking configurations

Use the following command to check configuration results.

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

1.11 Watchdog

1.11.1 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 known as the Watchdog is specially used.

The Gazelle S1512i-PWR will be restarted when it fails to work due to task suspension or endless loop, and it neither sends signals to restart the waterdog timer.

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

1.11.2 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

1.11.3 Default configurations of Watchdog

Default configurations of Watchdog are as below.

Function	Default value
Watchdog status	Enable Watchdog.

1.11.4 Configuring Watchdog

Configure Watchdog for the Gazelle S1512i-PWR as below.

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

1.11.5 Checking configurations

Use the following command to check configuration results.

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

2 Ethernet

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

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

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

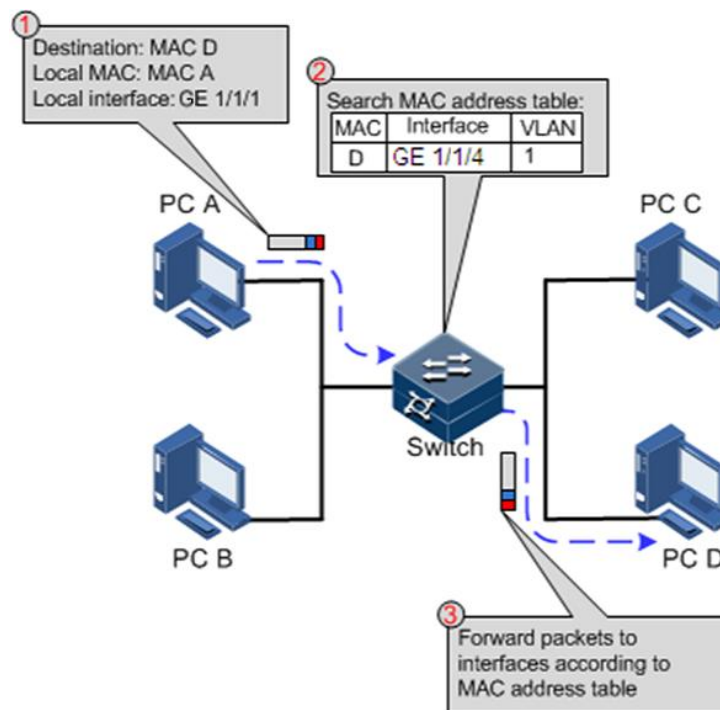
The Gazelle S1512i-PWR supports showing MAC address information by device, interface, or VLAN.

Forwarding modes of MAC addresses

When forwarding packets, based on the information about MAC addresses, the Gazelle S1512i-PWR 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 Gazelle S1512i-PWR will directly forward the packet to the Rx interface through the egress interface of the MAC address entry. If the entry is not listed, the Gazelle S1512i-PWR broadcasts the packet to all interfaces except the Rx interface, as shown in Figure 2-1.

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



- Multicast: when the Gazelle S1512i-PWR 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 Gazelle S1512i-PWR receives an all-F packet, or the MAC address is not listed in the MAC address table, the Gazelle S1512i-PWR forwards the packet to all interfaces except the interface that receives this packet. Broadcast addresses are special multicast addresses.

Classification of MAC addresses

The MAC address table contains static address entries and dynamic address entries.

- 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 restarted.

- Dynamic MAC address entry: the Gazelle S1512i-PWR can add dynamic MAC address entries through MAC address learning. The entries are aged according to the configured aging time, and will be cleared after the system is restarted.

The Gazelle S1512i-PWR supports up to 16K dynamic MAC addresses. Each interface supports 1024 static MAC addresses.

Aging time of MAC addresses

There is limit on the capacity of the MAC address table on the Gazelle S1512i-PWR. To maximize the use of the MAC address table, the Gazelle S1512i-PWR uses the aging mechanism to update the MAC address table. For example, when the Gazelle S1512i-PWR creates a dynamic entry, it starts the aging timer. If it fails to receive packets from the MAC address in the entry during the aging time, the Gazelle S1512i-PWR will delete the entry.

The Gazelle S1512i-PWR 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 Gazelle S1512i-PWR searches the MAC address table for the interface related to the destination MAC address of packets.

- If it is 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 interfaces are sent to the MAC address, the Gazelle S1512i-PWR can send them to the related interface.
- If it fails, 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. It is effective to manage the MAC address table.

The MAC address limit improves the rate 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, and financial staff), and fixed and important hosts to ensure that all data forwarded to these MAC addresses is forwarded from an interface related to the static MAC address in priority.

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

You can 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
Aging time of MAC addresses	300s
MAC address limit	Unlimited

2.1.4 Configuring static MAC address

Configure the static MAC address as below.

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



Note

- The MAC address of the source device, multicast MAC address, FFFF.FFFF.FFFF, and 0000.0000.0000 cannot be configured as the static unicast MAC address.
- The maximum number of static unicast MAC addresses supported by each interface on the Gazelle S1512i-PWR is 1024.

2.1.5 Configuring blackhole MAC address

Configure the blackhole MAC address as below.

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

2.1.6 Filtering unknown multicast packets

Filter unknown multicast packets for the Gazelle S1512i-PWR as below.

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

2.1.7 Configuring MAC address learning

Configure MAC address learning for the Gazelle S1512i-PWR as below.

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

2.1.8 Configuring MAC address limit

Configure the MAC address limit for the Gazelle S1512i-PWR as below.

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

2.1.9 Configuring aging time of MAC addresses

Configure the aging time of MAC addresses for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mac-address aging-time { 0 <i>period</i> }	Configure the aging time of MAC addresses. The value 0 indicates no aging.

2.1.10 Enabling suppression of MAC address flapping

Enable suppression of MAC address flapping for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mac-address mac-move enable	Enable global suppression of MAC address flapping.
3	Raisecom(config)#mac-address mac-move trap enable	Enable MAC address flapping Trap.

2.1.11 Checking configurations

Use the following commands to check configuration results.

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

2.1.12 Maintenance

Maintain the Gazelle S1512i-PWR as below.

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

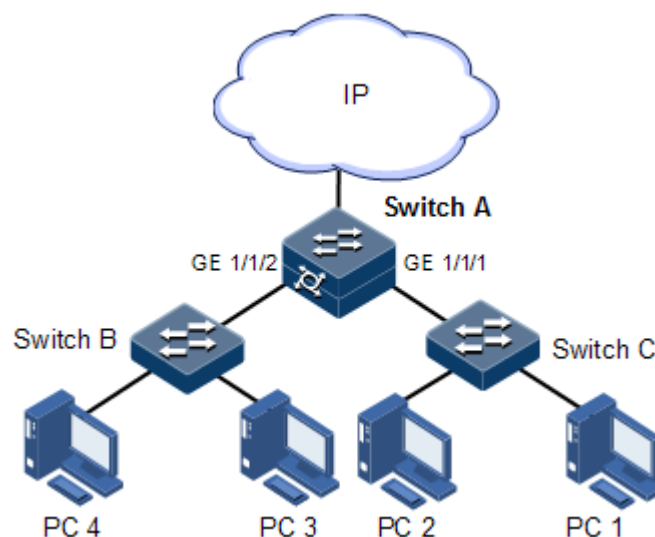
2.1.13 Example for configuring MAC address table

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

```
Raisecom#config
```



```
Raisecom(config)#create vlan 10 active
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport mode access
Raisecom(config-gigaethernet1/1/2)#switchport access vlan 10
Raisecom(config-gigaethernet1/1/2)#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
gigaethernet 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 gigaethernet 1/1/2
Aging time: 500 seconds
Mac Address      Port                vlan  Flags
-----
0001.0203.0405  gigaethernet1/1/2  10    Static
```

2.2 VLAN

2.2.1 Introduction

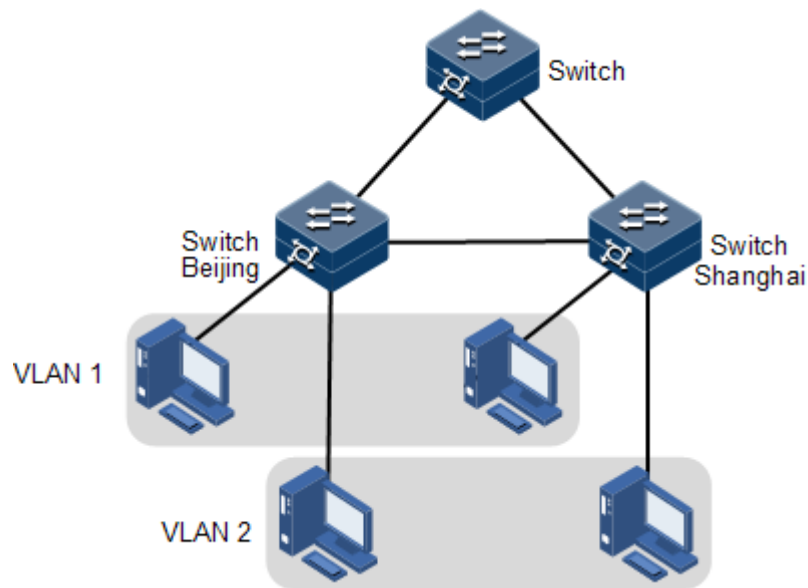
Overview

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 affecting each other. In terms of functions, VLAN has the same features as LAN, but members in one VLAN can access each other without restriction by physical location.

VLAN partitions

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

Figure 2-3 VLAN partitions



VLAN 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 Gazelle S1512i-PWR complies with IEEE 802.1Q standard VLAN and supports 4094 concurrent VLANs.

- VLAN partitions by interface

The Gazelle S1512i-PWR supports VLAN partitions by interface. The Gazelle S1512i-PWR 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"> • If the VLAN ID of the packet is equal to the Access VLAN ID, the interface will receive the packet. • If the VLAN ID of the packet is not equal to the Access VLAN ID, the interface will discard the packet. 	<ul style="list-style-type: none"> • If the VLAN ID of the packet is equal to the Access VLAN ID, the interface will remove the Tag and send the packet. • 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.
Trunk	Add the Native VLAN Tag to the packet.	<ul style="list-style-type: none"> • 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. • 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. 	<ul style="list-style-type: none"> • If the VLAN ID of the packet is equal to the Native VLAN ID, the interface will remove the Tag and send the packet. • 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.

- 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.

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 is that on 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 is that on 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 an enterprise that has many employees and needs a large number of hosts, in the same department but different positions. The hosts in one department can access one another so you 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 to 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 the static VLAN	Active
Interface mode	Access
Access VLAN	VLAN 1
Native VLAN of the 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 Gazelle S1512i-PWR as below.

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



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

2.2.5 Configuring interface mode

Configure the interface mode for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/port)#switchport mode { access trunk }</code>	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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/port)#switchport mode access Raisecom(config- gigaethernet1/1/port)#switchport access vlan <i>vlan-id</i></code>	Configure the interface to Access mode, and add the Access interface to the VLAN.

Step	Command	Description
4	Raisecom(config-gigaetherne1/1/port)# switchport access egress-allowed vlan { 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 permitted by the Access interface. The forwarded packets do not carry VLAN Tag.
- When you configure 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, default Access VLAN 1 is the VLAN allowed by the Access egress interface, you can delete Access VLAN 1 from the allowed VLAN list of Access the egress interface by deleting this VLAN.
- 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 default VLAN packets to pass.

2.2.7 Configuring VLAN on Trunk interface

Configure the VLAN on the Trunk interface for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaetherne1/1/port)# switchport mode trunk	Configure the interface to Trunk mode.
4	Raisecom(config-gigaetherne1/1/port)# switchport trunk native vlan <i>vlan-id</i>	Configure the Native VLAN of the interface.
5	Raisecom(config-gigaetherne1/1/port)# switchport trunk allowed vlan { all [add remove] <i>vlan-list</i> }	(Optional) configure VLANs allowed to pass by the Trunk interface.
6	Raisecom(config-gigaetherne1/1/port)# switchport trunk untagged vlan { all [add remove] <i>vlan-list</i> }	(Optional) configure VLANs from which the Trunk interface can remove Tags.
7	Raisecom(config-gigaetherne1/1/port)# switchport trunk native vlan { tagged untagged }	(Optional) configure Native VLAN packets of the Trunk interface to carry Tag or not.



- 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 the default VLAN if you have deleted or blocked Native VLAN manually.
- The interface allows ingress and egress VLAN packets allowed by the Trunk interface. If the VLAN is a Trunk untagged VLAN, the VLAN Tag is removed from the packets on the egress interface; otherwise the packets are not modified.
- When you configure the Trunk untagged VLAN list, the system automatically adds all untagged VLAN to the VLAN allowed by the Trunk interface.

2.2.8 Configuring VLAN partitions by MAC address

Configure VLAN partitions by MAC address for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mac-vlan mac-address vlan vlan-id [priority value]</code>	Associate the MAC address with the VLAN.
3	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
4	<code>Raisecom(config-gigaethernet1/1/1)#mac-vlan enable</code>	Enable MAC-VLAN.
5	<code>Raisecom(config-gigaethernet1/1/1)#vlan precedence mac-vlan</code>	Configure VLAN partitions by MAC address.



- When the MAC address is a multicast MAC address, all-0 MAC address, or all-F MAC address, the configuration will fail.
- If the association between a created MAC address and the VLAN conflicts with an existing association (for example, a MAC address is associated with different VLANs), this configuration will fail.

2.2.9 Configuring VLAN partitions by IP subnet

Configure VLAN partitions by IP subnet for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip-subnet-vlan ip-address [ip-mask] vlan vlan-id [priority priority]</code>	Associate the IP subnet with the VLAN.
3	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.

Step	Command	Description
4	Raisecom(config-gigaetherne1/1/port)# ip-subnet-vlan enable	Enable VLAN partitions by IP subnet.
5	Raisecom(config-gigaetherne1/1/port)# vlan precedence ip-subnet-vlan	(Optional) configure VLAN partitions by IP subnet with higher priority.

Caution

- When the IP address or subnet mask is invalid, this configuration will fail.
- If the association between a created IP subnet and the VLAN conflicts with an existing association (for example, an IP subnet is associated with different VLANs), this configuration will fail.

2.2.10 Checking configurations

Use the following commands to check configuration results.

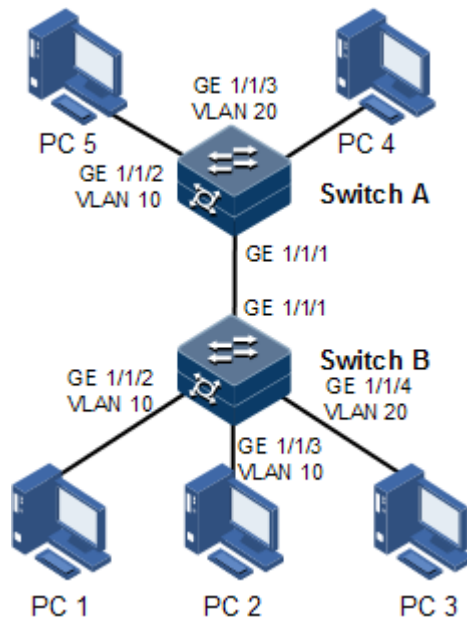
No.	Command	Description
1	Raisecom# show vlan [<i>vlan-list</i> static]	Show VLAN configurations.
2	Raisecom# show switchport interface <i>interface-type interface-number</i>	Show VLAN configurations on the interface.
3	Raisecom# show mac-vlan { all vlan <i>vlan-id</i> }	Show configurations of the association between the MAC address and VLAN.
4	Raisecom# show ip-subnet-vlan { all vlan <i>vlan-id</i> }	Show configurations of the association between the IP subnet and VLAN.
5	Raisecom# show vlan precedence	Show configurations of priorities of VLAN partitions.

2.2.11 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 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 Switch devices 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 as 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 gigaehternet 1/1/2
SwitchB(config-gigaehternet1/1/2)#switchport mode access
SwitchB(config-gigaehternet1/1/2)#switchport access vlan 10
SwitchB(config-gigaehternet1/1/2)#exit
SwitchB(config)#interface gigaehternet 1/1/3
SwitchB(config-gigaehternet1/1/3)#switchport mode access
SwitchB(config-gigaehternet1/1/3)#switchport access vlan 10
SwitchB(config-gigaehternet1/1/3)#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  --        gigabitEthernet1/1/2
gigabitEthernet1/1/3
20  VLAN0020         active  static  --        gigabitEthernet1/1/4
```

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 gigabitEthernet 1/1/2
Interface: gigabitEthernet1/1/2
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 QinQ

2.3.1 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 Tags 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 VLAN Tag is transmitted as data in packets.

Figure 2-5 Principles of basic QinQ

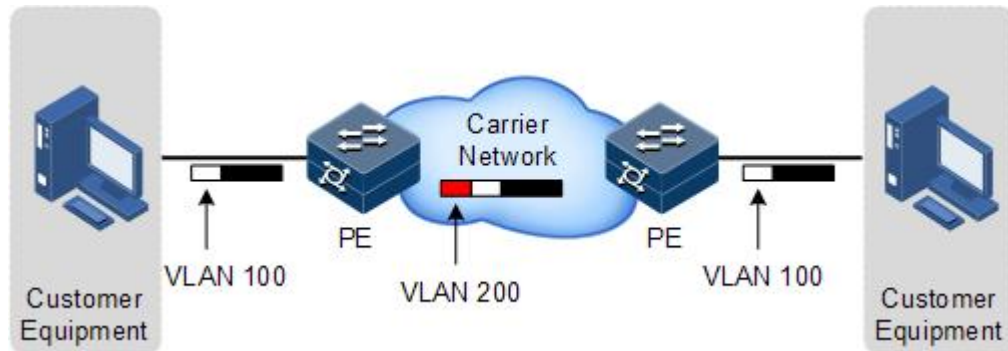


Figure 2-5 shows typical networking of basic QinQ; the Gazelle S1512i-PWR is the PE.

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.

QinQ 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 of flows 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.

2.3.2 Preparing for configurations

Scenario

Basic QinQ configuration and selective QinQ configuration for the Gazelle S1512i-PWR 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 the VLAN ID on the SP 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 IDs on the user network which are divided by adding different outer VLAN Tags 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

Basic QinQ and selective QinQ cannot be concurrently configured.

2.3.3 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

2.3.4 Configuring basic QinQ

Configure basic QinQ on the ingress interface for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/port)# dot1q-tunnel1	Enable basic QinQ on the interface.
4	Raisecom(config-gigaethernet1/1/port)# switchport reject-frame { tagged untagged }	Configure the types of packets disallowed to be forwarded.



Note

- To configure basic QinQ 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.

2.3.5 Configuring selective QinQ

Configure selective QinQ on the ingress interface for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaetherne1/1/port)#dot1q-tunnel</code>	Enable basic QinQ.
4	<code>Raisecom(config- gigaetherne1/1/port)#switchport vlan-mapping cvlan <i>custom-vlan-list</i> [cos <i>cos-value</i>] add-outer <i>outer- vlan-id</i> [local-priority <i>localpri- value</i>]</code>	Configure selective QinQ to add the outer VLAN ID based on inner VLAN.
5	<code>Raisecom(config- gigaetherne1/1/port)#switchport vlan-mapping-miss discard</code>	Configure the interface to discard tagged packets that fail to match selective QinQ or VLAN mapping rules.
6	<code>Raisecom(config- gigaetherne1/1/port)#switchport vlan-mapping both { priority-tagged cvlan <i>custom-vlan-list</i> } add-outer <i>outer-vlan-id</i> { remove translate <i>vlan-id</i> } Raisecom(config- gigaetherne1/1/port)#switchport vlan-mapping both { untag inner <i>inner-vlan-id</i> } add-outer <i>outer- vlan-id</i></code>	Configure bidirectional selective QinQ, and add outer VLAN rules.



Note

VLAN mapping based on VLAN+CoS and VLAN mapping based on VLAN cannot be concurrently configured.

2.3.6 Configuring network-side interface to Trunk mode

Configure the network-side interface to Trunk mode for the Gazelle S1512i-PWR as below.

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

Step	Command	Description
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/port)#switchport mode trunk</code>	Configure interface trunk mode, permit double-tagged packet to pass.

2.3.7 Configuring TPID

Configure TPID on the network side interface for the Gazelle S1512i-PWR as below.

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

2.3.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show dot1q-tunnel</code>	Show configurations of basic QinQ.
2	<code>Raisecom#show vlan-mapping both interface <i>interface-number</i></code>	Show configurations of QinQ in both the ingress and egress directions of the interface.

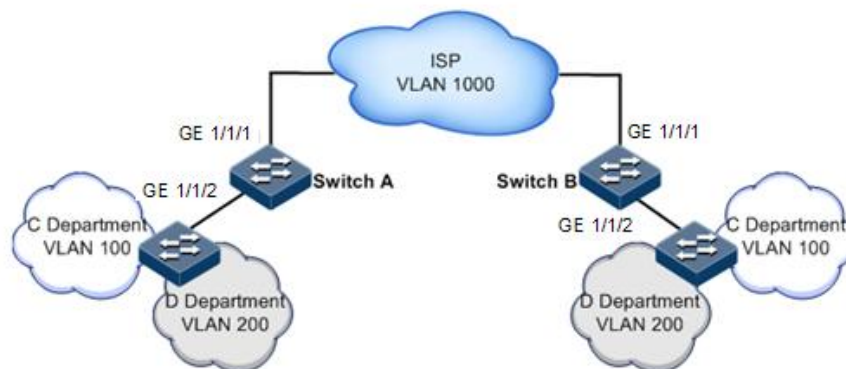
2.3.9 Example for configuring basic QinQ

Networking requirements

As shown in Figure 2-6, Switch A and Switch B are connected to two branches of Department C, which need to communicate through VLAN 1000 of the carrier network. Department C uses VLAN 100. 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 2-6 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, VLAN 200, and VLAN 1000, and activate them. TPID is 9100.

```
Raisecom#config
Raisecom(config)#create vlan 100,1000 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 1000
Raisecom(config-gigaethernet1/1/1)#tpid 9100
Raisecom(config-gigaethernet1/1/1)#exit
```

Step 2 Configure basic QinQ on the interface.

```
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport mode trunk
Raisecom(config-gigaethernet1/1/2)#switchport trunk native vlan 1000
Raisecom(config-gigaethernet1/1/2)#dot1q-tunnel
Raisecom(config-gigaethernet1/1/2)#switchport qinq default-cvlan 100
Raisecom(config-gigaethernet1/1/2)#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
```



```
-----
gigaehternet1/1/1    Enable    0x9100    -
gigaehternet1/1/2    Enable    0x8100    -
```

2.3.10 Example for configuring selective QinQ

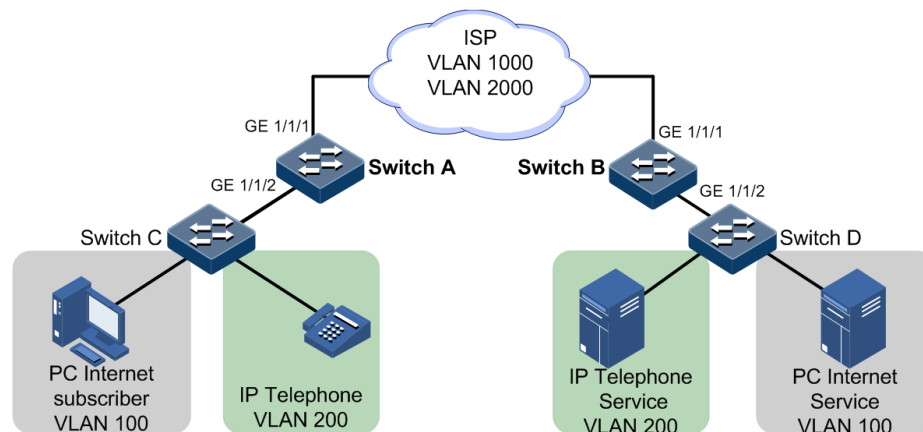
Networking requirements

As shown in Figure 2-7, the carrier network carries 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 VLAN 100 assigned to PC Internet access services.
- Add outer Tag 2000 to VLAN 200 for IP phone services.
- The carrier TPID is 9100.

Figure 2-7 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 VLAN 100, VLAN 200, VLAN 1000, and VAN 2000. The TPID is 9100.

```
Raisecom#name SwitchA
SwitchA#config
SwitchA(config)#create vlan 100,200,1000,2000 active
SwitchA(config)#interface gigaehternet 1/1/1
SwitchA(config-gigaehternet1/1/1)#switchport mode trunk
SwitchA(config-gigaehternet1/1/1)#switchport trunk allowed vlan 1000,2000
SwitchA(config-gigaehternet1/1/1)#tpid 9100
SwitchA(config-gigaehternet1/1/1)#exit
```

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

```
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
Raisecom(config-gigaethernet1/1/2)#switchport trunk allowed vlan
100,200,1000,2000
SwitchA(config-gigaethernet1/1/2)#switchport vlan-mapping both inner 100
add-outer 1000
SwitchA(config-gigaethernet1/1/2)#switchport vlan-mapping both inner 200
add-outer 2000
SwitchA(config-gigaethernet1/1/2)#exit
```

Checking results

Use the **show vlan-mapping inteface *interface-type interface-number* add-outer** command to show configurations of selective QinQ.

Take Switch A for example.

```
SwitchA#show vlan-mapping both interface gigaethernet 1/1/1
Original      Original  Add-outer  Add-outer  Add-Local  Hardware  Hardware
Port          Outer VLAN   COS      VLAN      COS        Prio      Status   ID
-----
GE1/1/2      100          --       1000     --         --        Enable   1
GE1/1/2      200          --       2000     --         --        Enable   2
```

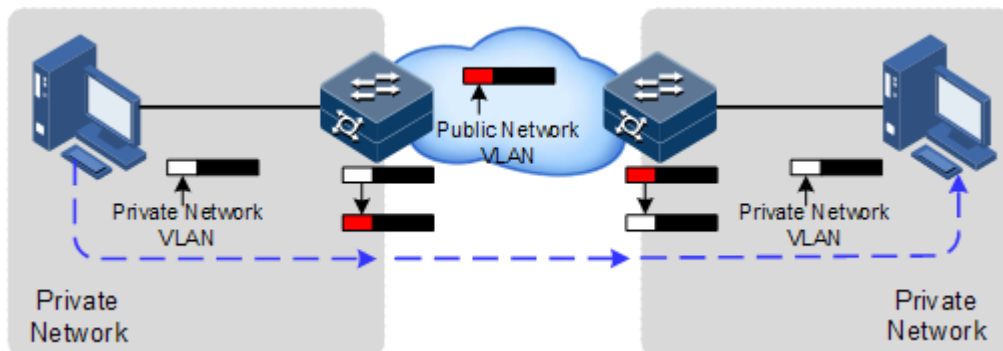
2.4 VLAN mapping

2.4.1 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 2-8 shows principles of VLAN mapping.

Figure 2-8 Principles of VLAN mapping



After receiving a user private network packet with a VLAN Tag, the Gazelle S1512i-PWR 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 Gazelle S1512i-PWR 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 need to modify VLAN Tag so that packets are transmitted according to the carrier's rules for forwarding VLAN packets.

2.4.2 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 into a carrier's VLAN ID.
- Multiple user services need to be mapped into a carrier's VLAN ID.

Prerequisite

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

2.4.3 Default configurations of VLAN mapping

Default configurations of VLAN mapping are as below.

Function	Default value
VLAN mapping status	Disable

2.4.4 Configuring VLAN mapping

Configure VLAN mapping for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaetherne t1/1/port) #switchport vlan-mapping ingress <i>outer-</i> <i>vlan-id</i> translate <i>outer-new-</i> <i>vlan-id</i>	Configure the VLAN mapping rule based on outer VLAN Tag in the ingress direction of the interface, and translate the outer VLAN only.
4	Raisecom(config- gigaetherne t1/1/port) #switchport vlan-mapping egress <i>outer-vlan-</i> <i>id</i> translate <i>outer-new-vlan-</i> <i>id</i>	Configure the VLAN mapping rule based on outer VLAN Tag in the egress direction of the interface, and translate the outer VLAN only.
5	Raisecom(config- gigaetherne t1/1/port) #switchport vlan-mapping both <i>outer</i> <i>outer-</i> <i>vlan-id</i> translate <i>outer-new-</i> <i>vlan-id</i>	Configure the VLAN mapping rule based on outer VLAN Tag in both the ingress and egress directions of the interface, and translate the outer VLAN only.
5	Raisecom(config- gigaetherne t1/1/port) #switchport vlan-mapping egress <i>outer</i> { all <i>outer-vlan-id</i> } inner <i>inner-</i> <i>vlan-id</i> outer { translate <i>outer-new-vlan-id</i> remove tagged unchanged } inner { translate <i>inner-new-vlan-id</i> remove tagged } Raisecom(config- gigaetherne t1/1/port) #switchport vlan-mapping egress <i>outer</i> { all <i>outer-vlan-id</i> } outer { translate <i>outer-new-vlan-id</i> remove tagged unchanged } inner { translate <i>inner-new-</i> <i>vlan-id</i> remove tagged }	Configure the VLAN mapping rule based on double Tag in the egress direction of the interface; in other words, VLANs are translated based on inner and outer VLAN Tag. Translate the inner and outer VLAN Tags.
6	Raisecom(config- gigaetherne t1/1/port) #switchport vlan-mapping ingress <i>outer</i> { all <i>outer-vlan-id</i> } inner { all <i>inner-vlan-id</i> } translate <i>outer</i> <i>outer-new-vlan-</i> <i>id</i>	Configure the VLAN mapping rule based on double Tag in the ingress direction of the interface; in other words, VLANs are translated based on inner and outer VLAN Tag. Translate the inner VLAN Tag.
7	Raisecom(config- gigaetherne t1/1/port) #switchport vlan-mapping both <i>outer</i> <i>outer-</i> <i>vlan-id</i> inner <i>inner-vlan-id</i> translate <i>outer</i> <i>outer-new-vlan-</i> <i>id</i> inner <i>inner</i> <i>-new-vlan-id</i>	Configure the VLAN mapping rule based on inner and outer VLAN Tag in both the ingress and egress directions of the interface.

Step	Command	Description
8	<code>Raisecom(config-gigaethernet1/1/port)#switchport vlan-mapping-miss discard</code>	Configure the rule for discard packet if VLAN mapping fails to be enabled.

2.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show switchport interface interface-type interface-number</code>	Show configurations of VLAN mapping.

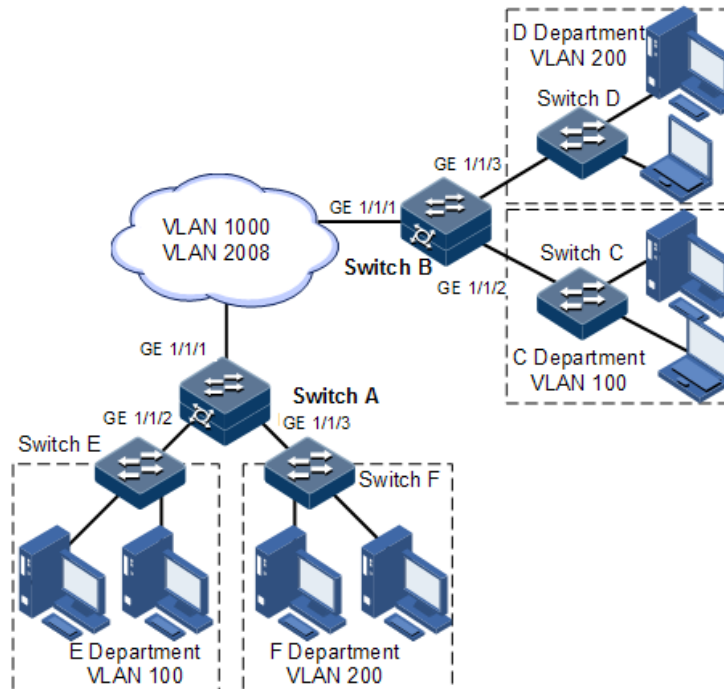
2.4.6 Example for configuring VLAN mapping

Scenario

As shown in Figure 2-9, 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 2-9 VLAN mapping networking



Configuration steps

Configure Switch A and Switch B.

Configurations of 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. Enable VLAN mapping.

```
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 gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk allowed vlan 1000,2008
confirm
SwitchA(config-gigaethernet1/1/1)#exit
```

Step 3 Configure GE 1/1/2 to Trunk mode, allowing packets of VLAN 1000 to pass. Configure VLAN mapping rules.

```
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
```

```
SwitchA(config-gigaethernet1/1/2)#switchport trunk allowed vlan 1000
SwitchA(config-gigaethernet1/1/2)#switchport vlan-mapping ingress 100
translate 1000
SwitchA(config-gigaethernet1/1/2)#switchport vlan-mapping egress 1000
translate 100
SwitchA(config-gigaethernet1/1/2)#exit
```

- Step 4 Configure GE 1/1/3 to Trunk mode, allowing packets of VLAN 2008 to pass. Configure VLAN mapping rules.

```
SwitchA(config)#interface gigaethernet 1/1/3
SwitchA(config-gigaethernet1/1/3)#switchport mode trunk
SwitchA(config-gigaethernet1/1/3)#switchport trunk allowed vlan 2008
SwitchA(config-gigaethernet1/1/3)#switchport vlan-mapping ingress 200
translate 2008
SwitchA(config-gigaethernet1/1/3)#switchport vlan-mapping egress 2008
translate 200
```

Checking results

Use the **show vlan-mapping interface tengigabitethernet 1/1/2 egress translate** command to show configurations of 1:1 VLAN mapping.

```
SwitchA#show vlan-mapping interface gigaethernet 1/1/2 egress translate
Interface : gigaethernet1/1/2
Hardware-ID: 2
Original Outer VLANs: 1000
Original Outer COS: --
Original Inner VLANs: --
Original Inner COS: --
Outer-tag Mode:      Translate
New Outer-VID:      100
New Outer-COS:      --
Inner-tag Mode:      --
New Inner-VID:      --
New Inner-COS:      --
```

2.5 STP/RSTP

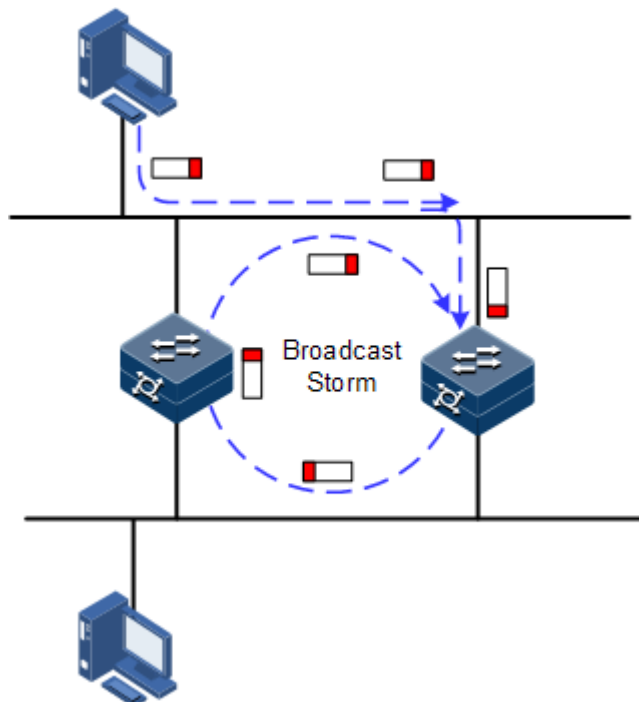
2.5.1 Introduction

STP

With the increasing complexity of network structure and growing number of switches on the network, Ethernet loops become the most prominent problem. Because of the packet

broadcast mechanism, a loop causes the network to generate storms, exhausts network resources, and seriously affects the forwarding of normal data. The network storm caused by the loop is shown in Figure 2-10.

Figure 2-10 Network storm due to loopback

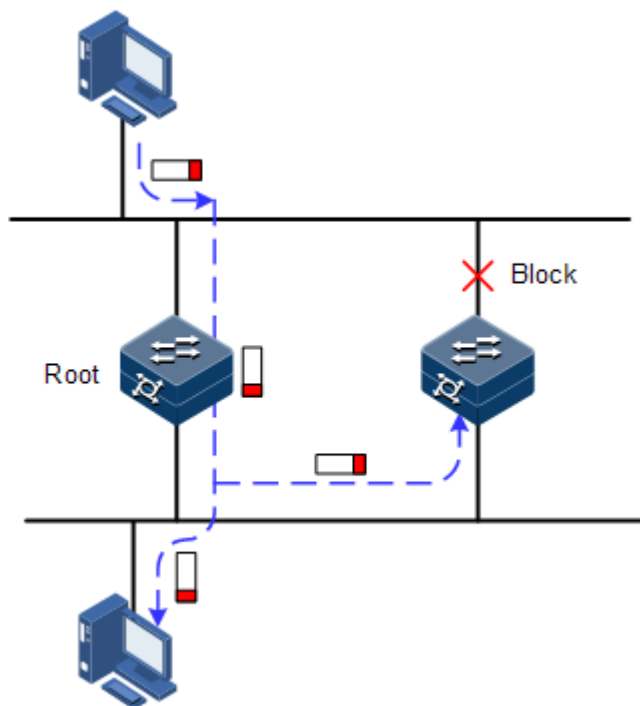


Spanning Tree Protocol (STP) is compliant to IEEE 802.1d standard and used to remove data physical loop in data link layer in the LAN.

The Gazelle S1512i-PWR running STP can process Bridge Protocol Data Unit (BPDU) with each other for the election of the root switch and selection of root port and designated port. It can also block the loop interface on the Gazelle S1512i-PWR logically according to the selection result, and finally trims the loop network structure to tree network structure without loops which takes an Gazelle S1512i-PWR as root. This prevents the continuous proliferation and limitless circulation of packets on the loop network from causing broadcast storms and avoids declining packet processing capacity caused by receiving the same packets repeatedly.

Figure 2-11 shows loop networking running STP.

Figure 2-11 Loop networking with STP



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

The major disadvantage of STP is the slow convergence rate.

RSTP

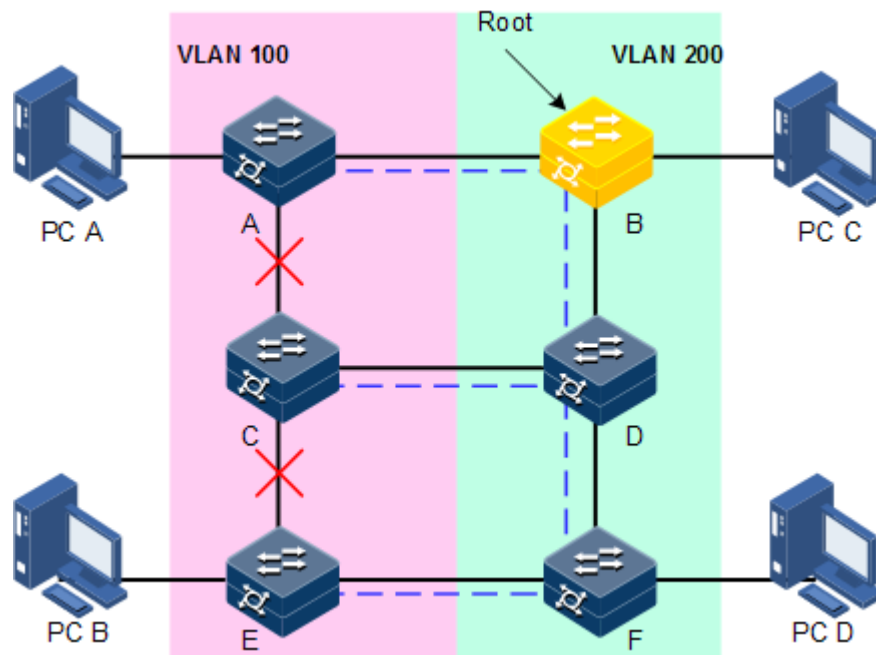
To improve the slow convergence rate of STP, IEEE 802.1w establishes Rapid Spanning Tree Protocol (RSTP), which increases the mechanism of the interface to transit from the blocking status to forwarding status, and thus speeds up the topology convergence rate.

The purpose of STP/RSTP is to simplify a bridged LAN to a single 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 single 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.
- Packets of partial VLANs cannot be forwarded when the network structure is asymmetrical. As shown in Figure 2-12, Switch B is the root switch; RSTP blocks the link between Switch A and Switch C logically, causing packets of VLAN 100 to fail to be forwarded and communication between Switch A and Switch C to fail.

Figure 2-12 Failure in forwarding VLAN packets due to RSTP



2.5.2 Preparing for configurations

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 loops, 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.

Prerequisite

N/A

2.5.3 Default configurations of STP

Default configurations of STP are as below.

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

Function	Default value
Forward Delay timer	15s

2.5.4 Enabling STP

Configure STP for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#spanning-tree enable	Enable global STP.
3	Raisecom(config)#spanning-tree mode { stp rstp }	Configure spanning tree mode.
4	Raisecom(config)#interface interface-type interface-number	Enter physical layer interface configuration mode.
5	Raisecom(config-gigaethernet1/1/port)#spanning-tree enable	Enable interface STP.

2.5.5 Configuring STP parameters

Configure STP parameters for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#spanning-tree priority priority-value	(Optional) configure device priorities.
3	Raisecom(config)#spanning-tree root { primary secondary }	(Optional) configure the Gazelle S1512i-PWR as the root or backup device.
4	Raisecom(config)#interface interface-type interface-number Raisecom(config-gigaethernet1/1/port)#spanning-tree priority priority-value	(Optional) configure interface priorities on the Gazelle S1512i-PWR.
5	Raisecom(config-gigaethernet1/1/port)#spanning-tree extern-path-cost cost-value Raisecom(config-gigaethernet1/1/port)#exit	(Optional) configure the external path cost of interfaces on the Gazelle S1512i-PWR.
6	Raisecom(config-gigaethernet1/1/port)#spanning-tree [instance instance-id] inter-path-cost cost	(Optional) configure the internal path cost of interfaces on the Gazelle S1512i-PWR.

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

2.5.6 (Optional) 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 quickly transfer to the 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 Gazelle S1512i-PWR are configured in auto-detection attribute.

Configure the edge interface for the Gazelle S1512i-PWR as below.

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

2.5.7 (Optional) 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 Gazelle S1512i-PWR as below.

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

2.5.8 Checking configurations

Use the following commands to check configuration results.

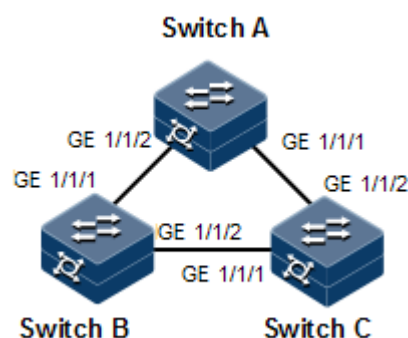
No.	Command	Description
1	Raisecom# show spanning-tree	Show basic configurations of STP.
2	Raisecom# show spanning-tree <i>interface-type interface-list</i> [detail]	Show STP configuration on the interface.

2.5.9 Example for configuring STP

Networking requirements

As shown in Figure 2-13, 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 2-13 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 the 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 gigabitEthernet 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
```

2.6 MSTP

2.6.1 Introduction

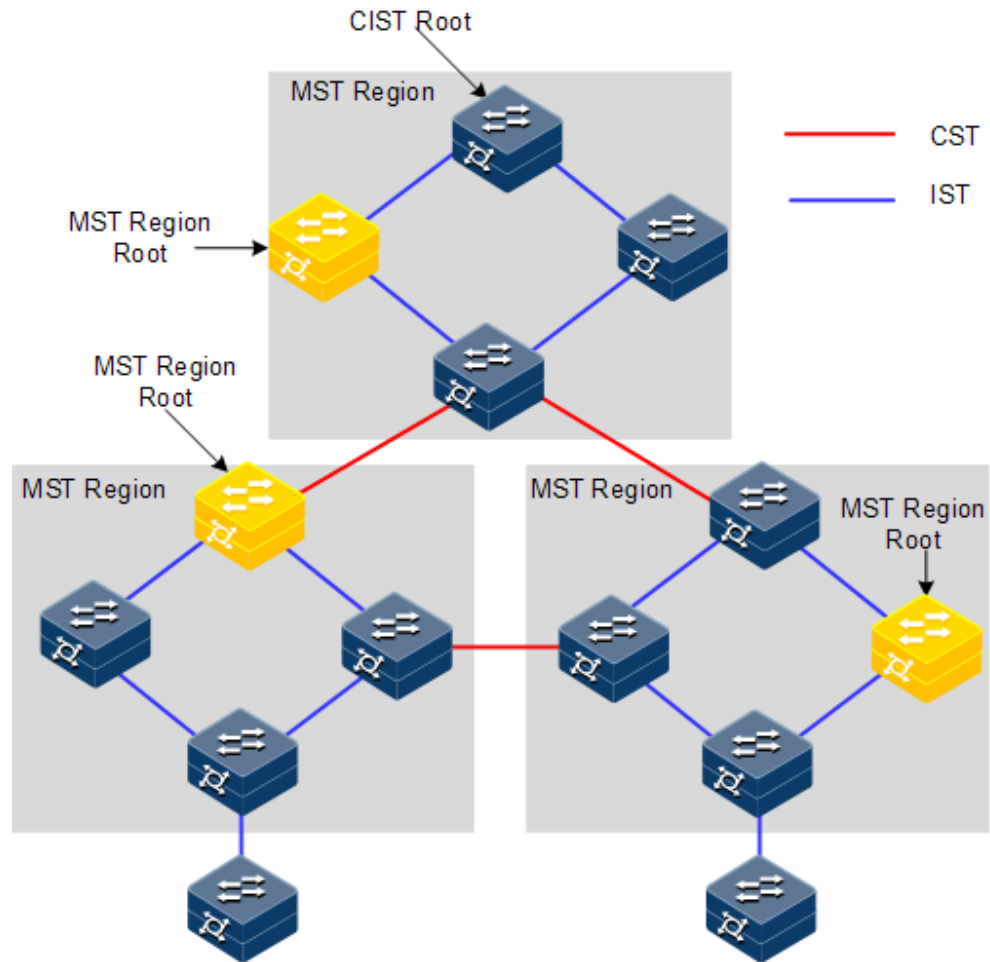
Multiple Spanning Tree Protocol (MSTP) is defined by IEEE 802.1s. Offsetting the disadvantages of STP and RSTP, the MSTP implements fast convergence and distributes traffic of different VLANs to follow its own path, thus providing an excellent load balancing mechanism.

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

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

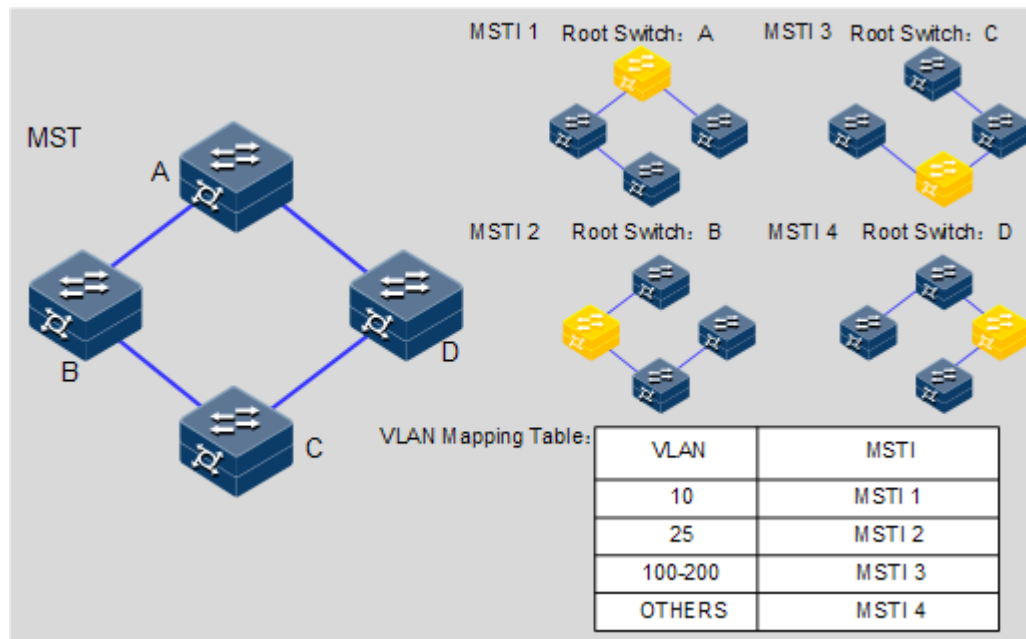
Compared with STP and RSTP, MSTP also introduces total root (CIST Root) and region root (MST Region Root) concepts. The total root is a global concept; all switches running STP/RSTP/MSTP can have only one total root, which is the CIST Root. The region root is a local concept, which is related to an instance in a region. As shown in Figure 2-14, all connected devices have only one total root, and the number of region roots contained in each region is associated with the number of instances.

Figure 2-14 Basic concepts of the MSTI network



There can be different MST instances in each MST region, which associates VLAN and MSTI by configuring the VLAN mapping table (relation table of VLAN and MSTI). The concept sketch map of MSTI is shown in Figure 2-15.

Figure 2-15 MSTI concepts

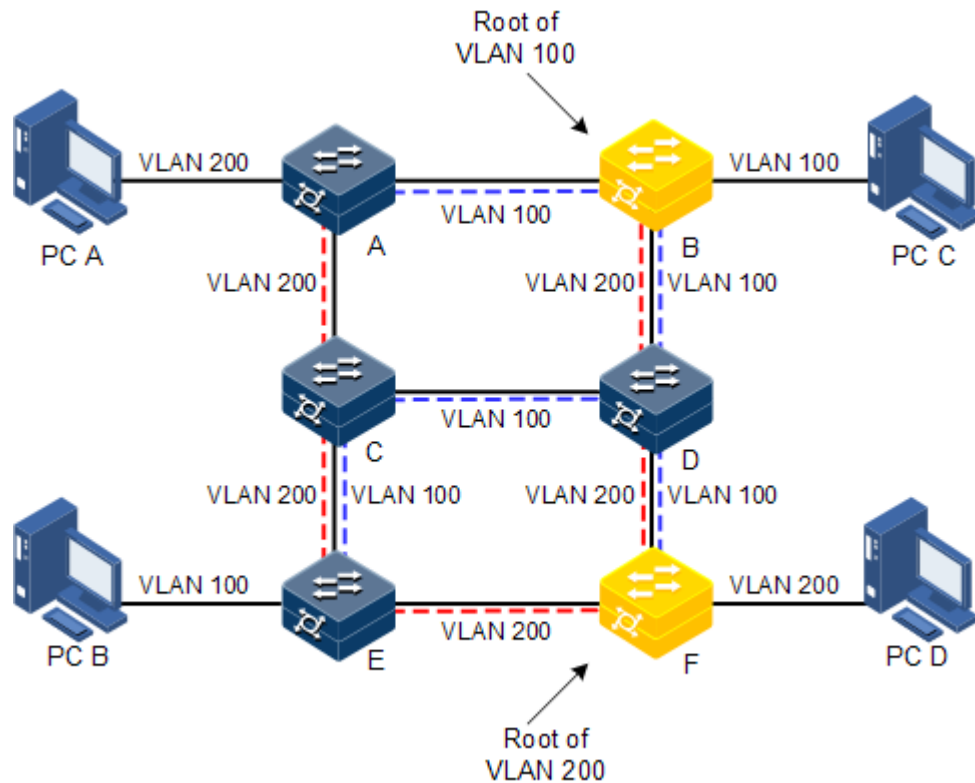


 **Note**

Each VLAN can be mapped into one MSTI; in other words, data of one VLAN can be transmitted in only 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 2-16 Networking with multiple spanning trees instances in MST region



Apply MSTP to the network as shown in Figure 2-16. After calculation, there are two spanning trees generated at last (two MST instances):

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

In this case, all VLANs can communicate internally, and packets of different VLANs are forwarded in different paths to balance load.

2.6.2 Preparing for configurations

Scenario

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

Prerequisite

N/A

2.6.3 Default configurations of MSTP

Default configurations of MSTP are as below.

Function	Default value
Global MSTP status	Disable
Interface MSTP status	Enable
Maximum numbers of hops in the MST region	20
Device MSTP priority	32768
Interface MSTP priority	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 MST region	0

2.6.4 Enabling MSTP

Enable MSTP for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#spanning-tree mode mstp</code>	Configure spanning tree for MSTP.
3	<code>Raisecom(config)#spanning-tree enable</code>	Enable global STP.
4	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
5	<code>Raisecom(config-gigaethernet1/1/port)#spanning-tree enable</code>	Enable interface STP.

2.6.5 Configuring MST region and its maximum number of hops

You can configure region information about the Gazelle S1512i-PWR when it is running in MSTP mode. The device MST region depends on 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 Gazelle S1512i-PWR 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 the MSTP region and its maximum number of hops for the Gazelle S1512i-PWR as below.

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

2.6.6 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 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, when 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 Gazelle S1512i-PWR as below.

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

Step	Command	Description
2	Raisecom(config)# spanning-tree [instance <i>instance-id</i>] root { primary secondary }	Configure the Gazelle S1512i-PWR as the root bridge or backup bridge of a STP instance.



Note

- You can confirm the effective instance of root bridge or backup bridge through the **instance** *instance-id* parameter. The current device will be assigned as 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 can be not only 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.

2.6.7 Configuring interface priority and system priority

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

The Bridge ID determines whether the Gazelle S1512i-PWR can be selected as the root of the spanning tree. Configuring smaller priority helps obtain smaller Bridge ID and designate the Gazelle S1512i-PWR as the root. If priorities of two Gazelle S1512i-PWR devices are identical, the Gazelle S1512i-PWR with lower MAC address will be selected 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/port)# spanning-tree [instance <i>instance-id</i>] priority <i>priority-value</i> Raisecom(config- gigaethernet1/1/port)# exit	Configure the interface priority for a STP instance.
4	Raisecom(config)# spanning-tree [instance <i>instance-id</i>] priority <i>priority-value</i>	Configure the system priority for a STP instance.



Note

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

2.6.8 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 in the whole network.

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

Similar to the maximum number of hops of MST region, only when the Gazelle S1512i-PWR 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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#spanning-tree bridge-diameter <i>bridge-diameter-value</i></code>	Configure the network diameter for the switching network.

2.6.9 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 the interface are mutually independent in different instances. You can configure internal path cost for instance through the **instance** *instance-id* parameter. Configure the internal path cost of the 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 Gazelle S1512i-PWR as below.

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

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

2.6.10 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 Gazelle S1512i-PWR as below.

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

2.6.11 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 Gazelle S1512i-PWR as below.

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

2.6.12 Configuring MSTP timer

- Hello Time: the Gazelle S1512i-PWR sends the interval of bridge configurations (BPDU) regularly to check whether there is failure in detection link of the Gazelle S1512i-PWR. The Gazelle S1512i-PWR 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 Gazelle S1512i-PWR 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 on 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# spanning-tree hello-time <i>value</i>	Configure Hello Time.
3	Raisecom(config)# spanning-tree forward-delay <i>value</i>	Configure Forward Delay.
4	Raisecom(config)# spanning-tree max-age <i>value</i>	Configure Max Age.

2.6.13 Configuring edge interface

The edge interface indicates the interface neither directly connected to any devices nor indirectly connected 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 Gazelle S1512i-PWR are configured in auto-detection attribute.

Configure the edge interface for the Gazelle S1512i-PWR as below.

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

2.6.14 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 Gazelle S1512i-PWR as below.

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

2.6.15 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.

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

Step	Command	Description
3	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
4	<code>Raisecom(config- gigaethernet1/1/port)#no spanning- tree bpduguard shutdown port</code>	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.

2.6.16 Configuring STP/RSTP/MSTP mode switching

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

- STP compatible mode: the Gazelle S1512i-PWR does not implement expedited 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 Gazelle S1512i-PWR implements expedited 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 Gazelle S1512i-PWR 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 Gazelle S1512i-PWR as below.

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

2.6.17 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 Gazelle S1512i-PWR 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.

2.6.18 Configuring root interface protection

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

Generally, the 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 Gazelle S1512i-PWR 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 rootguard enable</code>	Enable/Disable root interface protection.

2.6.19 Configuring interface loopguard

The spanning tree has two functions: loopguard and link backup. Loopguard requires trimming the network topology into tree structure. There must be redundant link 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. It regards the link as faulty if it has not received packets in a period. Then it selects a new link and enables backup interface. In

actual networking, the cause to failure in receiving packets may not link faults. In this case, enabling the backup interface may lead to a 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 Gazelle S1512i-PWR 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 loopguard enable</code>	Configure interface loopguard attributes.

2.6.20 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 Gazelle S1512i-PWR 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 tc-rejection { enable disable }</code>	Configure TC packet suppression.

2.6.21 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show spanning-tree</code>	Show basic configurations of STP.

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

2.6.22 Maintenance

Maintain the Gazelle S1512i-PWR as below.

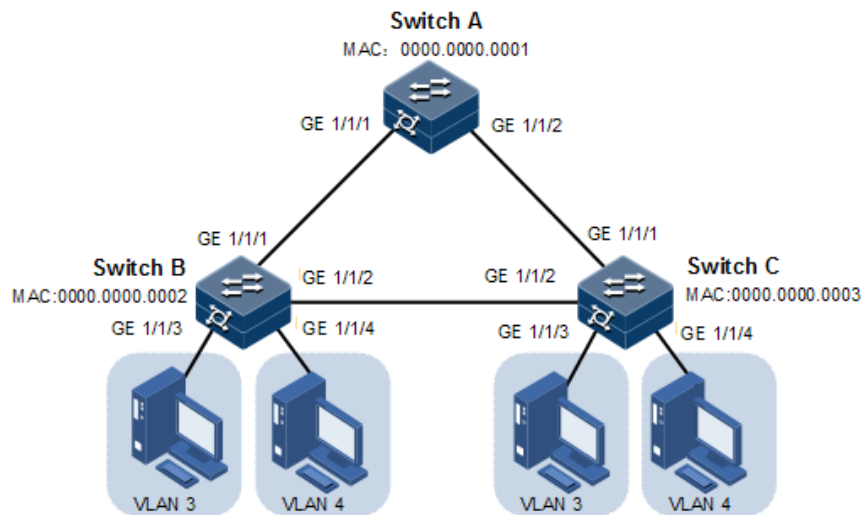
Command	Description
<code>Raisecom(config-gigaethernet1/1/port)#spanning-tree clear statistics</code>	Clear statistics on spanning tree on the interface.

2.6.23 Example for configuring MSTP

Networking requirements

As shown in Figure 2-17, three Gazelle S1512i-PWR 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 2-17 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 1/3/4 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 gig Ethernet 1/1/1
SwitchA(config-gig Ethernet1/1/1)#switchport mode trunk
SwitchA(config-gig Ethernet1/1/1)#exit
SwitchA(config)#interface gig Ethernet 1/1/2
SwitchA(config-gig Ethernet1/1/2)#switchport mode trunk
SwitchA(config-gig Ethernet1/1/2)#exit
```

Configure Switch B.

```
SwitchB(config)#interface gig Ethernet 1/1/1
SwitchB(config-gig Ethernet1/1/1)#switchport mode trunk
SwitchB(config-gig Ethernet1/1/1)#exit
SwitchB(config)#interface gig Ethernet 1/1/2
SwitchB(config-gig Ethernet1/1/2)#switchport mode trunk
SwitchB(config-gig Ethernet1/1/2)#exit
SwitchB(config)#interface gig Ethernet 1/1/3
SwitchB(config-gig Ethernet1/1/3)#switchport access vlan 3
SwitchB(config-gig Ethernet1/1/3)#exit
SwitchB(config)#interface gig Ethernet 1/1/4
SwitchB(config-gig Ethernet1/1/4)#switchport access vlan 4
SwitchB(config-gig Ethernet1/1/4)#exit
```

Configure Switch C.

```
SwitchC(config)#interface gig Ethernet 1/1/1
SwitchC(config-gig Ethernet1/1/1)#switchport mode trunk
SwitchC(config-gig Ethernet1/1/1)#exit
SwitchC(config)#interface gig Ethernet 1/1/2
SwitchC(config-gig Ethernet1/1/2)#switchport mode trunk
SwitchC(config-gig Ethernet1/1/2)#exit
SwitchC(config)#interface gig Ethernet 1/1/3
SwitchC(config-gig Ethernet1/1/3)#switchport access vlan 3
SwitchC(config-gig Ethernet1/1/3)#exit
SwitchC(config)#interface gig Ethernet 1/1/4
SwitchC(config-gig Ethernet1/1/4)#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, revised version to 0. Map instance 3 to VLAN 3, and instance 4 to VLAN 4. Exit 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 1/1/1 of spanning tree instance 3 to 500000 on Switch B.

```
SwitchB(config)#interface gigabitEthernet 1/1/1
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  Vlans Mapped  
-----  
0          1-2,5-4094  
3          3  
4          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  
-----
```

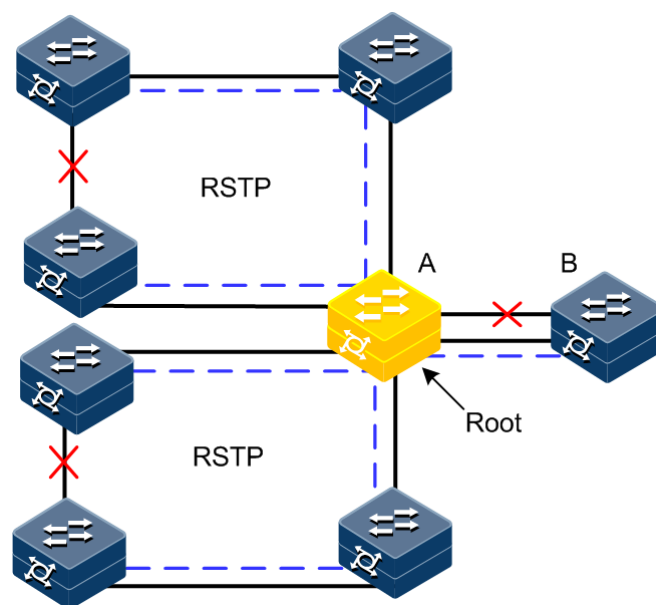
2.7 MRSTP

2.7.1 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 2-18, 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 2-18 Configuring MRSTP for specifying root bridge



2.7.2 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 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

2.7.3 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

2.7.4 Enabling MRSTP

Enable MRSTP for the Gazelle S1512i-PWR as below.

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

2.7.5 Configuring MRSTP parameters

Configure MRSTP parameters for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#spanning-tree mrstp pro-id priority priority	(Optional) configure the priority of the specified process.
3	Raisecom(config)#spanning-tree root {primary secondary}	(Optional) configure the device as the root device or secondary root device.

Step	Command	Description
4	Raisecom(config)# interface <i>interface-type interface-number</i> Raisecom(config- gigaethernet1/1/port)# spanning- tree priority <i>priority-value</i>	(Optional) configure the priority of the interface.
5	Raisecom(config)# spanning-tree hello-time <i>value</i>	(Optional) configure the Hello timer.
6	Raisecom(config)# spanning-tree transit-limit <i>value</i>	(Optional) configure the maximum transmission rate of the interface.
7	Raisecom(config)# spanning-tree forward-delay <i>value</i>	(Optional) configure the Forward Delay.
8	Raisecom(config)# spanning-tree max-age <i>value</i>	(Optional) configure the Max Age.

2.7.6 Checking configurations

Use the following commands to check configuration results.

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

2.8 Loop detection

2.8.1 Introduction

Loop detection can eliminate the influence on network caused by a loop, thus 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

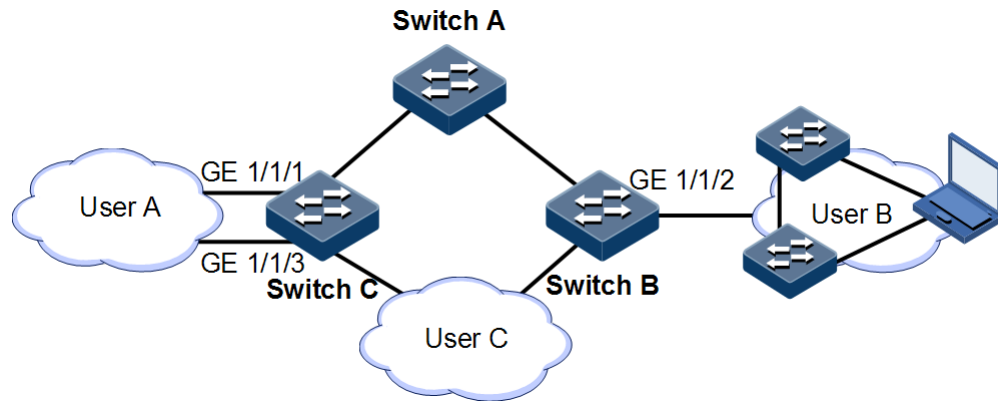
Common loop types include self-loop and inner loop.

As shown in Figure 2-19, 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 is a 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 form an inner loop with the user network A.

Figure 2-19 Loop detection networking



Principles of processing loops

The Gazelle S1512i-PWR 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 larger 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 2-19, assume that loop detection is enabled on Switch B and Switch C interfaces which connect user networks. The loop detection processing mechanism for the three loop types is 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 packet 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 Gazelle S1512i-PWR 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 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, namely, the automatic restoration time is infinite; it will not be automatically restored.

2.8.2 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. When 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.

2.8.3 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	5s
Mode for processing detected loops	block
Loop detection period	1s
Loop detection mode	VLAN

2.8.4 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 two directly-connected devices.

Configure loop detection based on interface+VLAN for the Gazelle S1512i-PWR as below.

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

Step	Command	Description
3	<pre>Raisecom(config- gigaethernet1/1/port)#loopback- detection [pkt-vlan { untag vlan-id }] [hello-time <i>second</i>] [restore-time <i>second</i>] [action { block trap-only shutdown }] [log-interval <i>log- interval</i> <i>time</i>] Raisecom(config- gigaethernet1/1/port)#loopback- detection detect-vlanlist <i>vlanlist</i> [hello-time <i>second</i>] [restore-time <i>second</i>] [action { block trap-only shutdown }] [log-interval <i>log- interval</i> <i>time</i>]</pre>	<p>Enable loop detection on the interface.</p> <p>Configure the VLAN for sending loop detection packets.</p> <p>(Optional) configure the period for sending Hello packets.</p> <p>(Optional) configure the time for automatically restoring the blocked interface due to loop detection and the action for processing loops.</p>
4	<pre>Raisecom(config- gigaethernet1/1/port)#loopback- detection manual restore</pre>	<p>Manually restore the interface blocked due to loop detection.</p>

2.8.5 Checking configurations

Use the following commands to check configuration results.

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

2.8.6 Maintenance

Use the following commands to maintain the Gazelle S1512i-PWR.

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

2.8.7 Example for configuring inner loop detection

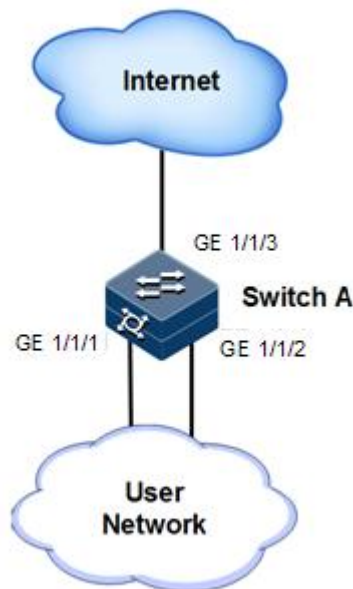
Networking requirements

As shown in Figure 2-20, 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, 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 of GE 1/1/2 to block, namely, sending Trap and blocking the interface.

Figure 2-20 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 gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport access vlan 3
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport access vlan 3
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 2 Configure the VLAN for sending loop detection packets, and interval for sending loop detection packets.

```
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#loopback-detection pkt-vlan 3 hello-time 3 action block
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
```

```
Raisecom(config-gigaetherne1/1/2)#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, 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 -- -- -- -- --
```

2.9 Interface protection

2.9.1 Introduction

With interface protection, you can add an interface, which needs to be controlled, to an interface protection group, isolating Layer 2 or 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.

2.9.2 Preparing for configurations

Scenario

Interface protection can mutually isolate interfaces in the same VLAN, enhance network security, and provide flexible networking solutions for you.

Prerequisite

N/A

2.9.3 Default configurations of interface protection

Default configurations of interface protection are as below.

Function	Default value
Interface protection status of each interface	Disable

2.9.4 Configuring interface protection



Caution

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

Configure interface protection for the Gazelle S1512i-PWR 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)#switchport protect</code>	Enable interface protection.

2.9.5 Checking configurations

Use the following commands to check configuration results.

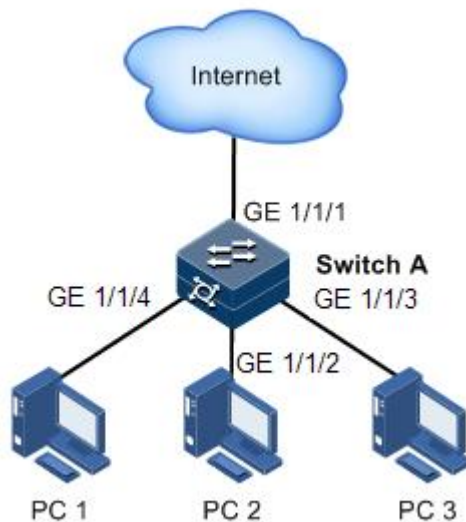
No.	Command	Description
1	<code>Raisecom#show switchport protect</code>	Show configurations of interface protection.

2.9.6 Example for configuring interface protection

Networking requirements

As shown in Figure 2-21, 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 2-21 Interface protection networking



Configuration steps

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

```
Raisecom#config  
Raisecom(config)#interface gigaethernet 1/1/1  
Raisecom(config-gigaethernet1/1/1)#switchport protect  
Raisecom(config-gigaethernet1/1/1)#exit
```

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

```
Raisecom(config)#interface gigaethernet 1/1/2  
Raisecom(config-gigaethernet1/1/2)#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.

2.10 Port mirroring

2.10.1 Introduction

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

Figure 2-22 Principles of port mirroring

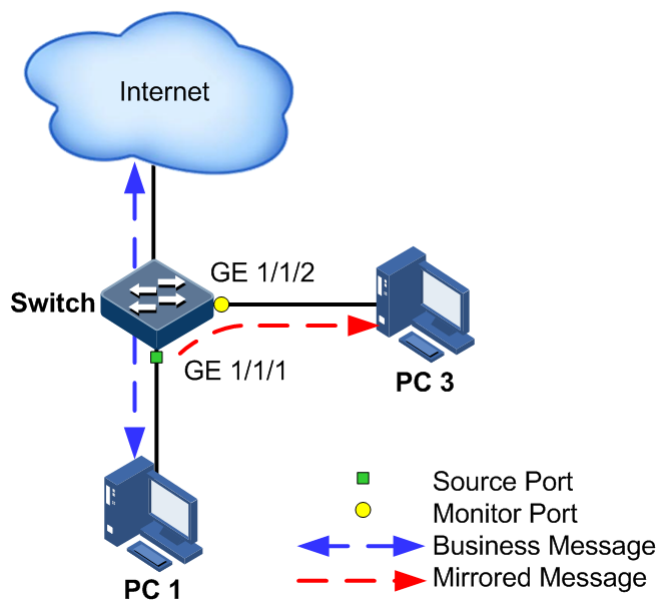


Figure 2-22 shows basic principles of port mirroring. PC 1 is connected to the external network through the GE 1/1/1. PC 3 is the monitor PC, connected to the external network through GE 1/1/2.

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 1/1/1 as the monitor port to mirror packets to the destination port.

When service packets from PC 1 enter the Gazelle S1512i-PWR, the Gazelle S1512i-PWR will forward and copy them to the monitor port (GE 1/1/2). The monitor device connected to the monitor port can receive and analyze these mirrored packets.

The Gazelle S1512i-PWR supports traffic mirroring on the ingress port and egress port. The packets on the ingress or 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.

2.10.2 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

2.10.3 Default configurations of port mirroring

Default configurations of port mirroring are as below.

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

2.10.4 Configuring port mirroring

Configure port mirroring for the Gazelle S1512i-PWR as below.

Step	Configure	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mirror remote-vlan <i>remote-vlan-id</i></code>	Configure the remote mirroring VLAN for the mirroring group.
3	<code>Raisecom(config)#mirror-group <i>group-id</i></code>	Create a port mirroring group.
4	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical interface configuration mode.
5	<code>Raisecom(config- gigaethernet1/1/port)#mirror-group <i>group-id</i> monitor-port</code>	Configure the monitor port for mirroring.

Step	Configure	Description
6	<pre>Raisecom(config- gigaethernet1/1/port)#mirror-group group-id source-port [ingress egress]</pre>	Configure the mirroring port of port mirroring, and specify the mirroring rule for port mirroring. Port mirroring supports mirroring packets in both the ingress and egress directions of the port.
7	<pre>Raisecom(config- gigaethernet1/1/port)#exit Raisecom(config)#mirror-group group- id source-cpu [ingress egress]</pre>	Configure port mirroring to mirror packets to or from the CPU.

2.10.5 Checking configurations

Use the following commands to check configuration results.

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

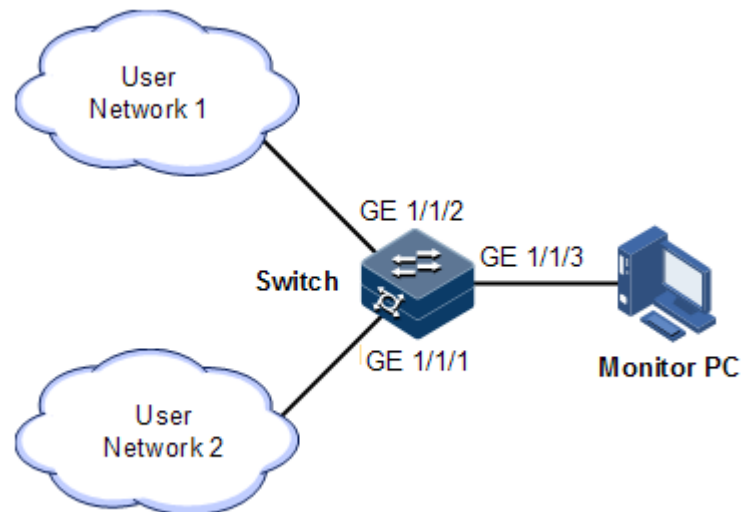
2.10.6 Example for configuring port mirroring

Networking requirements

As shown in Figure 2-23, the network administrator wants to monitor user network 1 through the monitor device, to catch the fault or abnormal data flow for analyzing and discovering faults, and to solve them in time.

The Gazelle S1512i-PWR is disabled with storm control and automatic packet sending. User network 1 accesses the Gazelle S1512i-PWR through GE 1/1/1, user network 2 accesses the Gazelle S1512i-PWR through GE 1/1/2, and the data monitor device is connected to GE 1/1/3.

Figure 2-23 Port mirroring networking



Configuration steps

Enable port mirroring on the Switch.

```
Raisecom#config
Raisecom(config)#mirror-group 1
Raisecom(config)interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#mirror-group 1 monitor-port
Raisecom(config-gigaethernet1/1/3)#exit
Raisecom(config)interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#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 :
    gigaethernet1/1/3
Source Port :
    gigaethernet1/1/1      : ingress
    gigaethernet1/1/2      : ingress
Remote Vlan: --
```


2.11 L2CP

2.11.1 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 Gazelle S1512i-PWR, 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.

2.11.2 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

2.11.3 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	0X010E-5E00-0003
Description of the L2CP profile	N/A

2.11.4 Configuring global L2CP

Configure global L2CP for the Gazelle S1512i-PWR as below.

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

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

2.11.5 Configuring L2CP profile

Configure the L2CP profile for the Gazelle S1512i-PWR as below.

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

2.11.6 Configuring L2CP profile on interface

Configure the L2CP profile on the interface for the Gazelle S1512i-PWR 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 interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/port)#l2cp profile profile-number</code>	Apply the L2CP profile on the interface.

2.11.7 Checking configurations

Use the following commands check configuration results.

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

2.11.8 Maintenance

Maintain the Gazelle S1512i-PWR as below.

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

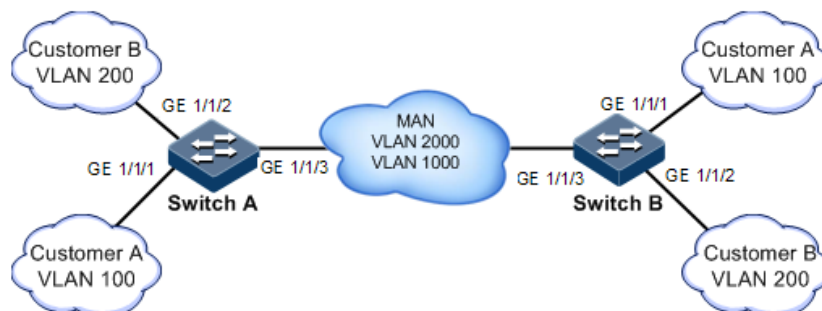
2.11.9 Example for configuring L2CP

Networking requirements

As shown in Figure 2-24, 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 2-24 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 gig Ethernet 1/1/1
Raisecom(config-gig Ethernet1/1/1)#l2cp-process profile 1
Raisecom(config-gig Ethernet1/1/1)#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 Customer B
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 fast Ethernet 1/1/2
Raisecom(config-fast Ethernet1/1/2)#l2cp-process profile 2
Raisecom(config-fast Ethernet1/1/2)#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	--	--	--	--

3 PoE

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

- Introduction
- Configuring PoE
- Example for configuring PoE power supply

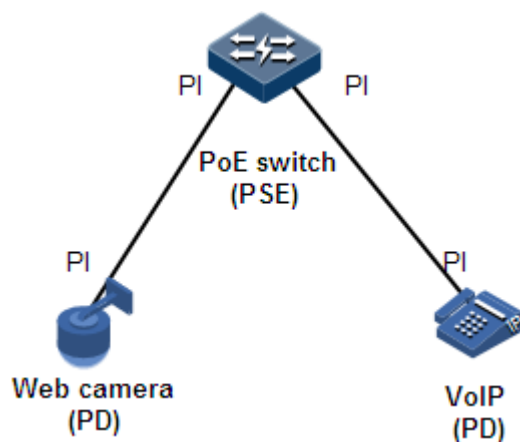
3.1 Introduction

3.1.1 Principles of PoE

Power over Ethernet (PoE) means that the Power Sourcing Equipment (PSE) both supplies power and transmits data to the remote Power Device (PD) through the Ethernet cable and Power Interface (PI).

Figure 3-1 shows principles of PoE.

Figure 3-1 Principles of PoE



3.1.2 PoE modules

The PoE system consists of the following modules:

- PSE: consist of the power module and PSE functional module. The PSE can detect PDs, obtain PD power information, remotely supply power, monitor power supply, and power off PDs.
- PD: supplied with power by the PSE. There are standard PDs and non-standard PDs. Standard PDs must comply with IEEE 802.3af or IEEE 802.3at, such as the IP phone and web camera.
- PI: the interface connecting the PSE/PD to the Ethernet cable, namely, the RJ45 interface

3.1.3 PoE advantages

PoE has the following advantages:

- Reliability: a centralized PSE supplies power with convenient backup, uniform management of power modules, and high security.
- Convenient connection: the network terminal does not need an external power supply; instead, it needs only one Ethernet cable connected to the PoE interface.
- Standardization: PoE complies with IEEE 802.3at and uses globally uniform power interface.
- Wide applications: applicable to IP phones, wireless Access Point (AP), portable device charger, credit card reader, web camera, and data collection system.

3.1.4 PoE concepts

- Maximum output power of PoE

It is the maximum output power output by the interface to the connected PD.

- Priority of PoE

There are three levels of priorities for power supply: critical, high, and low. The PSE supplies power to the PD connected to the PI with critical priority preferentially, the PD connected to the PI with the high priority, and finally the PD connected to the PI with the low priority.

- Overtemperature protection

When the current temperature exceeds the overtemperature threshold, overtemperature alarms occur and the system sends Trap to the Network Management System (NMS).

- Global Trap

When the current temperature exceeds the overtemperature threshold, the current PSE power utilization rate exceeds the threshold, or the status of PoE changes, the Gazelle S1512i-PWR sends Trap to the NMS.

- PSE power utilization rate threshold

When the PSE power utilization rate exceeds the threshold for the first time, the system sends Trap.

3.2 Configuring PoE

3.2.1 Preparing for configurations

Scenario

When the remotely connected PE is inconvenient to take power, it needs to take power from the Ethernet electrical interface to concurrently transmit power and data.

Prerequisite

N/A

3.2.2 Default configurations of PoE

Default configurations of PoE are as below.

Function	Default value
PI PoE status	Enable
Non-standard PD identification	Enable
Maximum output power of PoE	30000 mW
Power supply management mode	Auto
PoE priority	Low
Overtemperature protection status	Enable
Power supply global Trap switch status	Enable
PSE power utilization rate threshold	99%

3.2.3 Enabling interface PoE

Enable interface PoE for the Gazelle S1512i-PWR as below:

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#poe enable</code>	Enable interface PoE.

3.2.4 Configuring maximum output power of PoE

Configure the maximum output power of PoE for the Gazelle S1512i-PWR as below:

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#poe max-power <i>max-power-value</i>	Configure the maximum output power of PoE.

3.2.5 Configuring priority of PoE

Configure the priority of PoE for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#poe priority { critical high low }	Configure the priority of PoE.

3.2.6 Configuring PSE power utilization rate threshold

Configure the PSE power utilization rate threshold for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#poe pse power- threshold <i>percent</i>	Configure the PSE power utilization rate threshold.

3.2.7 Configuring identification of non-standard PDs



Caution

To use other non-standard PD, confirm its power consumption, voltage, and current in advance to properly configure the maximum output power on the PSE and to avoid damaging the PD due to too high output power.

Configure identification of non-standard PDs for the Gazelle S1512i-PWR as below.

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

Step	Command	Description
2	<code>Raisecom(config)#poel legacy enable</code>	Enable the PSE to identify non-standard PDs.

3.2.8 Enabling forcible power supply on interface



Caution

When using the Gazelle S1512i-PWR to supply power for a remote PD, we recommend using a standard PD, pre-standard PD, or Cisco-primate standard PD. To use other non-standard PD in forcible power supply mode, confirm its power consumption, voltage, and current in advance to properly set the maximum output power on the PSE and to avoid damaging the PD due to too high output power.

Enable forcible power supply on interfaces for the Gazelle S1512i-PWR 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)#poeforce-power</code>	Enable forcible PoE power supply on the interface.

3.2.9 Enabling overtemperature protection

Enable overtemperature protection for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#poetemperature- protection enable</code>	Enable overtemperature protection.

3.2.10 Enabling global Trap

Enable global Trap for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#poepse trap enable</code>	Enable global Trap.

3.2.11 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show poe interface- type interface-number [detail]	Show power supply status on specified interfaces.
2	Raisecom# show poe pse [detail]	Show PSE configurations and realtime operating information.

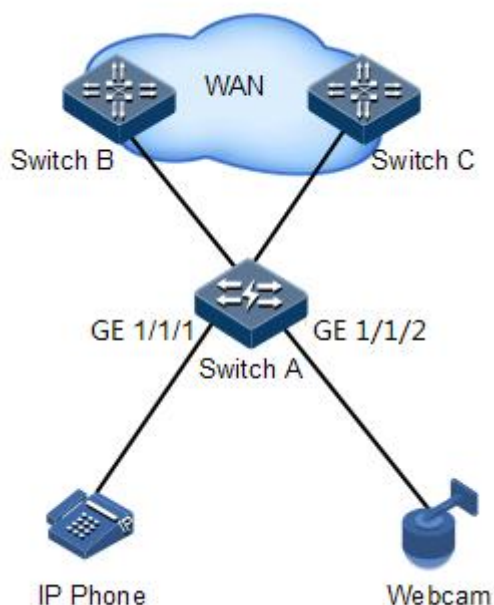
3.3 Example for configuring PoE power supply

Networking requirements

As shown in Figure 3-2, both Switch B and Switch C connect Switch A to the WAN, and PoE-supportive Switch A is used to supply power to an IP phone and a monitor camera. Switch A is required to supply power to the monitor camera preferentially when it runs at full load. Detailed requirements are as below:

- Configure the maximum output power of GE 1/1/1 and GE 1/1/2 to 30000 mW.
- Enable overtemperature protection on Switch A.
- Enable Trap for power supply on Switch A.
- Configure the priorities of GE 1/1/2 and GE 1/1/1 to high and low respectively.

Figure 3-2 PoE switch power supply networking



Configuration steps

Step 1 Enable PoE on GE 1/1/1 and GE 1/1/2.

```
Raisecom#config  
Raisecom(config)#interface gig Ethernet 1/1/1  
Raisecom(config-gig Ethernet1/1/1)#poe enable  
Raisecom(config-gig Ethernet1/1/1)#exit  
Raisecom(config)#interface gig Ethernet 1/1/2  
Raisecom(config-gig Ethernet1/1/2)#poe enable  
Raisecom(config-gig Ethernet1/1/2)#exit
```

Step 2 Configure the maximum output power of GE 1/1/1 and GE 1/1/2 to 30000 mW.

```
Raisecom(config)#interface gig Ethernet 1/1/1  
Raisecom(config-gig Ethernet1/1/1)#poe max-power 30000  
Raisecom(config-gig Ethernet1/1/1)#exit  
Raisecom(config)#interface gig Ethernet 1/1/2  
Raisecom(config-gig Ethernet1/1/2)#poe max-power 30000  
Raisecom(config-gig Ethernet1/1/2)#exit
```

Step 3 Enable overtemperature protection.

```
Raisecom(config)#poe temperature-protection enable
```

Step 4 Enable global Trap.

```
Raisecom(config)#poe pse trap enable
```

Step 5 Configure priorities of GE 1/1/2 and GE 1/1/1 to high and low respectively.

```
Raisecom(config)#interface gig Ethernet 1/1/2  
Raisecom(config-gig Ethernet1/1/2)#poe priority high  
Raisecom(config-gig Ethernet1/1/2)#exit  
Raisecom(config)#interface gig Ethernet 1/1/1  
Raisecom(config-gig Ethernet1/1/1)#poe priority low
```

Checking results

Use the **show poe gig Ethernet 1/1/1 detail** and **show poe gig Ethernet 1/1/2 detail** commands to show PoE configurations on GE 1/1/2 and GE 1/1/1.

```
Raisecom#show poe gigabitEthernet 1/1/1 detail
```

```
Port: gigabitEthernet 1/1/1
```

```
-----  
POE administrator status: Enable  
POE operation status: Enable  
Power detection status:Searching  
POE Power Pairs mode:Signal  
PD power classification:Class0  
POE power Priority:Low  
POE power max:30000 (mw)  
POE power output:0 (mw)  
POE power average:0 (mw)  
POE power peak:0 (mw)  
POE current output:0 (mA)  
POE voltage output:0 (V)
```

```
Raisecom#show poe gigabitEthernet 1/1/2 detail
```

```
Port: gigabitEthernet 1/1/1
```

```
-----  
POE administrator status: Enable  
POE operation status: Enable  
Power detection status:Searching  
POE Power Pairs mode:Signal  
PD power classification:Class0  
POE power Priority:High  
POE power max:30000 (mw)  
POE power output:0 (mw)  
POE power average:0 (mw)  
POE power peak:0 (mw)  
POE current output:0 (mA)  
POE voltage output:0 (V)
```

4 Ring network protection

This chapter describes principles and configuration procedures of ring network protection, including the following section:

- G.8032

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 the 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 Gazelle S1512i-PWR supports the single ring, intersecting ring, and tangent ring.

G.8032 provides a mode for detecting faults based on physical interface status. The Gazelle S1512i-PWR 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	5min
Ring protocol version	2
Guard timer	500ms
Ring Hold-off timer	0ms
ERPS 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 the G.8032 ring for the Gazelle S1512i-PWR as below.




Caution

- Only one device on the protection ring can be configured as the Ring Protection Link (RPL) Owner and only one device is configured as the RPL Neighbor. Other devices are configured as ring forwarding nodes.
- The tangent ring consists of 2 independent single rings. Configurations of the tangent ring are identical to those of the common single ring. The intersecting ring consists of a main ring and a tributary ring. Configurations of the main ring are identical to those of the common single ring. For detailed configurations of the tributary ring, see section 4.1.5 (Optional) creating G.8032 tributary ring.

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

Step	Command	Description
2	<pre>Raisecom(config)#ethernet ring-protection <i>ring-id</i> east { <i>interface-type</i> <i>interface-</i> <i>number</i> port-channel <i>port-</i> <i>channel-number</i> } west { <i>interface-type</i> <i>interface-</i> <i>number</i> port-channel <i>port-</i> <i>channel-number</i> } [node-type rpl-owner rpl { east west }] [not-revertive] [protocol-vlan <i>vlan-id</i>] [block-vlanlist <i>vlan-list</i>]</pre>	<p>Create a protection ring and configure the node as the RPL Owner.</p>  <p>Note The eastbound and westbound interfaces cannot be the same one.</p>
	<pre>Raisecom(config)#ethernet ring-protection <i>ring-id</i> east { <i>interface-type</i> <i>interface-</i> <i>number</i> port-channel <i>port-</i> <i>channel-number</i> } west { <i>interface-type</i> <i>interface-</i> <i>number</i> port-channel <i>port-</i> <i>channel-number</i> } node-type rpl-neighbour rpl { east west } [not-revertive] [protocol-vlan <i>vlan-id</i>] [block-vlanlist <i>vlan-list</i>]</pre>	<p>Create a protection ring, and configure the node as the RPL Neighbour.</p>
	<pre>Raisecom(config)#ethernet ring-protection <i>ring-id</i> east { <i>interface-type</i> <i>interface-</i> <i>number</i> port-channel <i>port-</i> <i>channel-number</i> } west { <i>interface-type</i> <i>interface-</i> <i>number</i> port-channel <i>port-</i> <i>channel-number</i> } [not- revertive] [protocol-vlan <i>vlan-id</i>] [block-vlanlist <i>vlan-list</i>]</pre>	<p>Create a protection line, and configure the node as the protection forwarding node.</p>
3	<pre>Raisecom(config)#ethernet ring-protection <i>ring-id</i> name <i>string</i></pre>	<p>(Optional) configure the name of the protection ring. Up to 32 bytes are available.</p>
4	<pre>Raisecom(config)#ethernet ring-protection <i>ring-id</i> version { 1 2 }</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	<code>Raisecom(config)#ethernet ring-protection ring-id guard-time guard-time</code>	(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 neighboring 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	<code>Raisecom(config)#ethernet ring-protection ring-id wtr-time wtr-time</code>	(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	<code>Raisecom(config)#ethernet ring-protection ring-id holdeoff-time holdeoff-time</code>	(Optional) configure the ring Hold-off timer. After the Hold-off timer is configured, the system will delay processing the fault when the working line fails. In other words traffic is delayed to be switched to the protection line. This helps prevent frequent switching caused by working line vibration.  Note If the ring Hold-off timer value is too great, it may influence 50ms switching performance. Therefore, we recommend configuring the ring Hold-off timer value to 0.


4.1.5 (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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>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]</code>	<p>Create a 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"> • In revertive mode, when the working line recovers from a fault, traffic is switched from the protection line to the working line. • In non-revertive mode, when the working line recovers from a fault, traffic is not switched from the protection line to the working line. <p>By default, the protection ring is in revertive mode.</p> <p> Note</p> <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>
	<code>Raisecom(config)#ethernet ring-protection ring-id { east west } { interface-type interface-number port- channel port-channel- number } node-type rpl- neighbour [not- revertive] [protocol- vlan vlan-id] [block- vlanlist vlan-list]</code>	Create a tributary ring on the intersecting node, and configure the intersecting node as the RPL Neighbour.
	<code>Raisecom(config)#ethernet ring-protection ring-id { east west } { interface-type interface-number port- channel port-channel- number } [not- revertive] [protocol- vlan vlan-id] [block- vlanlist vlan-list]</code>	Create a tributary ring on the intersecting node, and configure the intersecting node as the protection forwarding node.

Step	Command	Description
3	<code>Raisecom(config)#ethernet ring-protection ring-id raps-vc { with without }</code>	<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"> • 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. • 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). <p>By default, the virtual channel of the tributary ring adopts the with mode. Transmission modes on 2 intersecting nodes must be identical.</p>
4	<code>Raisecom(config)#ethernet ring-protection ring-id propagate enable</code>	<p>Enable the ring Propagate switch on the intersecting node.</p> <p>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.</p>

4.1.6 (Optional) configuring G.8032 switching control

Configure G.8032 switching control for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ethernet ring-protection ring-id force-switch { east west }</code>	<p>Switch the traffic on the protection ring to the west/east interface forcedly.</p> <p>FS can be configured on multiple interfaces of multiple ring nodes.</p>

Step	Command	Description
3	Raisecom(config)#ethernet ring-protection ring-id manual-switch { east west }	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	Raisecom(config)#clear ethernet ring-protection ring-id { command statistics }	Clear switching control commands, including force-switch , manual-switch , 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.

4.1.7 Configuring ERPS fault detection mode

Configure the ERPS fault detection mode for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ethernet ring-protection ring-number { east west} failure-detect physical-link	Configure the fault detection mode to physical link.

4.1.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show ethernet ring-protection	Show configurations of the G.8032 ring.
2	Raisecom#show ethernet ring-protection status	Show G.8032 ring status.
3	Raisecom#show ethernet ring-protection statistics	Show G.8032 ring statistics.

4.1.9 Maintenance

Maintain the Gazelle S1512i-PWR as below.

Command	Description
Raisecom(config)#clear ethernet ring-protection ring-id statistics	Clear statistics on the protection ring.

5 IP services

This chapter describes principles and configuration procedures of IP services, and provides related configuration examples, including the following sections:

- IP basis
- Loopback interface
- ARP
- NDP

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 Gazelle S1512i-PWR 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.

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
IP address of VLAN interface 1	192.168.0.1

5.1.4 Configuring IPv4 address of VLAN interface

Configure the IPv4 address of the VLAN interface for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#ip address <i>ip-address</i> [<i>ip-mask</i>] [<i>sub</i>]	Configure the IP address of the VLAN interface. Use the no ip address <i>ip-address</i> 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter Layer 3 interface configuration mode.
3	Raisecom(config-vlan1)#ipv6 address <i>ipv6-address/prefix-length</i>	Configure the IPv6 address of the VLAN interface.

5.1.6 Checking configurations

Use the following commands to check configuration results.

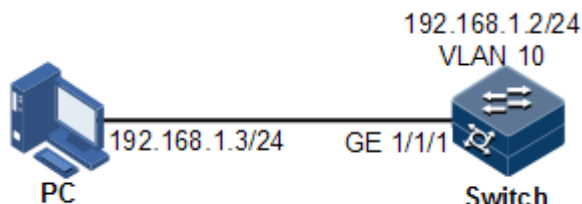
No.	Command	Description
1	Raisecom#show ip interface brief	Show configurations of the IP address of the VLAN interface.
2	Raisecom#show ipv6 interface brief	Show configurations of the IPv6 address of the VLAN interface.

5.1.7 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 Gazelle S1512i-PWR can ping each other.

Figure 5-1 VLAN interface networking



Configuration steps

Step 1 Create VLAN 10 and add GE 1/1/1 to VLAN 10.

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

Step 2 Create a Layer 3 interface on the Gazelle S1512i-PWR, configure its IP address, and associate it with VLAN 10.

```
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 Category	IF	Address	NetMask
Default-IP-Routing-Table	vlan10	192.168.1.2	
255.255.255.0	primary		

Use the **ping** command to check whether the Gazelle S1512i-PWR 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 Gazelle S1512i-PWR 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. 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface loopback <i>lb-number</i>	Enter loopback interface configuration mode.
3	Raisecom(config-loopback)#ip address <i>ip-address</i> [<i>ip-mask</i>]	Configure the IP address of the loopback interface.
4	Raisecom(config-loopback)#ipv6 address <i>ipv6-address/prefix-length</i>	Configure the IPv6 address of the loopback interface.

5.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show interface loopback	Show configurations of the loopback interface.

5.3 ARP

5.3.1 Introduction

In the 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 translate the 32-bit IP address of the destination host to the 48-bit Ethernet address for transmitting packets to the destination host correctly. Then Address Resolution Protocol (ARP) is applied to resolve the IP address to the MAC address and configures mapping between IP addresses and MAC addresses.

The ARP address table contains the following two types of entries:

- Static entry: bind an IP address and a MAC address to avoid ARP dynamic learning cheating.
 - The static ARP address entry needs to be added or deleted manually.
 - The static ARP address entry is not aged.
- Dynamic entry: the MAC address is automatically learned through ARP.
 - This dynamic entry is automatically generated by the switch. You can adjust some parameters of it manually.
 - The dynamic ARP address entry is aged after the aging time expires if it is not used.

The Gazelle S1512i-PWR supports the following two modes of dynamically learning ARP address entries:

- Learn-all: in this mode, the Gazelle S1512i-PWR learns both ARP request packets and response packets. When device A sends its ARP request, it writes the mapping between its IP address and physical address in the ARP request packet. When device B receives the ARP request packet from device A, it learns the mapping in its address table. In this way, device B will no longer send an ARP request when sending packets to device A.
- learn-reply-only mode: in this mode, the Gazelle S1512i-PWR learns ARP response packets corresponding to ARP request packets sent by itself only. For ARP request packets from other devices, it responds with ARP response packets only rather than learning ARP address mapping entry. In this way, the 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 the IP address and MAC address is saved in the ARP address table.

Generally, the ARP address table is dynamically maintained by the Gazelle S1512i-PWR. The Gazelle S1512i-PWR searches for the mapping between an IP address and MAC address automatically according to ARP. You just need to configure the Gazelle S1512i-PWR manually for preventing ARP dynamic learning 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
Gratuitous ARP packet learning on the interface	Enable

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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#arp ip-address mac-address</code>	Configure static ARP entry.

5.3.5 Configuring dynamic ARP entries

Configure dynamic ARP entries for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#arp mode { learn-all learn-reply-only }</code>	Configure the aging time of dynamic ARP entries.
3	<code>Raisecom(config)#arp aging-time time</code>	Enter Layer 3 interface configuration mode.
4	<code>Raisecom(config)#arp max-learning-num number</code>	(Optional) configure the maximum number of dynamic ARP entries allowed to learn on the Layer 3 interface.

5.3.6 Configuring gratuitous ARP packet learning

Configure gratuitous ARP packet learning for the Gazelle S1512i-PWR 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.
3	<code>Raisecom(config gigaethernet1/1/1)#gratuitous-arp-learning{ enable disable }</code>	Configure gratuitous ARP packet learning. By default, it is enabled.

5.3.7 Configuring local proxy ARP

Configure local proxy ARP for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#arp local-proxy { enable disable }	Enable local proxy ARP. By default, it is disabled.

5.3.8 Configuring ARP anti-attack

Configure ARP anti-attack for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-list</i>	Enter Layer 3 interface configuration mode.
3	Raisecom(config-vlan1)# arp anti- attack entry-check { fixed-all fixed-mac send-ack }	Configure the detection mode for ARP anti-attack.
4	Raisecom(config-vlan1)#arp check- destination-ip {enable disable}	Configure source IP address detection for ARP anti-attack.
5	Raisecom(config-vlan1)#arp filter{ gratuitous mac-illegal tha-filled-request }	Configure the ARP filter.

5.3.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show arp [<i>ip-address</i> interface <i>interface-type</i> <i>interface-number</i> static]	Show information about entries in the ARP address table.
2	Raisecom#show arp local-proxy [interface vlan <i>vlan-id</i>]	Show information about local proxy ARP.

5.3.10 Maintenance

Maintain the Gazelle S1512i-PWR as below.

Command	Description
raisecom(config)#clear arp	Clear all entries in the ARP address table.

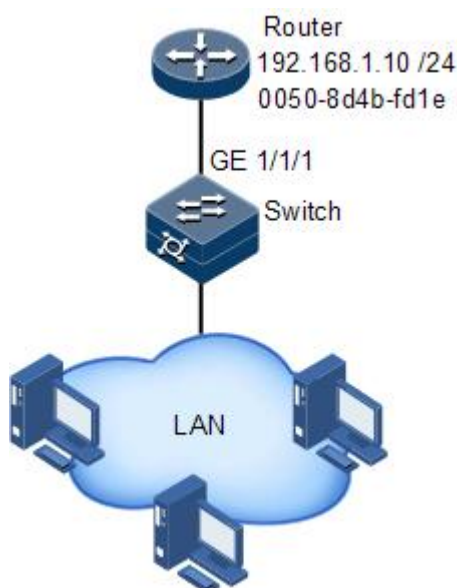
5.3.11 Example for configuring ARP

Networking requirements

As shown in Figure 5-2, the Gazelle S1512i-PWR is connected to the host, and is also connected to the upstream Router through GE 1/1/1. For the Router, the IP address is 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 Gazelle S1512i-PWR.

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
IP Address      Mac Address      Interface      Type
Age(s)      status
-----
192.168.1.10    0050.8D4B.FD1E   vlan10         static  --
PERMANENT
    
```

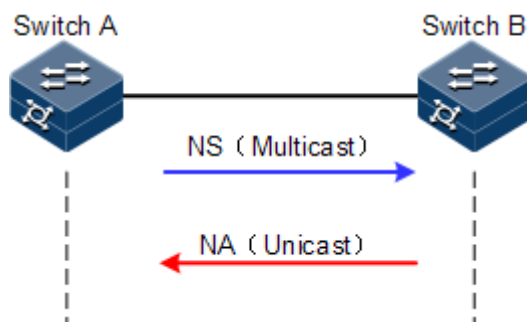
5.4 NDP

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.
- 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	256

5.4.4 Configuring static neighbor entries

To resolve the IPv6 address of a neighbor into the data link layer address, you can use the NS message and NA message, or manually configure static neighbor entries.

Configure static neighbor entries for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ipv6 neighbor ipv6-address mac-address</code>	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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-ip)#ipv6 nd dad attempts <i>value</i>	Configure times of sending NS messages for detecting duplicated addresses.



Note

When the Gazelle S1512i-PWR 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config)#ipv6 neighbors max-learning-num <i>number</i>	Configure the maximum number of NDPs allowed to be learnt on Layer 3 interface.

5.4.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show ipv6 neighbors	Show all NDP neighbor information.
2	Raisecom#show ipv6 neighbors <i>ipv6-address</i>	Show neighbor information about a specified IPv6 address.
3	Raisecom#show ipv6 neighbors vlan <i>vlan-id</i>	Show neighbor information about a specified layer 3 interface.
4	Raisecom#show ipv6 neighbors static	Show information about IPv6 static neighbor.

No.	Command	Description
5	Raisecom# show ipv6 interface prefix [<i>interface-type</i> <i>interface-number</i>]	Show information about the IPv6 address prefix.
6	Raisecom# show ipv6 interface nd [<i>interface-type</i> <i>interface-number</i>]	Show ND configurations on the interface.

5.4.8 Maintenance

Maintain the Gazelle S1512i-PWR as below.

Command	Description
Raisecom(config)# clear ipv6 neighbors	Clear information about all IPv6 neighbors.

6 IP routing

This chapter describes basic principles and configuration procedure of IP routing, and provides related configuration examples.

- Introduction
- Configuring route management
- Configuring static route
- Configuring routing policy
- Configuring OSPFv2
- Configuring RIP

6.1 Introduction

6.1.1 Route management

Routing is a behavior of forwarding packets to the destination through the network. The routing table is used in packet transmission. Routing is implemented for communication between devices of different VLANs or the same VLANs across different network segments.

Route management is targeted for providing uniform management of the routing table, static routes, and dynamic routing protocols.

6.1.2 Default route

The static route is the route configured manually, thus bringing low requirements for 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.

The default route is a special route that can be used only when there is no matched entry 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 Gazelle S1512i-PWR has not been configured with default route and the destination IP of the packet is not in the routing table, the Gazelle S1512i-PWR will discard the packet and return an ICMP packet to the Tx end to inform that the destination address or network is unavailable.

6.1.3 Routing policy

Routing policy is used to:

- Filter broadcasted, received, and imported routing information.
- Modify route attributes after match.
- Modify content of the routing table.
- Support special networking applications.

For example,

- A route needs to apply some policy when a routing device broadcasts or receives routing information so that it can filter routing information, such as receiving or broadcasting routing information that matches certain conditions.
- Routing protocols, such as RIP and OSPF, need routing information discovered by other routing protocols to rich their own routing information. Sometimes, they only need some routing information that matches certain conditions, and configures the routing information to meet their own requirements.

To implement routing policy, define matching rules first, which are characteristics of routing information targeted for routing policy. You can apply these rules to route advertisement, receiving, importing, and so on. You can use different attributes of routing information as matching rules, such as destination address, the address of the device that advertises routing information.

Classification of matching rules

When configured with unicast routing policy, the Gazelle S1512i-PWR supports matching with the following modes.

- Access Control List (ACL)

ACL can contain multiple matching rules, such as source address or destination address of packets, and protocol port number. When ACL is applied to routing policy, only IP ACL with specified IP address and mask information is supported to match prefix information of router address.

- IP Prefix-list

The IP prefix list acts like ACL, but is more flexible and easier to be understood. When being applied to routing policy, its matching target is the prefix of route address.

The IP prefix list is identified by the name of the prefix list. Each prefix list can contain multiple prefix list nodes, which are in OR relation to each other. Each node defines a matching rule and is identified by a serial number (SN). Each entry (matching rule) can independently specify a matching range of network prefix and is identified by an identification number, which indicates the sequence for matching. Different tables of the same node are in AND relation. During matching, the device matches each entry identified by SN in ascending order. Once an entry is matched, this matching process ends and no more matching for next entry will be performed. If all nodes do not match, the packet will not be filtered by matching rules.

- Route-Map

The routing map is a complex filter. Besides matching routing information, it can even change attributes of routing information if permitted. When applied to routing policy, its matching target is routing information or some attributes of routing information, such as prefix, matrix

value, route mark, and route type. It can even use ACL and IP prefix list to match routing information.

A routing map consists of multiple nodes which are in OR relation to each other. During matching, the device matches each node identified by SN in ascending order. Once a node is matched, this policy takes effect and no more matching for next node will be performed.

Each node of a routing map consists of a group of match and set sub-sentences.

- The match subsentence defines match rules and its matching object is some attributes of routing information. Different match sub-sentences of the same node are in AND relation. Only conditions specified by all match sub-sentences are met, the node is matched.
- The set sub-sentence specifies the action. Namely, when routing information matches the match sub-sentences of the node, some attributes of routing information will be modified.

Modes for applying routing policy

A routing policy consists of multiple nodes. Each node is a unit for matching check. During matching, the device matches each node identified by SN in ascending order. Different nodes are in OR relation. Once a node is matched, this policy takes effect and no more matching for next node will be performed.

A routing policy is applied in the following two modes:

- When a routing protocol uses routes discovered by other routing protocols, it can apply a routing policy to use the routing information that meets specified conditions.
- When a routing protocol advertises or receives routes discovered by it, it can apply a routing policy to filter routing information so that it receives or advertises route information meeting specified conditions.

6.1.4 OSPF

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).
- 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).
- **Non-Broadcast Multi-Access (NBMA):** when the link layer protocol is the frame relay, ATM, or X.25, OSPF regards the default network type as NBMA. The NBMA network sends protocol packets in unicast mode.
- **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.



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

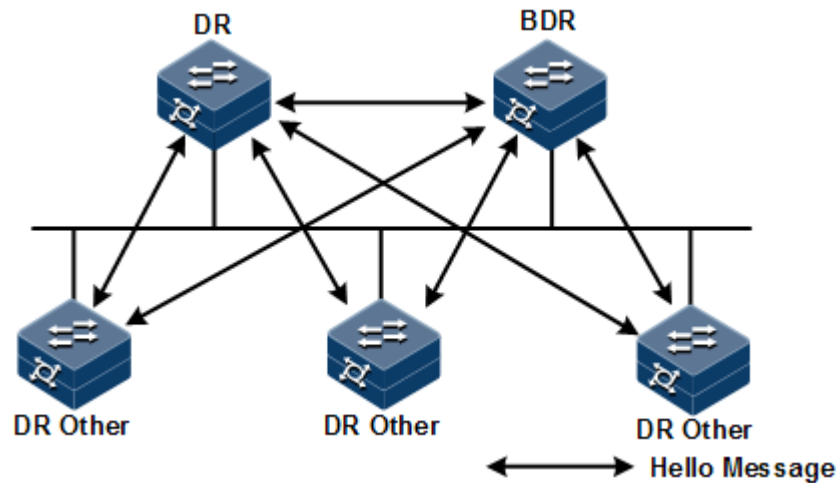
In a broadcast network, any two routers need to exchange routing information. Thus route change on a router causes multiple transmissions, which wastes bandwidth resources. To solve this problem, OSPF defines the Designated Router (DR), which receives information from all routers and then advertises 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 6-1. It reduces the number of relations between routers in the broadcast network and NBMA network, reduces network traffic, and saves bandwidth resource.

Figure 6-1 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 Gazelle S1512i-PWR supports up to 32 neighbors.

Calculating OSPF routes

OSPF calculates routes as below:

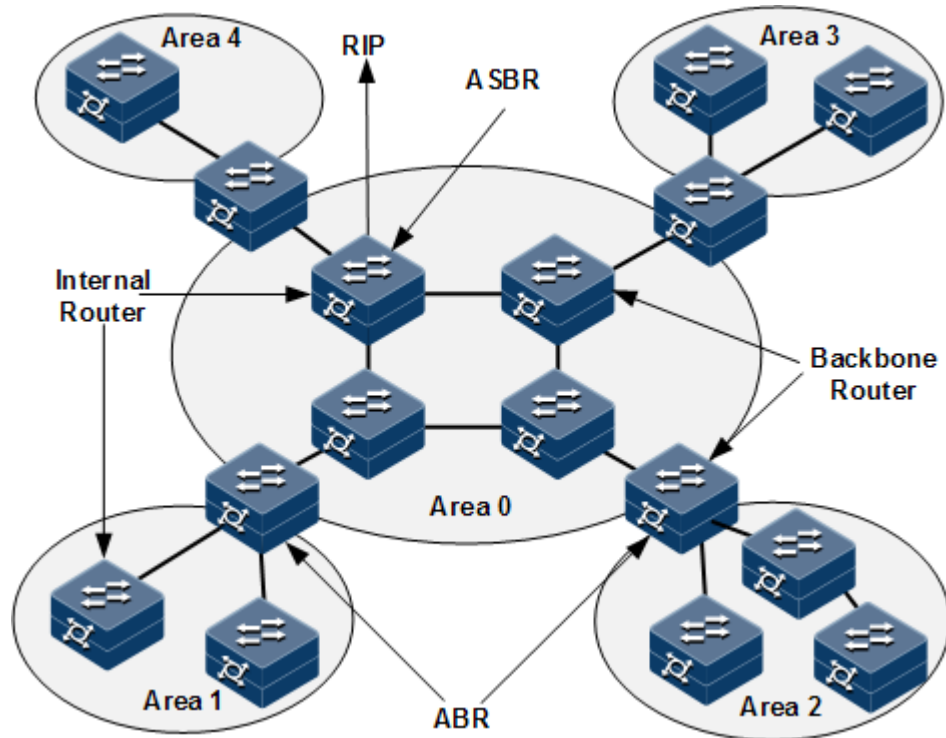
- Step 1 Each OSPF router generates LSAs according to network topology, and sends LSAs to other OSPF routers through updating packets.
- Step 2 Each OSPF router collects LSAs from other OSPF routers. All LSAs form LSDB. LSA describes network topology around the router. LSDB describes network topology 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 6-1, a route in an area maintains routing information of the area instead of the entire AS.

Figure 6-2 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 6-2, 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.

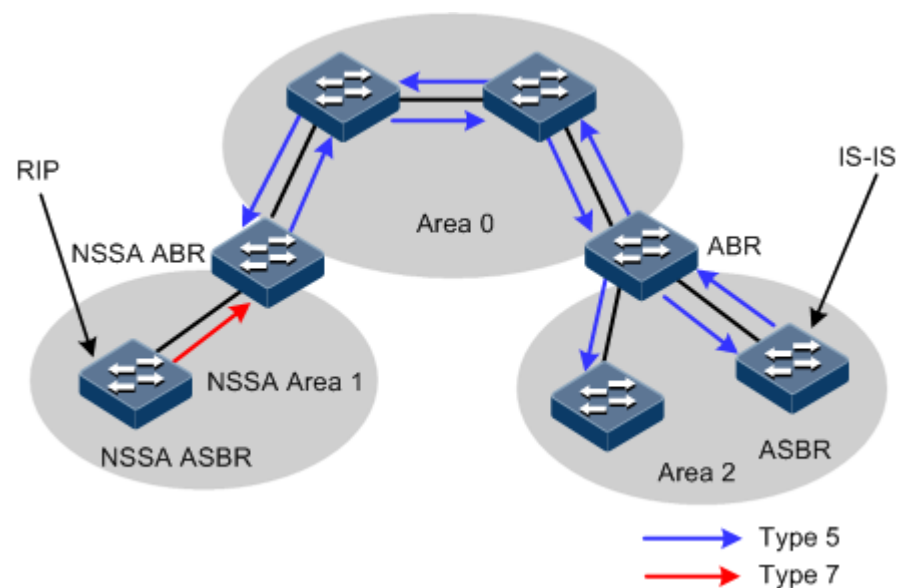
In the Stub area, only Type1, Type2, and Type3 LSAs are advertised, and Type5 LSAs are not allowed to enter, which reduces the size of the routing table and the number of transmitted routes. In addition, you can configure the area to Totally Stub area which allows Type1 and Type2 LSAs and a default Type3 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.

NSSA

Not-So-Stubby Area (NSSA, not the total Stub area) is similar to the Stub area. In the NSSA area, Type5 LSAs are not allowed to enter, but Type7 LSAs are allowed. Type7 LSAs are generated by ASBR and spread in the NSSA area. When reaching ABR in the NSSA area, Type7 LSAs are transformed to Type5 LSAs and spread to other areas, as shown in Figure 6-3.

Figure 6-3 NSSA area



External routers of the AS cannot enter the NSSA area, but ASE routers imported by routers in the AS can be spread in the NSSA area and transmitted out of the NSSA area. Namely, cancel restriction on ASE bidirectional spread in the Stub area (routers out of the area cannot enter

the area, and ones in the area cannot be spread out of the area), and change the bidirectional restriction as unidirectional restriction (routers out of the area cannot enter the area, but ones in the area can be spread out of the area).



- To solve the ASE unidirectional transmission, the NSSA area defines Type7 LSAs, which are used as inner routers when importing external routers. Except type identifier, Type7 LSAs are similar to Type5 LSAs. Thus, routers in the area can judge whether routes are from the area through their LSAs.
- Because Type7 LSAs are newly-defined LSAs, routers that do not support NSSA cannot identify them. Thus, there is a protocol regulation: transform Type7 LSAs on ASE to Type5 LSAs in the NSSA area and then advertised them out of the area; meanwhile, the advertiser is changed as ABR. In this case, external routers of the NSSA area can identify Type7 LSAs although they do not support NSSA.

As shown in Figure 6-3, AS running OSPF includes Area 0, Area 1, and Area 2. There are 2 ASs running RIP and Intermediate System to Intermediate System Routing Protocol (IS-IS).

- Area 1 is the NSSA area. After received RIP routes are spread to the NSSA ASBR, Type7 LSAs generated by NSSA ASBR are spread in the Area 1. When reaching NSSA ABR, Type7 LSAs are transformed as Type5 LSAs and spread to Area 2 from Area 0.
- IS-IS routes are spread in the AS through Type5 LSAs generated by ASBR. Because Area 1 is not the NSSA area, Type5 LSAs cannot reach Area 1. Same as the Stub area, virtual connectivity cannot traverse the NSSA 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.

6.1.5 RIP

Routing Information Protocol (RIP) is a simple Interior Gateway Protocol (IGP) based on distance-vector algorithm. It measures the distance to the destination address by hops, namely, the measurement value. The hops are usually within 15. RIP exchanges routing information through UDP packets.

Simple in configuration, maintenance, and management, SIP is widely used in small to medium-sized networks and regional networks with slow change of network topology. Defined by RIP, when the measurement value equals to or exceeds 16, the distance is taken

infinite; in other words, the destination network or host is unreachable; thus, RIP is unfit for large networks.

RIP versions

RIP has the following two versions:

- **RIPv1:** a classful routing protocol, supporting advertisement of protocol packets in broadcast mode. RIPv1 is used on UDP. Its packets cannot exceed 512 bytes, and do not carry mask information, so they can identify natural segment route of Class A, Class B, and Class C and do not support continuous subnets.
- **RIPv2:** a classless routing protocol, with the following advantages over RIPv1:
 - Support external route mark, and flexibly control routes by Tag through routing policy.
 - Carry mask information in packets, and support route aggregation and Classless Inter-Domain Routing (CIDR).
 - Support specifying the next hop and choosing the optimal next hop in a broadcast network.
 - Support sending update packet through multicast route. Only RIPv2-supportive devices can receive packets of this type, thus reducing resource waste.
 - Support verifying protocol packets in plaintext and MD5 verification modes, thus enhancing security.

RIP principles

The Gazelle S6028i running RIP manages a route database, which contains entries of all routes reachable to the destination, including the destination address, next hop address, egress interface, measurement value, and routing time. RIP works as below:

- Step 1 After enabling RIP, the Gazelle S6028i sends a request packet to neighbors. Those neighbors running RIP will respond to the request, and then send back a response packet containing local routing table information.
- Step 2 After receiving the response packet, the Gazelle S6028i updates the local routing table, and sends update packets to its neighbors at the same time, informing them of routing update information. After receiving routing update information, its neighbors send routing update packet to their neighbors to update their routing information.
- Step 3 In this way, the Gazelle S6028i running RIP ensures that its routes and neighbors' routes are updated. In addition, RIP uses the aging mechanism to age expired routes to ensure validness and realtime performance.

RIP is a routing protocol based on distance-vector algorithm. Because the Gazelle S6028i informs its neighbors of its entire routing table, route loop is possible to occur. To improve performance and avoid loop, RIP supports infinite counters, split horizon, poison reverse, and triggered update mechanism.

Key-chain

RIPv2 packets support plaintext authentication, MD5 authentication, and no authentication. During authentication, the password to be used is kept in Key-chain. The Key-chain provides authentication to all application layer protocols. It can dynamically change password chain without losing packets.

To ensure security, the network keeps changing authentication information about the application layer, uses authentication algorithms, and shares security key to judge whether information is tampered with during transmission on an unsecure network. If each application layer protocol maintains a set of authentication rules and a large number of applications use the same authentication modes, authentication information will be copied and changed. If each application uses a fixed authentication key, it has to inform the administrator of manually changing the key. It is difficult to manually change keys or authentication algorithms and change password for all devices without losing packets.

In this way, the system has to manage all authentications, change authentication algorithms and keys in a centralized way without much manual load. The Key-chain is thus introduced.

6.2 Configuring route management

6.2.1 Configuring route management

Configure route management for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router id router-id</code>	(Optional) configure the router ID.
3	<code>Raisecom(config)#route recursive-lookup tunnel [ip-prefix listname]</code>	Configure the route for the public network to transmit unlabeled packets to be recursive to the LSP tunnel.

6.2.2 Checking configurations

Use the following commands to check configuration results as below. Gazelle S1512i-PWR

No.	Command	Description
1	<code>Raisecom#show router id</code>	Show the router ID.
2	<code>Raisecom#show ip route [detail]</code>	Show information about the routing table.
3	<code>Raisecom#show ip route protocol { static connected bgp ospf isis rip } [detail]</code>	Show information about routes of a specified protocol.
4	<code>Raisecom#show ipv6 route [protocol { static connected bgp ospf isis rip }]</code>	Show information about IPv6 routes of a specified protocol.
5	<code>Raisecom#show ip route ip-address1 [mask-address1] ip-address2 [mask- address2] [detail]</code>	Show information about routes of an IP address range.
6	<code>Raisecom#show { ip ipv6 } route summary</code>	Show route statistics.
7	<code>Raisecom#show ip route ip-address [mask-address] [longer-prefixes]</code>	Show information about the

No.	Command	Description
	Raisecom# show ipv6 route { <i>ipv6-address</i> <i>ipv6-address/prefix-length</i> }	route to a specified IP address.

6.3 Configuring static route

6.3.1 Preparing for configurations

Scenario

The static route has the following advantages:

- Consume less time for the CPU to process them.
- Facilitate the administrator to learn the route.
- Be configured easily.

However, when configuring the static route, you need to consider the whole network. If the network structure is changed, you need to modify the routing table manually. Once the network scale is enlarged, it will consume lots of time to configure and maintain the network. In addition, it may cause more errors.

The default route is a specific static route. It will be used when no matched route is found in the routing table.

Prerequisite

N/A

6.3.2 Configuring static route

Configure static route for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# ip route <i>ip-address</i> { <i>masklength</i> <i>ip-mask</i> } <i>next-hop-ip-address</i> [<i>interface-type interface-num</i>] [distance <i>distance</i>] [description <i>text</i>] [tag <i>tag</i>]	Configure the IPv4 static route.
3	Raisecom(config)# ip route static distance <i>distance</i>	(Optional) configure the default administrative distance of the IPv4 static route. By default, it is 1.

6.3.3 Checking configurations

Use the following commands to check configuration results.

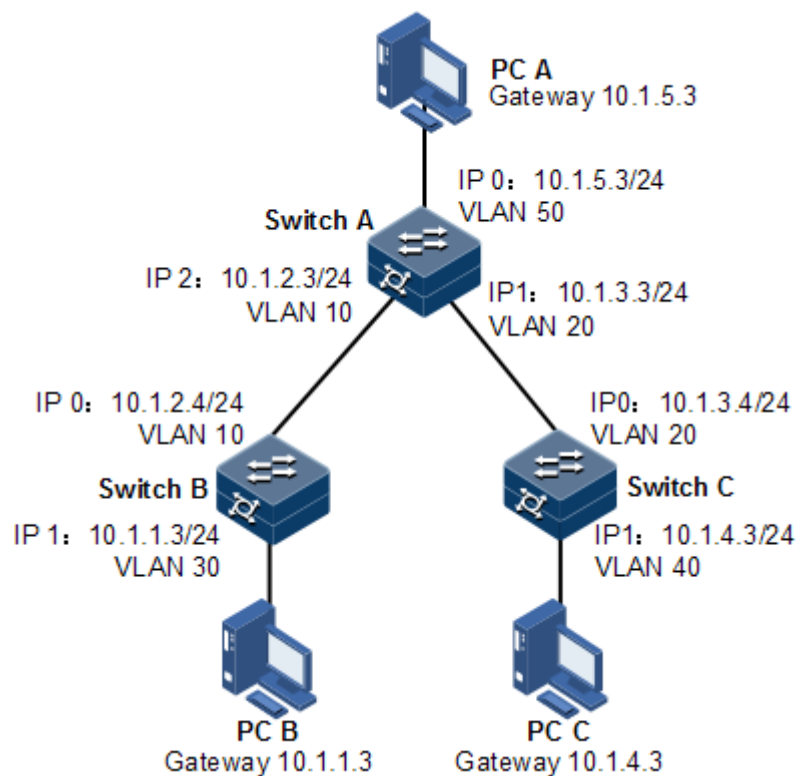
No.	Command	Description
1	Raisecom# show ip route [detail]	Show information about the IPv4 route.

6.3.4 Example for configuring static route

Networking requirements

Configure the static route to enable any two hosts or switches to ping through each other, as shown in Figure 6-4.

Figure 6-4 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#hostname 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#hostname 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 result

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.
```

6.4 Configuring routing policy

6.4.1 Configuring IP prefix-list

Configure the IP prefix-list for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip prefix-list prefix-name [seq seq-number] { deny permit } any</code> <code>Raisecom(config)#ip prefix-list prefix-name [seq seq-number] { deny permit } ip- address/mask [ge min-length] [le max-length]</code>	Create an IP prefix-list or add a node to the IP prefix-list. If no prefix-list ID (<i>seq-number</i>) is configured, the system will generate a prefix-list ID automatically. The generated pre-fix list ID has 5 digits.
3	<code>Raisecom(config)#ip prefix-list prefix-name description string</code>	Configure descriptions of the IP prefix-list. If the length of descriptions exceeds 80 characters, the first 80 characters are available.



Note

- If one record is in permit type, all mismatched routes are in deny type by default. Only matched routes can pass filtering of the IP prefix-list.
- If one record is in deny type, all mismatched routes are in deny type by default. Even matched routes cannot pass filtering of the IP prefix-list. Therefore, you need to add a permit record after multiple deny records to allow other routes to pass.
- If there are multiple records in the IP prefix-list, there must be a record in permit type.

6.4.2 Configuring route mapping table

Configure the route mapping table for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#route- map map-name { permit deny } number</code>	Create the route mapping table and enter route mapping configuration mode.
3	<code>Raisecom(config-route- map)#description string</code>	Configure descriptions of the route mapping table. If there is any space in descriptions, descriptions should be within quotes.
4	<code>Raisecom(config-route- map)#on-match next</code>	Configure the on-match sub-clause to continuing to match at the next node. By default, the process is finished after matching.
5	<code>Raisecom(config-route- map)#on-match goto number</code>	Configure the on-match sub-clause to continuing to match at some node. By default, the process is finished after matching.

Step	Command	Description
6	Raisecom(config-route-map)# match ip next-hop acl-number	Configure the match sub-clause to matching the next hop based on extended IP ACL.
7	Raisecom(config-route-map)# match ip next-hop prefix-list prefix-name	Configure the match sub-clause to matching the next hop based on IP prefix-list.
8	Raisecom(config-route-map)# match ip address acl-number	Configure the match sub-clause to matching the IP address based on extended IP ACL.
9	Raisecom(config-route-map)# match ip address prefix-list prefix-name	Configure the match sub-clause to matching the IP address based on IP prefix-list.
10	Raisecom(config-route-map)# match interface name	Configure the match sub-clause to matching the interface name.
11	Raisecom(config-route-map)# match metric metric	Configure the match sub-clause to the matching rule that is based on route metric value.
12	Raisecom(config-route-map)# match tag tag	Configure the match sub-clause to the matching rule that is based on Tag field of the route tagging.
13	Raisecom(config-route-map)# set metric [+ -] metric	Configure the set sub-clause to modifying the route metric value after matching.
14	Raisecom(config-route-map)# set metric-type { type-1 type-2 }	Configure the set sub-clause to modifying the route metric type after matching.
15	Raisecom(config-route-map)# set src ip-address	Configure the set sub-clause to modifying the source IP address after matching.
16	Raisecom(config-route-map)# set ip next-hop ip-address	Configure the set sub-clause to modifying the next-hop IP address of the route after matching.
17	Raisecom(config-route-map)# set tag tag	Configure the set sub-clause to modifying the routing information tag after matching.

6.4.3 Checking configurations

Use the following commands to check configurations.

No.	Command	Description
1	Raisecom# show ip prefix-list [prefix-name] [seq seq-number]	Show information about the IP prefix list.
2	Raisecom# show ip prefix-list summary prefix-name	Show summary of the IP prefix list.
3	Raisecom# show ip prefix-list detail prefix-name	Show statistics on the IP prefix list.

No.	Command	Description
4	Raisecom# show route-map [<i>map-name</i>]	Show configurations of the route mapping table.

6.5 Configuring OSPFv2

6.5.1 Configuring basic functions of OSPF

Configure basic functions of OSPF for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Start OSPF process, and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)# network <i>ip-address wild-card-mask</i> area <i>area-id</i>	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.

6.5.2 Configuring OSPF route attributes

Configuring interface cost

Configure the interface cost for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)# ip ospf cost <i>cost</i>	Configure the route cost of the VLAN interface.

Configure the OSPF reference bandwidth for the Gazelle S1512i-PWR 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.



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: $\text{cost} = \text{link bandwidth reference value (bit/s)} / \text{link bandwidth}$. 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 Gazelle S1512i-PWR 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>	Enable an OSPF process and enter OSPF configuration mode.
3	<code>Raisecom(config-router-ospf)#distance administrative-distance</code>	Configure the OSPF administrative distance. By default, it is 110.
4	<code>Raisecom(config-router-ospf)#distance ospf { intra-area inter-area external } distance</code>	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 Gazelle S1512i-PWR 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>	Enable an OSPF process, and enter OSPF configuration mode.

Step	Command	Description
3	Raisecom(config-router-ospf)# compatible rfc1583	Configure OSPF to be compatible with RFC1583. By default, OSPF is compatible with RFC1583.

6.5.3 Configuring OSPF network

Configuring OSPF network type

Configure the OSPF network type for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)# ip ospf network { broadcast non-broadcast ptmp ptp }	Configuring the network type of the VLAN interface. By default, it is the broadcast network.

Configuring DR election priority

Configure the DR election priority for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)# ip ospf priority <i>priority</i>	Configure the DR election priority. By default, it is 1.

Configuring OSPF NBMA network neighbor

Configure the OSPF NBMA network neighbor for the Gazelle S1512i-PWR as below.

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

Step	Command	Description
2	Raisecom(config)# interface <i>vlan</i> <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)# ip ospf network non-broadcast Raisecom(config-vlan1)# exit	Configure the VLAN interface network mode to NBMA and exit Layer 3 interface configuration mode.
4	Raisecom(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
5	Raisecom(config-router-ospf)# neighbor <i>ip-address</i> [priority <i>priority</i>]	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 send 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.

6.5.4 Configuring OSPF NBMA network neighbor

Configure the OSPF NBMA network neighbor for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Start an OSPF process, and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)# area <i>area-id</i> nssa [no-summary]	Configure the area as a NSSA. Only the non-backbone area can be the NSSA. By default, all non-backbone areas are common areas.

6.5.5 Optimizing OSPF network

Configuring OSPF packet timer

Configure the OSPF packet timer for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface vlan vlan-id</code>	Enter VLAN interface configuration mode.
3	<code>Raisecom(config-vlan1)#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-vlan1)#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-vlan1)#ip ospf poll-interval seconds</code>	Configure the OSPF Poll timer interval. By default, it is 120s.
6	<code>Raisecom(config-vlan1)#ip ospf retransmit-interval seconds</code>	Configure the LAS retransmission interval on the IP interface. By default, it is 5s.
7	<code>Raisecom(config-vlan1)#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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router ospf process-id [router-id router-id]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#timers spf delay-time hold-time	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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan vlan-id	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#ip ospf passive-interface enable	Configure the passive interface on the OSPF interface. By default, it is disabled.

Configuring MTU ignorance

By default, the value of MTU domain in the packet is the MTU value of the interface, which sends the 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 packet will be discarded. To ensure receiving the 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan vlan-id	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#ip ospf mtu-ignore enable	Enable MTU ignorance on the VLAN interface. By default, MTU ignorance is disabled on the IP interface to check MTU of the OSPF Hello packet.

6.5.6 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router ospf process-id [router-id router-id]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#area area-id authentication { md5 simple }	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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan vlan-id	Enter VLAN interface configuration mode.

Step	Command	Description
3	<code>Raisecom(config-vlan1)#ip ospf authentication { md5 simple }</code>	Configure the authentication mode of the VLAN interface. By default, it is non-authentication. It means adopting the area authentication mode.
4	<code>Raisecom(config-vlan1)#ip ospf authentication-key { simple [0 7] password md5 { [key-id [0 7] password] keychain keychain-name } }</code>	Configure the authentication password of the VLAN interface.

6.5.7 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 Gazelle S1512i-PWR 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>	Enable an OSPF process and enter OSPF configuration mode.
3	<code>Raisecom(config-router-ospf)#area area-id stub [no-summary]</code>	Configure the area to a Stub area. The no-summary 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	<code>Raisecom(config-router-ospf)#area area-id default-cost cost</code>	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.



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.

6.5.8 Controlling OSPF routing information

Configuring OSPF redistributed routes

Configure OSPF redistributed routes for the Gazelle S1512i-PWR 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>	Enable an OSPF process and enter OSPF configuration mode.
3	<code>Raisecom(config-router-ospf)#redistribute { static connected isis bgp } [metric metric] [metric-type { 1 2 }] [tag tag-value] [route-map map-name]</code> <code>Raisecom(config-router-ospf)#redistribute ospf [process-id] [metric metric] [metric-type { 1 2 }] [tag tag-value] [route-map map-name]</code>	Configure OSPF route redistribution policy. By default, no external route is redistributed. When an external route is redistributed: <ul style="list-style-type: none"> • 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. • If no Metric-type is specified, the Metric-type is Type2 by default. • If no Tag is specified, take the original Tag of the external route as the Tag of the LSA.
4	<code>Raisecom(config-router-ospf)#redistribute limit limit-number</code>	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 Gazelle S1512i-PWR 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>	Enable an OSPF process and enter OSPF configuration mode.

Step	Command	Description
3	<code>Raisecom(config-router-ospf)#area <i>area-id</i> range <i>ip-address ip-mask</i> [not-advertise]</code>	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 Gazelle S1512i-PWR 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router ospf <i>process-id</i> [router-id <i>router-id</i>]</code>	Enable an OSPF process and enter OSPF configuration mode.
3	<code>Raisecom(config-router-ospf)#summary-address <i>ip-address ip-mask</i> [not-advertise] [metric <i>metric</i>]</code>	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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router ospf <i>process-id</i> [router-id <i>router-id</i>]</code>	Enable an OSPF process and enter OSPF configuration mode.
3	<code>Raisecom(config-router-ospf)#default-information originate [always] [metric <i>metric</i>] [type { 1 2 }]</code>	Redistribute the default route. By default, no default route is generated. When the default LSA is generated, if the always key word is specified, the default Metric is 1. If the always key word is not specified, the Metric is 10.

6.5.9 Configuring NSSA

The Stub area cannot redistribute external routes. To allow the device to redistribute external routes inside the OSPF area and keep characteristics of the Stub area in other parts, you can configure the area as a NSSA.

Configure the NSSA for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Start an OSPF process, and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)# area <i>area-id</i> nssa [no-summary]	Configure the area as a NSSA. The no-summary parameter is used on the ABR in the NSSA only. After the area is configured as a NSSA, the NSSA ABR advertises the default route to the area through Type-3 Summary-LSA, rather than flooding any other Summary-LSA.
4	Raisecom(config-router-ospf)# area <i>area-id</i> default-cost <i>cost</i>	Configure the default route cost of the area.



Note

- All devices in the NSSA must be configured with NSSA attributes through the **nssa** command.
- The backbone area cannot be configured as the NSSA.
- The virtual connection cannot traverse the NSSA.

6.5.10 Controlling OSPF routing information

Configuring OSPF redistributed routes

Configure OSPF redistributed routes for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.

Step	Command	Description
3	<pre>Raisecom(config-router-ospf)#redistribute { static connected rip isis ospf bgp } [metric metric] [metric-type { 1 2)] [tag tag-value] [route-map map-name]</pre> <pre>Raisecom(config-router-ospf)#redistribute ospf [process-id] [vrf vrf-name] [metric metric] [metric-type { 1 2] [tag tag- value] [route-map map- name]</pre>	<p>Configure OSPF route redistribution polity.</p> <p>By default, no external route is redistributed. When an external route is redistributed:</p> <ul style="list-style-type: none"> • 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. • If no Metric-type is specified, the Metric-type is Type2 by default. • If no Tag is specified, take the original Tag of the external route as the Tag of the LSA.
4	<pre>Raisecom(config-router-ospf)#redistribute limit limit-number</pre>	<p>Configure the threshold of redistributed OSPF external routes.</p> <p>By default, no threshold is configured.</p>

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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#router ospf process-id [router-id router-id]</pre>	Enable an OSPF process and enter OSPF configuration mode.
3	<pre>Raisecom(config-router-ospf)#area area-id range ip-address ip-mask [not-advertise]</pre>	<p>Configure the inter-area route aggregation.</p> <p>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.</p>

Configuring redistributed external route aggregation

After the external route is redistributed, configure route aggregation on the ASBR. The Gazelle S1512i-PWR just puts the aggregated route on the ASE LSA. This helps reduces the number of LSAs in the LSDB.

Configure inter-area route aggregation for the Gazelle S1512i-PWR 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>	Enable an OSPF process and enter OSPF configuration mode.
3	<code>Raisecom(config-router-ospf)#summary-address ip-address ip-mask [not-advertise] [metric metric]</code>	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 Gazelle S1512i-PWR 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>	Enable an OSPF process and enter OSPF configuration mode.
3	<code>Raisecom(config-router-ospf)#default-information originate [always] [metric metric] [type { 1 2 }]</code>	Redistribute the default route. By default, no default route is generated. When the default LSA is generated, if the always key word is specified, the default Metric is 1. If the always key word is not specified, the Metric is 10.

6.5.11 Configuring OSPF routing policy

Configuring OSPF receiving policy

Configure the OSPF receiving policy for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip prefix-list list-name [index number] { permit deny } ip-address mask-length [greater-equal ge-length] [less-equal le-length]</code>	Configure the address prefix list. Use the no ip prefix-list list-name [index number] command to delete this configuration.

Step	Command	Description
3	Raisecom(config)# ip-access-list <i>acl-number</i> { deny permit } ip any { <i>destination-ip-address ip-mask</i>	Configure the IP ACL rule. At present, the Gazelle S1512i-PWR just supports matching the address prefix of the route by specifying the destination IP address and subnet mask.
4	Raisecom(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process, and enter OSPF configuration mode.
5	Raisecom(config-router-ospf)# distribute-list { ip-access-list <i>acl-number</i> prefix-list <i>list-name</i> } in	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 Gazelle S1512i-PWR 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 Gazelle S1512i-PWR does not filter received routes.

Configuring OSPF advertising policy

Configure the OSPF advertising policy for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# ip prefix-list <i>list-name</i> [index <i>number</i>] { permit deny } <i>ip-address mask-length</i> [greater-equal <i>ge-length</i>] [less-equal <i>le-length</i>]	Configure the IP prefix-list. You can use the no ip prefix-list <i>list-name</i> [index <i>number</i>] command to delete the configuration.
3	Raisecom(config)# ip-access-list <i>acl-number</i> { deny permit } ip any { <i>destination-ip-address ip-mask</i>	Configure the IP ACL rule. At present, the Gazelle S1512i-PWR just supports matching the address prefix of the route by specifying the destination IP address and subnet mask.
4	Raisecom(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.

Step	Command	Description
5	<code>Raisecom(config-router-ospf)#distribute-list { ip-access-list <i>acl-number</i> prefix-list <i>list-name</i> } out</code>	Configure the filtering policy that the OSPF releases type5 LSAs of to the AS.
6	<code>Raisecom(config-router-ospf)#distribute-list { ip-access-list <i>acl-number</i> prefix-list <i>list-name</i> } out [static connected rip isis bgp]</code> <code>Raisecom(config-router-ospf)#distribute-list { ip-access-list <i>acl-number</i> prefix-list <i>list-name</i> } out ospf <i>process-id</i> [vrf <i>vrf-name</i>]</code>	Configure the OSPF advertising policy.



Note

- Before configuring OSPF global advertising policy, ensure that the IP ACL used by the OSPF global advertising 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip prefix-list <i>list-name</i> { permit deny } <i>ip-address mask-length</i> [ge <i>ge-length</i>] [le <i>le-length</i>]</code>	Configure the IP prefix-list. You can use the no ip prefix-list list-name [index number] command to delete the configuration.
3	<code>Raisecom(config)#router ospf <i>process-id</i> [router-id <i>router-id</i>]</code>	Enable an OSPF process and enter OSPF configuration mode.
4	<code>Raisecom(config-router-ospf)#area <i>area-id</i> filter prefix-list <i>list-name</i> { in out }</code>	Configure Type3 LSA filtering policy in the area.



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.

6.5.12 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show ip ospf [<i>process-id</i>]	Show OSPF basic information.
2	Raisecom# show ip ospf [<i>process-id</i>] interface [<i>interface-type interface-number</i>]	Show OSPF interface information.
3	Raisecom# show ip ospf [<i>process-id</i>] neighbor [<i>interface-type interface-number</i>] [<i>neighbor-id</i>]	Show OSPF neighbor information.
4	Raisecom# show ip ospf [<i>process-id</i>] route	Show OSPF routing information.
5	Raisecom# show ip ospf [<i>process-id</i>] database [<i>max-age</i> <i>self-originate</i>]	Show OSPF link status database information and statistics.
	Raisecom# show ip ospf [<i>process-id</i>] database [<i>router</i> <i>network</i> <i>summary</i> <i>asbr-summary</i> <i>external</i>] [<i>linkstate-id</i>] [<i>adv-router ip-address</i> <i>self-originate</i>]	
	Raisecom# show ip ospf [<i>process-id</i>] database statistics	
6	Raisecom# show ip ospf [<i>process-id</i>] border-routers	Show information about routers at edges of the area and AS.
7	Raisecom# show ip ospf [<i>process-id</i>] neighbor statistics	Show OSPF statistics or OSPF neighbor statistics.
8	Raisecom# show ip ospf [<i>process-id</i>] summay-address	Show OSPF ASBR external route aggregation information.
9	Raisecom# show cspf tedb [<i>detail</i>]	Show information about the TEDB database.

6.5.13 Maintenance

Maintain the Gazelle S1512i-PWR as below.

Command	Description
Raisecom# clear ip ospf [<i>process-id</i>] process [<i>graceful</i>]	Restart the OSPF process.

6.6 Configuring RIP

6.6.1 Configuring basic RIP functions

Configure basic RIP functions for the Gazelle S1512i-PWR 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)#network ip-address</code>	Configure a directly-connected and effective network based on RIP.
4	<code>Raisecom(config-rip)#offset-list access-list-name { in out } offset-value [interface-type interface-number]</code>	Configure the additional metrics when the interface receives or sends RIP routes. By default, it is 0.
5	<code>Raisecom(config-rip)#passive-interface { interface-type interface-number vlan vlan-id default }</code>	(Optional) configure the interface to be a passive interface. By default, it is a non-passive interface.

6.6.2 Configuring RIP version

Configure the RIP version for the Gazelle S1512i-PWR 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)#version version-id</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)#exit</code> <code>Raisecom(config)#interface vlan vlan-id r</code> <code>Raisecom(config-vlan1)#</code>	Enter VLAN interface configuration mode.
5	<code>Raisecom(config-vlan1)#ip rip receive version { 1 2 }*</code>	Configure the receiving RIP version. By default, the receiving RIP version is subjected to the global RIP version.

Step	Command	Description
6	<code>Raisecom(config-vlan1)#ip rip send version { 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)#ip rip v2-broadcast</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 Gazelle S1512i-PWR. If the interface is configured with RIP version, then this RIP version prevails.

6.6.3 Configuring redistribution of external routes

Configure redistribution of external routes for the Gazelle S1512i-PWR 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)#host- route</code>	Enable the function of receiving host routes. By default, it is enabled.
4	<code>Raisecom(config- rip)#default-information originate</code>	Enable broadcasting the default route. By default, it is disabled.
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>	Enabled the function of checking the source IP address of the received RIP packets. By default, it is enabled.

6.6.4 Configuring RIP timer

Configure the RIP timer for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router rip	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)#timers basic <i>update-time invalid-time holddown-time flush-time</i>	Configure RIP timer. By default, the update interval is 30s. The invalid interval is 180s. The suppression interval is 120s. The refreshing interval is 120s.

6.6.5 Configuring loop suppression

Configure loop suppression for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan vlan-id	Enter interface configuration mode.
3	Raisecom(config-vlan1)#ip rip split-horizon	Enable split horizon on the interface; in other words, the route learned from one interface will not be broadcasted from the interface. By default, it is enabled.
4	Raisecom(config-vlan1)#ip rip poisoned-reverse	Enable poison reverse on the interface, namely, 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 concurrently, split horizon will be invalid.

6.6.6 Configuring authentication

Configure authentication for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	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 rip authentication mode { text md5 }</code>	Configure the packet authentication mode on the interface. By default, the authentication mode of RIPv2 packets on the interface is no authentication.
4	<code>Raisecom(config- gigaethernet1/1/port)#ip rip authentication string password- string</code>	Configure the interface-associated password.
5	<code>Raisecom(config- gigaethernet1/1/port)#ip rip authentication key-chain key- chain-name</code>	Configure the interface-associated authentication secret string.

6.6.7 Configuring routing policy

Configure the routing policy for the Gazelle S1512i-PWR 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)#distribute-list { ip-access-list acl-number prefix- list list-name route-map rmap-name } in [interface-type interface-number]</code>	Configure RIP ingress routing policy.
4	<code>Raisecom(config-rip)#distribute-list { ip-access-list acl-number prefix- list list-name route-map rmap-name } out [interface-type interface-number]</code>	Configure RIP egress routing policy.
5	<code>Raisecom(config-rip)#distribute-list gateway list-name in [interface-type interface-number]</code>	Execute routing policies on the source address of the received packets through RIP.

6.6.8 Configuring route calculation

Configure route calculation for the Gazelle S1512i-PWR as below.

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

Step	Command	Description
2	Raisecom(config)#router rip	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)#distance <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)#maximum load-balancing <i>number</i>	Configure the maximum number of IP equal-cost multi-path load balancing paths.

6.6.9 Checking configurations

Use the following commands to check configurations.

No.	Command	Description
1	Raisecom#show ip rip	Show basic information about RIP.
2	Raisecom#show ip rip database	Show information about RIP routing database.
3	Raisecom#show ip rip interface	Show configurations and status of the interface which runs RIP.

6.6.10 Maintenance

Maintain the Gazelle S1512i-PWR as below.

Command	Description
Raisecom(config-rip)#clear rip database	Clear information about RIP routing database.
Raisecom(config-rip)#clear rip statistics	Clear RIP interface statistics.

7 DHCP

This chapter describes basic principles and configuration procedures of DHCP, and providing related configuration examples, including the following sections:

- DHCP Client
- DHCP Snooping
- DHCP Options
- DHCP Server
- DHCP Relay

7.1 DHCP Client

7.1.1 Introduction

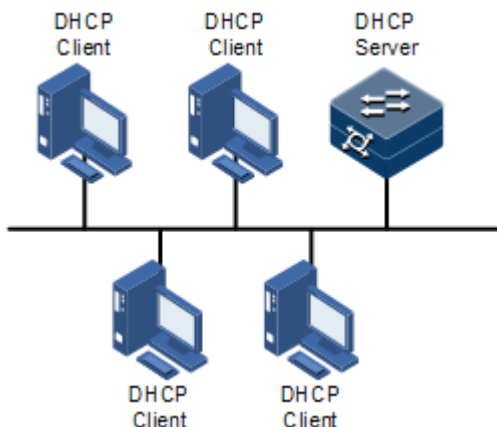
Dynamic Host Configuration Protocol (DHCP) refers to the protocol which assigns configurations, such as the IP address, to users on the TCP/IP network. Based on BOOTP (Bootstrap Protocol) protocol, it has additional features, such as automatically assigning available network addresses, reusing network 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 wide 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 configuration to the server (including IP address, subnet mask, and default gateway), and the server replies with IP address for the client and other related configurations to implement dynamic configurations of IP address.

Typical applications of DHCP usually include a set of DHCP server and multiple clients (for example PC or laptop), as shown in Figure 7-1.

Figure 7-1 DHCP typical networking



DHCP ensures rational allocation, avoids waste, and improves the utilization rate of IP addresses in the entire network.

Figure 7-2 shows the structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

Figure 7-2 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 7-1 describes fields of a DHCP packet.

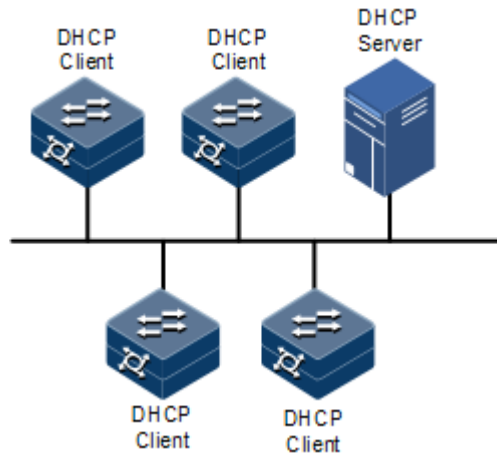
Table 7-1 Fields of a DHCP packet

Field	Length	Description
OP	1	Packet type • 1: a request packet • 2: a reply packet
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 at 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"> • 0: unicast • 1: broadcast 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 Gazelle S1512i-PWR can be used as a DHCP client to obtain the IP address from the DHCP server for future management, as shown in Figure 7-3.

Figure 7-3 DHCP Client networking



7.1.2 Preparing for configurations

Scenario

As a DHCP client, the Gazelle S1512i-PWR 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 withdraw 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.
- Disable DHCP Snooping.

7.1.3 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

7.1.4 Configuring DHCP Client

Before a DHCP client applies for an IP address, you must create a VLAN, and add the interface with the IP address to the VLAN. Meanwhile you must configure the DHCP server, otherwise the interface will fail to obtain an IP address through DHCP.


For VLAN interface 0, the IP addresses obtained through DHCP and configured manually can overwrite each other.



Note

- If the Gazelle S1512i-PWR is enabled with DHCP Server or DHCP Relay, it cannot be enabled with DHCP Client; vice versa.
- By default, the Gazelle S1512i-PWR is enabled with DHCP Client. Use the **no ip address dhcp** command to disable DHCP Client.
- If the Gazelle S1512i-PWR 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface vlan 1	Enter Layer 3 interface configuration mode.
3	Raisecom(config-vlan)# ip dhcp client { class-id class-id client-id client-id hostname hostname }	(Optional) configure DHCP client information, including the type identifier, client identifier, and host name.  Caution After the IP address is obtained by a DHCP client, client information cannot be modified.
4	Raisecom(config-vlan)# ip address dhcp [server-ip ip-address]	Configure the DHCP client to obtain IP address through DHCP.
5	Raisecom(config-vlan)# ip dhcp client renew	(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-vlan)# no ip address dhcp	(Optional) release the IP address.

7.1.5 Configuring DHCPv6 Client

Configure the DHCPv6 client for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)# interface vlan vlan-id	Enter VLAN interface configuration mode.
3	Raisecom(config- vlan1)#ipv6 address dhcp [server-ip ipv6- address]	Configure applying for IPv6 address through DHCPv6. If the Gazelle S1512i-PWR 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	Raisecom(config- vlan1)#ipv6 dhcp client renew	(Optional) renew the IPv6 address. If the Layer 3 interface on the Gazelle S1512i-PWR has obtained an IP address through DHCP, it will automatically renew the IPv6 address when the lease period expires.
5	Raisecom(config- vlan1)#ipv6 dhcp client rapid- commit	(Optional) enable DHCPv6 clients to apply for rapid interaction.

7.1.6 Checking configurations

Use the following commands to check configuration results.

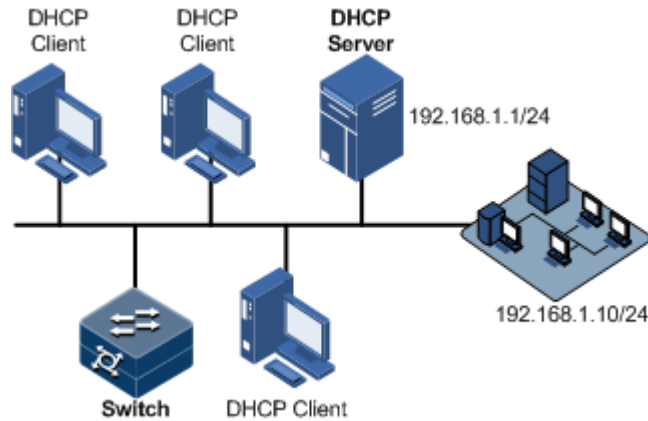
No.	Command	Description
1	Raisecom#show ip dhcp client	Show configurations of DHCP Client.
2	Raisecom#show ipv6 dhcp client	Show configurations of DHCPv6 Client.

7.1.7 Example for configuring DHCP Client

Networking requirements

As shown in Figure 7-4, 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 7-4 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 :            v1an10
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:           --
```

7.2 DHCP Snooping

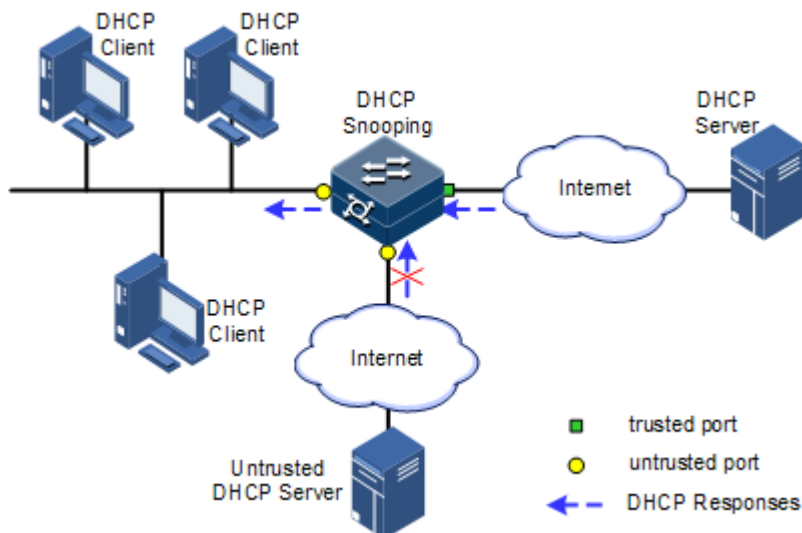
7.2.1 Introduction

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 7-5, 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 the reply packets from the DHCP server.

Figure 7-5 DHCP Snooping



- Record mapping between DHCP client IP address and MAC address.

DHCP Snooping records entries by monitoring 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. DHCP works based on the following 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 Gazelle S1512i-PWR is configured with DHCP Snooping to support DHCP Option:

- When the Gazelle S1512i-PWR receives a DHCP request packet, it processes the packet according to Option fields included or not, padding mode, and configured processing policy, then forwards the processed packet to the DHCP server.
- When the Gazelle S1512i-PWR 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.

7.2.2 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

7.2.3 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

7.2.4 Configuring DHCP Snooping

Generally, you must ensure that the Gazelle S1512i-PWR 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 Gazelle S1512i-PWR will do nothing to Option fields in packets. For packets without Option fields, the Gazelle S1512i-PWR 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip dhcp snooping</code>	Enable global DHCP Snooping.
3	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
4	<code>Raisecom(config-gigaethernet1/1/port)#ip dhcp snooping</code>	(Optional) enable interface DHCP Snooping.
5	<code>Raisecom(config-gigaethernet1/1/port)#ip dhcp snooping trust</code>	Configure the trusted interface of DHCP Snooping.
6	<code>Raisecom(config-gigaethernet1/1/port)#ip dhcp snooping information option vlan-list vlan-list</code>	Configure the DHCP Snooping VLAN list that supports Option 82.

Step	Command	Description
7	Raisecom(config-gigaetherne1/1/port)#exit Raisecom(config)#ip dhcp snooping option <i>option-id</i>	(Optional) configure DHCP Snooping to support user-defined Option.
8	Raisecom(config)#ip dhcp snooping option <i>client-id</i>	(Optional) configure DHCP Snooping to support Option 61.
9	Raisecom(config)#ip dhcp snooping information option	(Optional) configure DHCP Snooping to support Option 82.

7.2.5 Configuring DHCPv6 Snooping

Configure DHCPv6 Snooping for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ipv6 dhcp snooping	Enable global DHCPv6 Snooping.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	(Optional) enable interface DHCPv6 Snooping.
4	Raisecom(config-gigaetherne1/1/port)#ipv6 dhcp snooping	(Optional) enable DHCPv6 Snooping on the interface.
5	Raisecom(config-gigaetherne1/1/port)#ipv6 dhcp snooping trust	Enter physical layer interface configuration mode.
6	Raisecom(config-gigaetherne1/1/port)#exit Raisecom(config)#ipv6 dhcp snooping option <i>number</i>	(Optional) configure DHCPv6 Snooping to support customized Options.
7	Raisecom(config)#ipv6 dhcp snooping option <i>interface-id</i>	(Optional) configure DHCPv6 Snooping to support Option 18.

7.2.6 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	Raisecom#show ip dhcp snooping	Show configurations of DHCP Snooping.
2	Raisecom#show ip dhcp snooping binding	Show configurations of the DHCP Snooping binding table.
3	Raisecom#show ipv6 dhcp snooping	Show configurations of DHCPv6 Snooping.

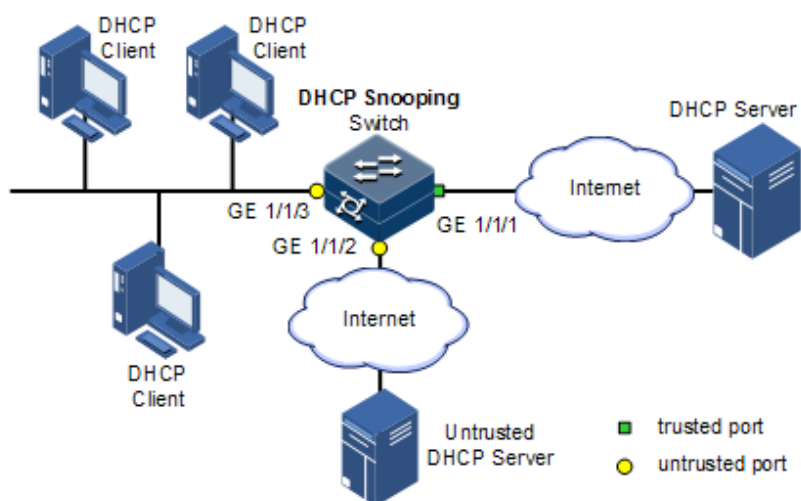
Step	Command	Description
4	raisecom#show ipv6 dhcp snooping binding	Show configurations of the DHCPv6 Snooping binding table.

7.2.7 Example for configuring DHCP Snooping

Networking requirements

As shown in Figure 7-6, 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 7-6 DHCP Snooping networking



Configuration steps

Step 1 Configure global DHCP Snooping.

```
raisecom#config
raisecom(config)#ip dhcp snooping
```

Step 2 Configure the trusted interface.

```
raisecom(config)#interface gigaethernet 1/1/1
raisecom(config-gigaethernet1/1/1)#ip dhcp snooping trust
raisecom(config-gigaethernet1/1/1)#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  4094  --          enabled        yes            1-
gigaethernet1/1/2  4094  --          enabled        no             1-
gigaethernet1/1/3  4094  --          enabled        no             1-
gigaethernet1/1/4  4094  --          enabled        no             1-
gigaethernet1/1/5  4094  --          enabled        no             1-
gigaethernet1/1/6  4094  --          enabled        no             1-
.....
```

7.3 DHCP Options

7.3.1 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 7-2 lists frequently used DHCP options.

Table 7-2 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
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, customized, 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 record 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 Gazelle S1512i-PWR 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 Gazelle S1512i-PWR, or user-defined string in request packets of the DHCP client.

7.3.2 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 and 37 are used to record information about IPv6 DHCP clients. Options 61 and 82 are used to record information about IPv4 DHCP clients. By cooperating with other software, the DHCP server can implement the following functions based on these Option fields, such as limit on IP address distribution and accounting.

Prerequisite

N/A

7.3.3 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

7.3.4 Configuring DHCP Option fields

Configure DHCP Option fields for the Gazelle S1512i-PWR as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip dhcp information option attach-string attach-string</code>	(Optional) configure additional information for Option 82 field.
	<code>Raisecom(config)#interface interface-type interface-number</code> <code>Raisecom(config-gigaethernet1/1/port)#ip dhcp information option circuit-id circuit-id [prefix-mode]</code>	(Optional) configure circuit ID sub-option information for Option 82 field on the interface.

Step	Command	Description
	<code>Raisecom(config)#ip dhcp information option { attach-string circuit-id format circuit-id hex } string</code>	(Optional) configure the attached string in Option 82 of DHCP packets.
	<code>Raisecom(config)#ip dhcp information option circuit-id mac-format string</code>	(Optional) configure the format of the MAC address in the variable of Circuit ID in Option 82 of DHCP packets.
	<code>Raisecom(config)#ip dhcp information option remote-id { client-mac client-mac-string hostname string string switch-mac switch-mac-string }</code>	(Optional) configure remote ID sub-option information for Option 82 field.
3	<code>Raisecom(config)#ipv4 dhcp option option-id { ascii ascii-string hex hex-string ip-address ip-address }</code>	(Optional) create user-defined Option based on IPv4.
	<code>Raisecom(config)#interface interface-type interface-number</code> <code>Raisecom(config-gigaethernet1/1/port)#ipv4 dhcp option option-id { ascii ascii-string hex hex-string ip-address ip-address }</code>	(Optional) create user-defined Option field information on the interface.
4	<code>Raisecom(config-gigaethernet1/1/port)#exit</code> <code>Raisecom(config)#ipv4 dhcp option client-id { ascii ascii-string hex hex-string ip-address ip-address }</code>	(Optional) configure Option 61 field information.
	<code>Raisecom(config-gigaethernet1/1/port)#ipv4 dhcp option client-id { ascii ascii-string hex hex-string ip-address ip-address }</code>	(Optional) configure Option61 field information on the interface.

7.3.5 Configuring DHCP Option 18 over IPv6

Configure DHCP Option 18 over IPv6 for the Gazelle S1512i-PWR 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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ipv6 dhcp option interface-id { ascii ascii-string hex hex-string ipv6-address ipv6-address }</code>	(Optional) configure information about Option 18.

Step	Command	Description
3	<pre>Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i> 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> }</pre>	(Optional) configure information about Option 18 on the interface.

7.3.6 Configuring DHCP Option 37 over IPv6

Configure DHCP Option 37 over IPv6 for the Gazelle S1512i-PWR 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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<pre>Raisecom(config)#ipv6 dhcp option remote-id { ascii hex } <i>string</i></pre>	(Optional) configure information about Option 37.
3	<pre>Raisecom(config)#ipv6 dhcp option remote-id mac- format <i>string</i></pre>	(Optional) configure the format of the MAC address of the Circuit ID variable in Option 37 in DHCPv6 packets.

7.3.7 Configuring user-defined DHCP Option over IPv6

Configure user-defined DHCP Option over IPv6 for the Gazelle S1512i-PWR 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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<pre>Raisecom(config)#ipv6 dhcp option <i>number</i> { ascii <i>ascii-string</i> hex <i>hex-string</i> ipv6-address <i>ipv6-address</i> }</pre>	(Optional) create user-defined Option information over IPv6.
3	<pre>Raisecom(config)#interface <i>interface- type</i> <i>interface-number</i> Raisecom(config- gigaethernet1/1/port)#ipv6 dhcp option <i>number</i> { ascii <i>ascii-string</i> hex <i>hex- string</i> ipv6-address <i>ipv6-address</i> }</pre>	(Optional) create user-defined Option information over IPv6 on the interface.

7.3.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show ip dhcp information option</code>	Show configurations of DHCP Option fields.

7.4 DHCP Server

7.4.1 Introduction

Dynamic Host Configuration Protocol (DHCP) refers to assigning IP address configurations dynamically for users in 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:

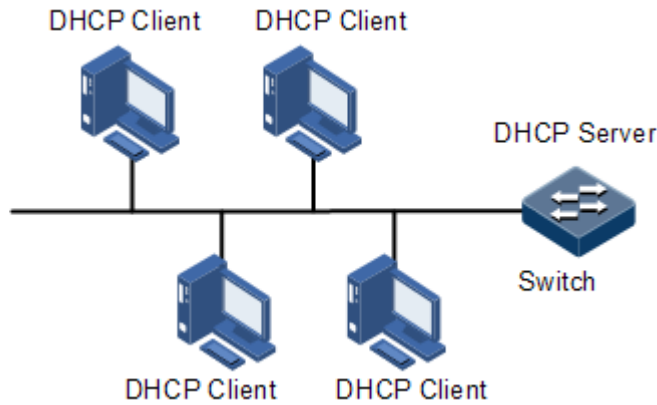
- The network scale is large. It requires much workload for manual configurations, and is difficult to manage the entire network intensively.
- The number of hosts on the network is greater than that of IP addresses, which makes it unable to assign a fixed IP address for each host and restricts the number of users connected to network simultaneously.
- Only the minority of hosts on the network requires fixed IP addresses, and most of hosts do not.

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.

The DHCP technology ensures rational allocation, avoids waste of IP addresses, and improves the utilization rate of IP addresses on the entire network.

The Gazelle S1512i-PWR, as the DHCP server, assigns dynamic IP addresses to clients, as shown in Figure 7-7.

Figure 7-7 DHCP Server and Client networking



DHCP packets

Figure 7-8 shows the structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

Figure 7-8 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 7-3 describes fields of a DHCP packet.

Table 7-3 Fields of a DHCP packet

Field	Length	Description
OP	1	Packet type <ul style="list-style-type: none"> • 1: a request packet • 2: a reply packet
Hardware type	1	Hardware address type of a DHCP client
Hardware length	1	Hardware address length of a DHCP client

Field	Length	Description
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 at 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"> • 0: unicast • 1: broadcast 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, and IP address of the WINS

7.4.2 Preparing for configurations

Scenario

When working as the DHCPv4 server, the Gazelle S1512i-PWR can assign IP addresses to DHCPv4 clients.

Prerequisite

- Disable DHCPv4 Client on the Gazelle S1512i-PWR.

- The DHCP server is a common one.

7.4.3 Creating and configuring IPv4 address pool

Configure the IPv4 address pool for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip dhcp server pool <i>pool-name</i></code>	Create an IPv4 address pool, and enter address pool configuration mode.
3	<code>Raisecom(config-pool)#address <i>start-ip-address end-ip-address mask { mask mask-length }</i></code>	Configure the range of IP addresses in the IPv4 address pool.
4	<code>Raisecom(config-pool)#lease expired { <i>minute</i> infinite }</code>	Configure the lease period for the IPv4 address pool.
5	<code>Raisecom(config-pool)#dns-server <i>ip-address</i> [secondary]</code>	Configure the DNS server of the IPv4 address pool.
6	<code>Raisecom(config-pool)#gateway <i>ip-address</i></code>	Configure the default gateway of the IPv4 address pool.
7	<code>Raisecom(config-pool)#option 60 <i>vendor-string</i></code>	Configure information carried by Option 60.
8	<code>Raisecom(config-pool)#tftp-server <i>ip-address</i></code>	Configure the TFTP server of the IPv4 address pool.
9	<code>Raisecom(config-pool)#trap server-ip <i>ip-address</i></code>	Configure the Trap server of the IPv4 address pool.

7.4.4 Enabling DHCPv4 Server

Enable DHCPv4 Server on the VLAN interface for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface vlan <i>vlan-id</i></code>	Enter interface configuration mode.
3	<code>Raisecom(config-vlan1)#ip dhcp server</code>	Enable DHCPv4 Server on the VLAN interface.

7.4.5 Checking configurations

Use the following commands to check configuration results.

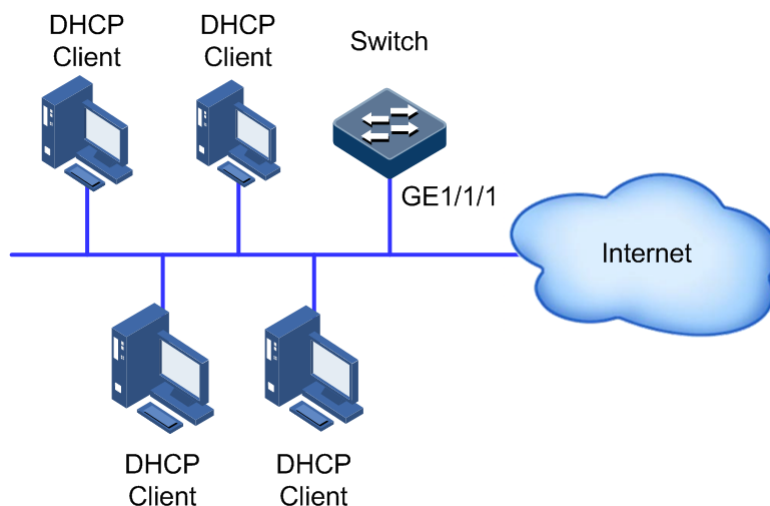
No.	Command	Description
1	Raisecom#show ip dhcp server	Show configurations of DHCP Server.
2	Raisecom#show ip dhcp server lease	Show assigned IP addresses and clients information.
3	Raisecom#show ip dhcp server statistics	Show packet statistics on the DHCP Server.
4	Raisecom#show ip dhcp static-bind	Show DHCPv4 static binding.
5	Raisecom#show ip server pool	Show configurations of the address pool of DHCP Server.

7.4.6 Example for configuring DHCPv4 Server

Networking requirements

As shown in Figure 7-9, 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 7-9 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 Configur 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 the 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      : pool
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      : DHCP Relay
```

7.5 DHCP Relay

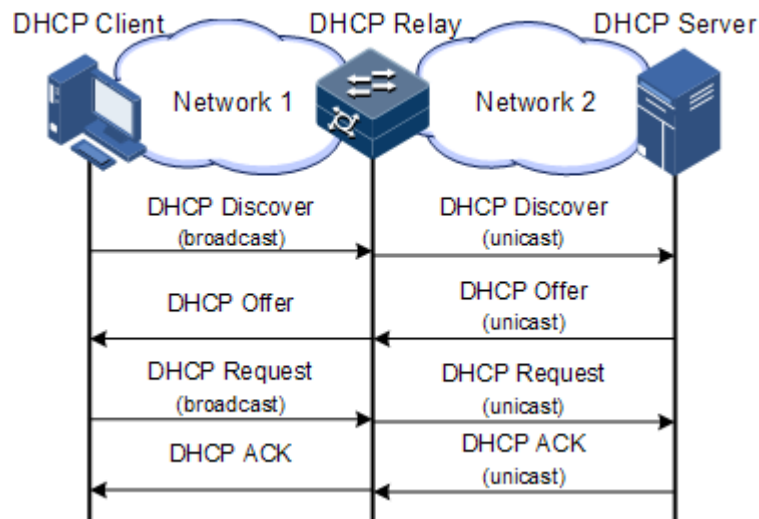
7.5.1 Introduction

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 7-10 shows typical application of DHCP Relay.

Figure 7-10 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.

7.5.2 Preparing for configurations

Scenario

When DHCP Client and DHCP Server are not in the same segment, you can use DHCP Relay to make DHCP Client and DHCP Server in different segments carry relay services, and relay DHCP packets across segments to the destination DHCP server, so that DHCP Client in different segments can share the same DHCP server.

Prerequisite

DHCP Relay is exclusive from DHCP Server, DHCP Client, and DHCP Snooping, so ensure that DHCP Server, DHCP Client, and DHCP Snooping are disabled when configuring DHCP Relay.

7.5.3 Default configurations of DHCP Relay

Default configurations of DHCP Relay are as below.

Function	Default value
Global DHCP Relay	Disable
Interface DHCP Relay	Disable

7.5.4 Configuring global DHCP Relay

Configure global DHCP Relay for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip dhcp relay</code>	Enable global DHCP Relay.

7.5.5 Configuring destination IP address for forwarding packets

Configure the destination IP address for forwarding packets for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface vlan vlan-id</code>	Enter VLAN interface configuration mode.
3	<code>Raisecom(config-vlan1)#ip dhcp relay target-ip ip-address</code>	Configure the destination IP address for forwarding packets.

7.5.6 Configuring IP address of DHCP relay device

Configure the IP address of DHCP relay device on the VLAN interface for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface vlan vlan-id</code>	Enter VLAN interface configuration mode.
3	<code>Raisecom(config-vlan1)#ip dhcp relay relay-ip ip-address</code>	Configure the IP address of the DHCP relay device.

7.5.7 (Optional) configuring DHCP Relay to support Option 82

Configure DHCP Relay to support Option 82 for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip dhcp relay information option</code>	Configure DHCP Relay to support Option 82.
3	<code>Raisecom(config)#ip dhcp relay information policy { drop keep replace }</code>	Configure the policy for DHCP Relay to process Option 82 request packets

Step	Command	Description
4	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
5	Raisecom(config- gigaethernet1/1/port)# ip dhcp relay information trusted	Configure the trusted interface of DHCP Relay.

7.5.8 Checking configurations

Use the following commands to check configuration results.

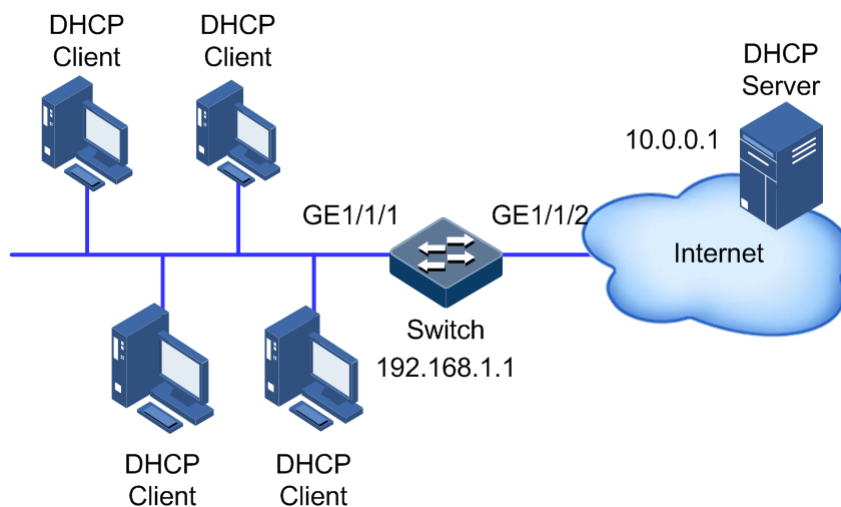
No.	Command	Description
1	Raisecom# show ip dhcp relay	Show configurations of DHCP Relay.
2	Raisecom# show ip dhcp relay information	Show information about Option 82 supported by DHCP Relay.

7.5.9 Example for configuring DHCPv4 Relay

Networking requirements

As shown in Figure 7-11, 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 7-11 DHCP Relay networking



Configuration steps

Step 1 Enable global DHCP Relay.

```
Raisecom#config
Raisecom(config)#ip dhcp relay
Raisecom(config)#create vlan 2,3 active
Raisecom(config)#interface vlan 2
Raisecom(config-vlan2)#ip dhcp relay relay-ip 192.168.1.1
Raisecom(config-vlan2)#exit
Raisecom(config)#interface vlan 3
Raisecom(config-vlan3)#ip dhcp relay relay-ip 192.168.1.1
Raisecom(config-vlan3)#exit
```

Step 2 Configure the destination IP address of DHCP Relay.

```
Raisecom(config)#interface vlan 2
Raisecom(config-vlan2)#ip dhcp relay target-ip 10.0.0.1
```

Checking results

Use the **show ip dhcp relay** command to show configurations of DHCP Relay.

```
DHCP Relay Global Status: Enable
Interface                Status      Relay Address    Target Address
-----
vlan2                    Enable     192.168.1.1     10.0.0.1
vlan3                    Enable     192.168.1.1     --
```

8 QoS

This chapter describes principles and configuration procedures of QoS, and provides related configuration examples, including the following sections:

- Introduction
- Configuring priority
- Configuring congestion management
- Configuring traffic classification and traffic policy
- Configuring rate limiting
- Configuration examples

8.1 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
- Congestion avoidance

8.1.1 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, applicable to most network applications, such as FTP and Email. It is implemented by First In First Out (FIFO) queues.

DiffServ

DiffServ is a multi-service model, which can meet different QoS requirements.

DiffServ does not need to maintain the status of each flow. It provides differentiated services according to the QoS classification of each packet. Multiple different methods can be used for classifying QoS packets, such as the IP packet priority (IP precedence), packet source address, and 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 the IP precedence, packet source address, or destination address. The system continues to send the packets if the flow complies with rules of the token bucket. Otherwise, it discards the packets or remarks the IP precedence, DSCP, EXP, and so on. CAR can not only control flows, but also mark and remark packets.
- **Queuing technology:** the queuing technologies of SP, WRR, DRR, SP+WRR, and SP+DRR cache and schedule congested packets to implement congestion management.

8.1.2 Priority trust

Priority trust means that the Gazelle S1512i-PWR uses priority of packets for classification and performs QoS management.

The Gazelle S1512i-PWR supports packet priority trust based on interface, including:

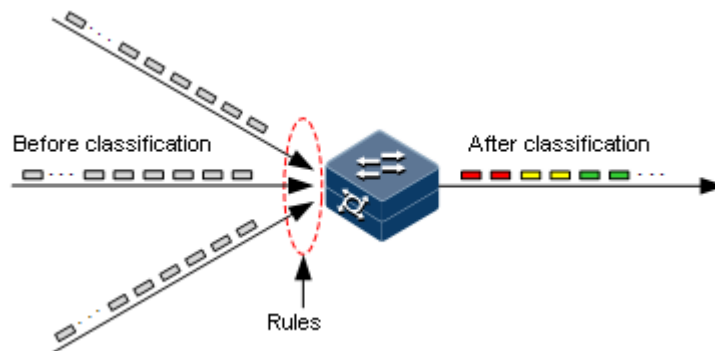
- Differentiated Services Code Point (DSCP) priority
- Class of Service (CoS) priority
- ToS priority

8.1.3 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 Gazelle S1512i-PWR supports traffic classification based on ToS priority, DSCP, CoS over IP packets, and based on Access Control List (ACL) rules and VLAN ID. The traffic classification procedure is shown in Figure 8-1.

Figure 8-1 Traffic classification



IP precedence and DSCP

Figure 8-2 shows the structure of the IP packet header. The header 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 8-3 shows the structure of ToS and DSCP.

Figure 8-2 Structure of the IP packet header

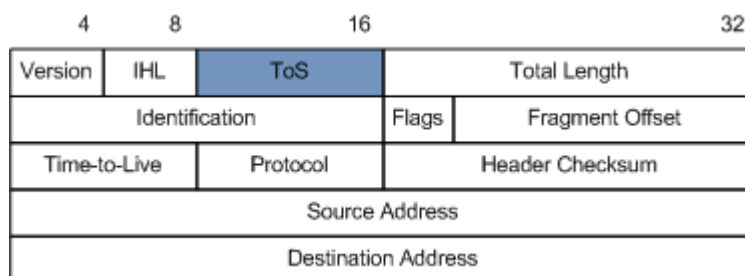
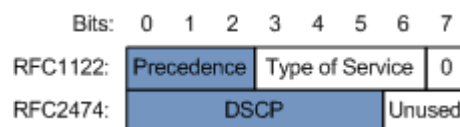


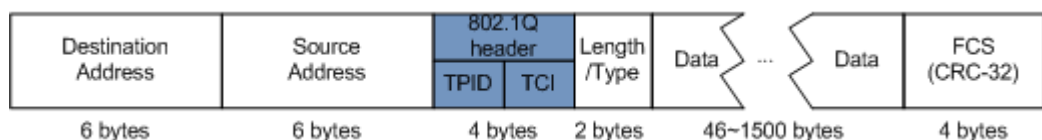
Figure 8-3 Structures of ToS priority and DSCP



CoS

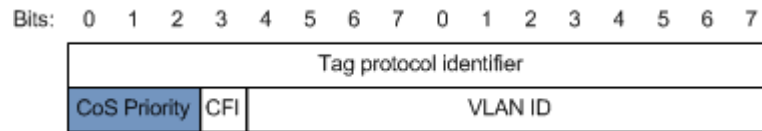
IEEE802.1Q-based VLAN packets are modifications of Ethernet packets. A 4-byte 802.1Q header is added between the source MAC address and protocol type, as shown in Figure 8-4. The 802.1Q header consists of a 2-byte Tag Protocol Identifier (TPID, valuing 0x8100) filed and a 2-byte Tag Control Information (TCI) field.

Figure 8-4 Structure of a VLAN packet



The first 3 bits of the TCI field represent the CoS, which ranges from 0 to 7, as shown in Figure 8-5. CoS is used to guarantee QoS only on the Layer 2 network.

Figure 8-5 Structure of CoS



8.1.4 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 Gazelle S1512i-PWR supports rate limiting based on traffic policy in the ingress direction on the interface.

The Gazelle S1512i-PWR supports using token buckets for rate limiting. It supports two modes: single token bucket and double token buckets.

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 Gazelle S1512i-PWR 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 services according to remarking information.

The Gazelle S1512i-PWR 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, including the following indexes about packets or bytes matching the traffic class: the number of passing packets, number of passing bytes, number of discarded packets, and number of discarded bytes.

Traffic statistics is not a QoS control measure, but can be used in combination with other QoS actions to improve network supervision.

8.1.5 Priority mapping

Priority mapping refers to sending packets to different queues with different local priorities according to preconfigured mapping from external priority to local priority. Therefore, packets in different queues can be scheduled on the egress interface.

The Gazelle S1512i-PWR supports performing priority mapping based on DSCP of IP packets or the 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 DSCP or CoS to local priority of the Gazelle S1512i-PWR is listed in Table 8-1 and Table 8-2.

Table 8-1 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 packet priority with internal meaning assigned by the Gazelle S1512i-PWR and is the priority corresponding to queue in QoS queue scheduling.

Local priority ranges from 0 to 7. Each interface of the Gazelle S1512i-PWR 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 8-2.

Table 8-2 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

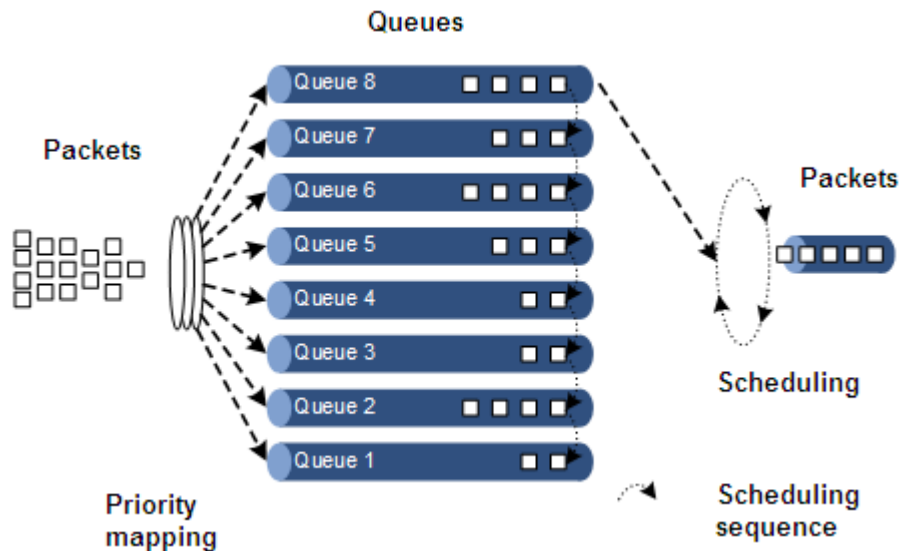
8.1.6 Queue scheduling

Queue scheduling is performed when delay-sensitive services need better QoS services than delay-insensitive services and when the network is congested sometimes.

Queue scheduling adopts different scheduling algorithms to send packets in a queue. Scheduling algorithms supported by the Gazelle S1512i-PWR 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.

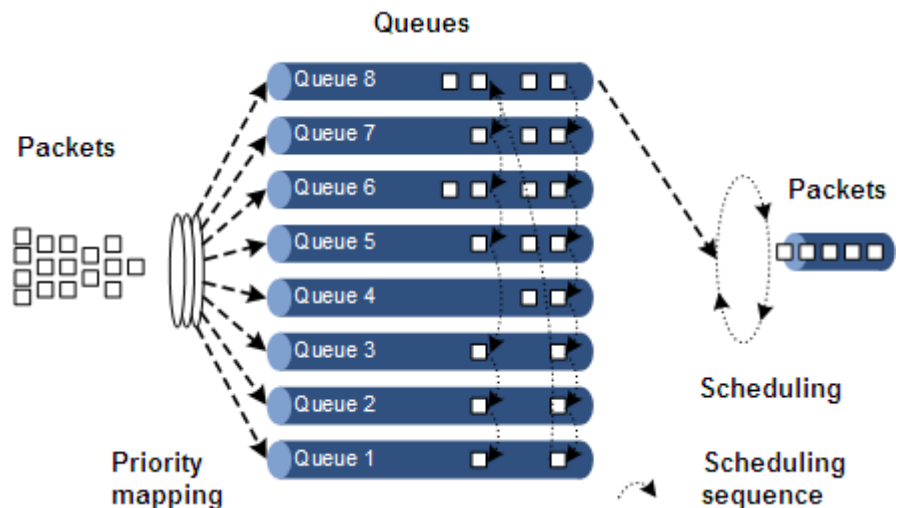
- SP: the Gazelle S1512i-PWR strictly schedules packets in a descending order of priority. Packets with lower priority cannot be scheduled until packets with higher priority are scheduled, as shown in Figure 8-6.

Figure 8-6 SP scheduling



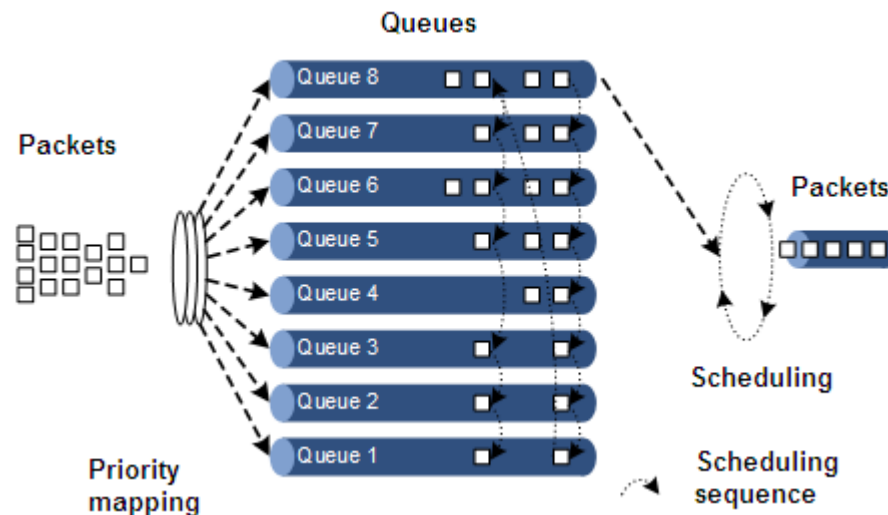
- WRR: on the basis of scheduling packets in a polling manner according to the priority, the Gazelle S1512i-PWR schedules packets according to the weight (based on byte) of the queue, as shown in Figure 8-7.

Figure 8-7 WRR scheduling



- DRR: similar with WRR, on the basis of scheduling packets in a polling manner according to the scheduling sequence, the Gazelle S1512i-PWR schedules packets according to the weight of the queue (based on packet), as shown in Figure 8-8.

Figure 8-8 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.

8.1.7 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 relieve 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 removed.

This Tail-Drop policy may cause TCP global synchronization, making network traffic change intermittently between high 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.

8.1.8 Rate limiting based on interface and VLAN

The Gazelle S1512i-PWR supports rate limiting based on traffic policy, interface, or VLAN, and interface+VLAN. Similar to rate limiting based on traffic policy, the Gazelle S1512i-PWR discards the excess traffic.

8.1.9 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 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. 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 Gazelle S1512i-PWR 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 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 Gazelle S1512i-PWR is in color-aware status, in which it can identify whether the ingress flow is marked with color. If disabled with color-aware, the Gazelle S1512i-PWR 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.

8.2 Configuring priority

8.2.1 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 traffic classification and traffic policy. After being configured to priority trust mode, the Gazelle S1512i-PWR processes packets according to their priorities and provides services accordingly.

Specifying 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 Gazelle S1512i-PWR will conduct queue scheduling according to local priority of packets. Generally, IP packets need to be configured with mapping from IP precedence/DSCP and local priority; while VLAN packets need to be configured with mapping from CoS to local priority.

Prerequisite

N/A

8.2.2 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 8-3.
Mapping from DSCP to local priority	See Table 8-4.
Mapping from ToS to local priority and color	See Table 8-5.
Interface priority	0

Table 8-3 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 8-4 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 8-5 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)

8.2.3 Configuring types of priorities trusted by interface

Configure types of priorities trusted by interface for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/port)#mls qos trust { cos dscp port- priority }</code>	Configure types of priorities trusted by interface. CoS priority exists in the header of 802.1q packets. When it is used, the interface type must be Trunk Tunnel.
4	<code>Raisecom(config- gigaethernet1/1/port)#mls qos priority <i>portpri-value</i></code>	Configure the interface priority.

8.2.4 Configuring mapping from CoS to local priority and color

Configure the mapping from CoS to local priority and color for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mls qos mapping cos-to-local-priority <i>profile-id</i></code>	Create a profile of mapping from CoS to local priority and color, and enter cos-to-pri configuration mode.
3	<code>Raisecom(cos-to-pri)#cos <i>cos- value to local-priority</i> <i>localpri-value</i> [color { green red yellow }]</code>	(Optional) modify the profile of mapping from CoS to local priority and color.

Step	Command	Description
4	Raisecom(cos-to-pri)# exit Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
5	Raisecom(config-gigaethernet1/1/port)# mls qos cos-to-local-priority <i>profile-id</i>	Configure the profile of mapping from CoS to local priority and color.

8.2.5 Configuring mapping from DSCP to local priority and color

Configure the mapping from DSCP to local priority and color for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# mls qos mapping dscp-to-local-priority <i>profile-id</i>	Create a profile of mapping from DSCP to local priority and color, and enter dscp-to-pri configuration mode.
3	Raisecom(dscp-to-pri)# dscp <i>dscp-value to local-priority localpri-value</i> [color { green red yellow }]	(Optional) modify the profile of mapping from DSCP to local priority and color.
4	Raisecom(dscp-to-pri)# exit Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
5	Raisecom(config-gigaethernet1/1/port)# mls qos dscp-to-local-priority <i>profile-id</i>	Configure the profile of mapping from DSCP to local priority and color.

8.2.6 Configuring DSCP mutation

Configure DSCP mutation for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# mls qos mapping dscp-mutation <i>profile-id</i>	Create a DSCP mutation mapping profile, and enter dscp mutation configuration mode.
3	Raisecom(dscp-mutation)# dscp <i>dscp-value to new-dscp newdscp-value</i>	(Optional) modify the DSCP mutation profile.
4	Raisecom(dscp-mutation)# exit Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.

Step	Command	Description
5	Raisecom(config-gigaetherne ^t 1/1/port)#m ^l s qos dscp-m ^u tation <i>profile-id</i>	Apply the DSCP mutation profile to the interface.

8.2.7 Configuring CoS remarking

Configure CoS remarking for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaetherne ^t 1/1/1)#m ^l s qos cos- remark-mapping enable Raisecom(config-gigaetherne ^t 1/1/1)# exit	Enable CoS remarking on the interface.
4	Raisecom(config)#m ^l s qos mapping cos-remark <i>profile-id</i>	Create a CoS remarking profile, and enter cos-remark configuration mode.
5	Raisecom(cos-remark)# local-priority <i>localpri-value to cos newcos-value</i>	Modify the CoS remarking profile.
6	Raisecom(dscp-remark)# exit Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
7	Raisecom(config-gigaetherne ^t 1/1/port)#m ^l s qos cos-remark <i>profile-id</i>	Apply the CoS remarking profile to the interface.
8	Raisecom(config-gigaetherne ^t 1/1/port)#m ^l s qos cos- remark-mapping enable dei { enable disable }	Enable the mapping from local priority to CoS.

8.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show m^ls qos interface [<i>interface-type interface-number</i>]	Show QoS priority, trust mode, and scheduling mode on the interface.
2	Raisecom# show m^ls qos mapping cos-to-local-priority [default <i>profile-id</i>]	Show information about mapping from CoS to local priority and color profile.

No.	Command	Description
3	<code>Raisecom#show mls qos mapping dscp-to-local-priority [default profile-id]</code>	Show information about mapping from DSCP to local priority and color profile.
4	<code>Raisecom#show mls qos mapping dscp-mutation [profile-id]</code>	Show mapping information about the DHCP mutation profile
5	<code>Raisecom#show mls qos mapping cos-remark [default profile-id]</code>	Show information about the CoS remarking profile.

8.3 Configuring congestion management

8.3.1 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 current service conditions and customer requirements.

Prerequisite

Enable global QoS.

8.3.2 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"> • WRR weight for scheduling 8 queues is 1. • DRR weight for scheduling 8 queues is 81.

8.3.3 Configuring SP queue scheduling

Configure SP queue scheduling for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/port)#mls qos queue scheduler sp	Configure queue scheduling mode as SP on the interface.

8.3.4 Configuring WRR or SP+WRR queue scheduling

Configure WRR or SP+WRR for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/port)#mls qos queue scheduler wrr <i>weigh1 weight2 weight3...weight8</i>	Configure queue scheduling mode as WRR on the interface and the weight for each queue.

8.3.5 Configuring DRR or SP+DRR queue scheduling

Configure DRR or SP+DRR for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/port)#mls qos queue scheduler drr <i>weight1weight2weight3...weight8</i>	Configure queue scheduling mode as DRR, and configure weight for various queues. Conduct SP scheduling when priority of a queue is 0.

8.3.6 Configuring queue bandwidth guarantee

Configure queue bandwidth guarantee for the Gazelle S1512i-PWR as below.

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

Step	Command	Description
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/port)#mls qos queue <i>queue-id shaping cir cir pir pir</i>	(Optional) configure queue bandwidth guarantee on the interface and configure burst size.

8.3.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show mls qos queue interface <i>interface-type interface-number</i>	Show the weight of queues on the interface.
2	Raisecom#show mls qos queue statistics interface <i>interface-type interface-number</i>	Show queue statistics on the interface.
3	Raisecom#show mls qos queue shaping interface <i>interface-type interface-list</i>	Show queue shaping on the interface.

8.4 Configuring congestion avoidance

8.4.1 Preparing for configurations

Scenario

To avoid network congestion and implement TCP global synchronization, you can configure congestion avoidance to adjust network flow and relieve network overload.

The Gazelle S1512i-PWR conducts congestion avoidance based on SRED.

Prerequisite

Enable global QoS.

8.4.2 Default configurations of congestion avoidance

Default configurations of congestion avoidance are as below.

Function	Default value
Global SRED status	Enable

8.4.3 Configuring SRED

Configure SRED for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mls qos sred profile profile-id</code>	Create a SRED profile, and enter SRED configuration mode.
3	<code>Raisecom(sred)#sred [color { red yellow }] start-drop-threshold start-drop value drop-probability drop probability value</code>	Modify the SRED profile.
4	<code>Raisecom(sred)#exit</code> <code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
5	<code>Raisecom(config-gigaethernet1/1/1)#mls qos queue queue-id sred profile-id</code>	Apply the SRED profile to the interface.

8.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show mls qos sred profile [profile-list]</code>	Show information about the SRED profile.

8.5 Configuring traffic classification and traffic policy

8.5.1 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 Gazelle S1512i-PWR 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 Gazelle S1512i-PWR 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.

8.5.2 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

8.5.3 Creating traffic class

Create a traffic class for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#class-map class-map-name [match-all match-any]</code>	Create a traffic class and enter traffic classification cmap configuration mode.
3	<code>Raisecom(config- cmap)#description string</code>	(Optional) configure the description of traffic class.

8.5.4 Configuring traffic classification rules

Configure traffic classification rules for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#class-map class-map-name [match-all match-any]</code>	Create a traffic class and enter traffic classification cmap configuration mode.
3	<code>Raisecom(config-cmap)#match access-list { access-list name } Raisecom(config-cmap)#exit</code>	(Optional) configure the traffic class based on ACL rule. The ACL rule must be defined first and the type must be permit .
4	<code>Raisecom(config-cmap)#match cos cos-value</code>	(Optional) configure the traffic class based on CoS of packets.
5	<code>Raisecom(config-cmap)#match inner-vlan inner-vlan-value</code>	(Optional) configure the traffic class based on inner VLAN of packets.
6	<code>Raisecom(config-cmap)#match vlan vlan-value</code>	(Optional) configure the traffic class based on VLAN 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 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 traffic classification; in other words, the **match** parameter must be configured.
- For the traffic class quoted by traffic policy, do not modify traffic classification rule; in other words, do not modify the **match** parameter of traffic classification.

8.5.5 Creating rate limiting rule and shapping rule

To limit the 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 Gazelle S1512i-PWR 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</code>	Create a traffic policer profile, and enter traffic-policer configuration mode.
3	<code>Raisecom(traffic-policer)#cir cir cbs cbs</code>	(Optional) configure parameters of the token bucket in flow mode. <div style="text-align: right;">  <h3>Note</h3> <p>The token bucket in flow mode is the single token bucket, and can be configured with actions for red and green packets only.</p> </div>
4	<code>Raisecom(traffic-policer)#cir cir cbs cbs ebs ebs</code>	(Optional) configure parameters of the token bucket in RFC2697 mode.
5	<code>Raisecom(traffic-policer)#cir cir cbs cbs pir pir pbs pbs</code>	(Optional) configure parameters of the token bucket in RFC2698 mode.
6	<code>Raisecom(traffic-policer)#cir cir cbs cbs eir eir ebs ebs [coupling]</code>	(Optional) configure parameters of the token bucket in RFC4115 mode or parameters of the MEF token bucket.

Step	Command	Description
7	Raisecom(traffic-policer)# drop-color red	(Optional) configure the token bucket to discard red packets.
8	Raisecom(traffic-policer)# recolor { green-recolor red red-recolor green }	(Optional) configure packet recoloring.
9	Raisecom(traffic-policer)# set-cos { green cos red cos }	(Optional) configure the mapping from packets color to CoS.
10	Raisecom(traffic-policer)# set-dscp { green green-value red red-value }	(Optional) configure the mapping from packets color to DSCP.
11	Raisecom(traffic-policer)# set-pri { green green-value red red-value }	(Optional) configure the mapping from packets color to local priority.

8.5.6 Creating traffic policy

Create a traffic policy for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# policy-map <i>policy-map-name</i>	Create a traffic policy, and enter traffic policy pmap configuration mode.
3	Raisecom(config-pmap)# description <i>string</i>	(Optional) configure the description of traffic policy.

8.5.7 Defining traffic policy mapping




Note

Define one or more defined traffic classes to one traffic policy.

Define traffic policy mapping for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# policy-map <i>policy-map-name</i>	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>	<p>Bind the traffic class with a traffic policy. The traffic policy is applied to the packets matching the traffic class.</p> <p> Note At least one rule is required for traffic classification to bind traffic policy; otherwise the binding will fail.</p>

8.5.8 Defining traffic policy operation



Define different operations to different flows in policy.

Define a traffic policy operation for the Gazelle S1512i-PWR 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>	<p>Bind the traffic class with a traffic policy. The traffic policy is applied to the packets matching the traffic class.</p> <p> Note At least one rule is necessary for traffic classification to bind traffic policy; otherwise the binding will fail.</p>
4	<code>Raisecom(config-pmap-c)#police policer-name</code>	<p>(Optional) apply the token bucket on traffic policy and conduct rate limiting and shaping.</p> <p> Note The token bucket needs to be created in advance and be configured with rate limiting and shaping rules. Otherwise, the operation will fail.</p>
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 <i>cos-value</i> dscp <i>dscp-value</i> local-priority <i>value</i> }</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 <i>mirror-id</i></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 matched traffic class.

8.5.9 Applying traffic policy to interface

Apply traffic policy to the interface for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/port)#service-policy ingress <i>policy-map-name</i></code>	Apply the configured traffic policy in batches to the ingress direction of the interface.

8.5.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show service-policy statistics interface <i>interface-type interface-number</i> ingress [class-map <i>class-map-name</i>]</code>	Show statistics on applied traffic policy.
2	<code>Raisecom#show service-policy interface [<i>interface-type interface-number</i>] [ingress]</code>	Show information about the applied traffic policy.
3	<code>Raisecom#show class-map [<i>class-map-name</i>]</code>	Show information about the traffic class.
4	<code>Raisecom#show policy-map [<i>policy-map-name</i>]</code>	Show information about traffic policy.
5	<code>Raisecom#show policy-map [<i>policy-map-name</i>] [class <i>class-map-name</i>]</code>	Show information about the traffic class in traffic policy.

No.	Command	Description
6	Raisecom# show mls qos policer [<i>policer-name</i>]	Show information about the assigned token bucket (rate limiting and shaping).

8.5.11 Maintenance

Maintain the Gazelle S1512i-PWR as below.

Command	Description
Raisecom(config)# clear service-policy statistics interface <i>interface-type interface-number</i> ingress	Clear statistics on QoS packets.

8.6 Configuring rate limiting

8.6.1 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

8.6.2 Configuring rate limiting based on interface

Configure rate limiting based on interface for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config- gigaethernet1/1/port)# rate-limit ingress cir <i>cir-value</i> cbs <i>cbs-value</i>	Configure rate limiting based on interface.



- 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 on packet loss of the ingress interface.

8.6.3 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</i> <i>interface-number</i> [<i>ingress</i> <i>egress</i>]</code>	

8.7 Configuration examples

8.7.1 Example for configuring congestion management

Networking requirements

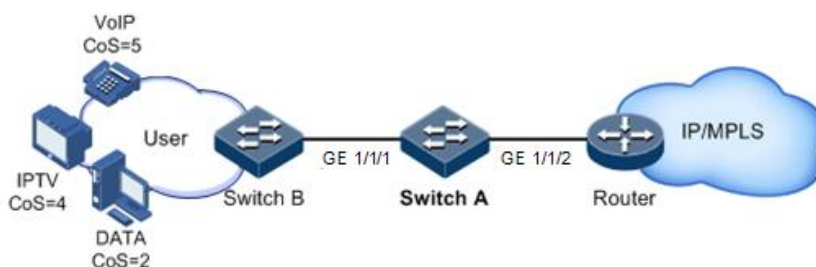
As shown in Figure 8-9, the user use voice, video and data services.

CoS of voice service is 5. CoS of video service is 4. 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 services, perform SP schedule to grant high priority.
- For video services, perform WRR schedule, with weight of 50.
- For data services, perform WRR schedule, with weight of 20.

Figure 8-9 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              0
0
```

```

gigaethernet1/1/2    cos    0          1          0          0
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)      7(G)      1      localpri(color) :0(G)  1(G)  2(G)  3(G)  5(G)
6(G)

```

Use the following command to show configurations of queue scheduling on the interface.

```

Raisecom#show mls qos queue interface gigaethernet 1/1/1
gigaethernet1/1/1
Queue  Weight(WRR)
-----
1      1
2      1
3      20
4      1
5      1
6      50
7      0
8      0

```

8.7.2 Example for configuring rate limiting based on traffic policy

Networking requirements

As show in Figure 8-10, User A, User B, and User C respectively belong to VLAN 1, VLAN 2, and VLAN 3, and are connected to the Gazelle S1512i-PWR by Switch A, Switch B, and Switch C.

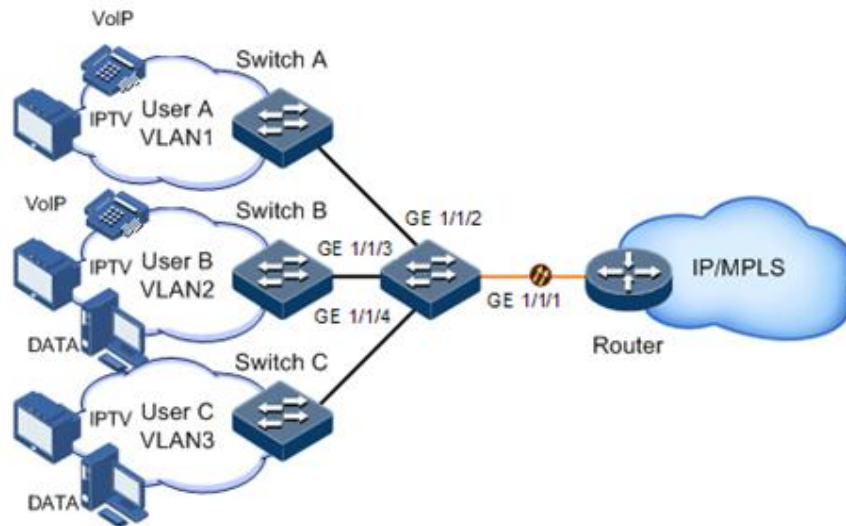
User A uses voice and video services, User B uses voice, video and data services, and User C uses video and data services.

According to service requirements, make rules as below.

- For User A, provide 25 Mbit/s guaranteed bandwidth, permit burst flow of 100 Kbytes, discard excess flow.

- For User B, provide 35 Mbit/s guaranteed bandwidth, permit burst flow of 100 Kbytes, discard excess flow.
- For User C, provide 30 Mbit/s guaranteed bandwidth, permit burst flow of 100 Kbytes, discard excess flow.

Figure 8-10 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
```

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 gig Ethernet 1/1/1
Raisecom(config-gig Ethernet1/1/1)#service-policy ingress usera
Raisecom(config-gig Ethernet1/1/1)#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 gig Ethernet 1/1/2
Raisecom(config-gig Ethernet1/1/2)#service-policy ingress userb
Raisecom(config-gig Ethernet1/1/2)#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 gig Ethernet 1/1/3
Raisecom(config-gig Ethernet1/1/3)#service-policy userc ingress 4
Raisecom(config-gig Ethernet1/1/3)#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 userc (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
```

8.7.3 Example for configuring rate limiting based on interface

Networking requirements

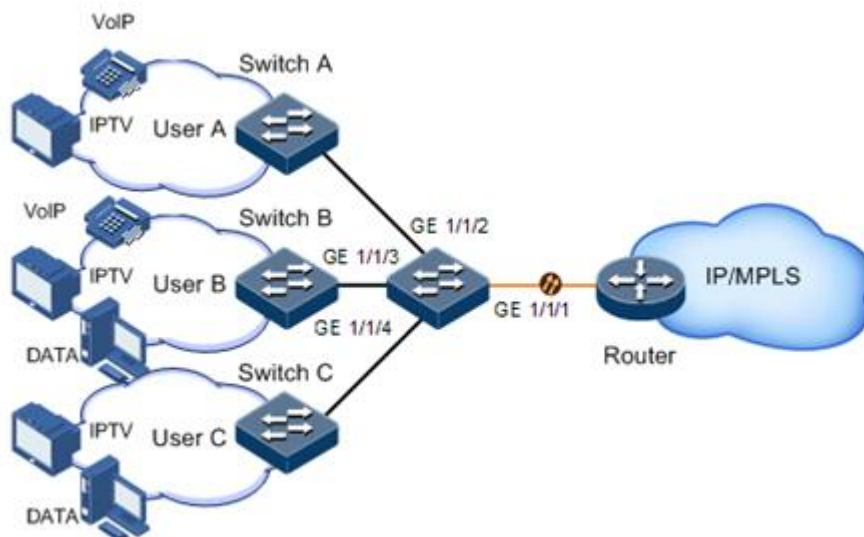
As shown in Figure 8-11, User A, User B, and User C are respectively connected to the Gazelle S1512i-PWR by Switch A, Switch B, and Switch C.

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.

- For User A, provide 25 Mbit/s guaranteed bandwidth, permit burst flow of 100 Kbytes, discard excess flow.
- For User B, provide 35 Mbit/s guaranteed bandwidth, permit burst flow of 100 Kbytes, discard excess flow.
- For User C, provide 30 Mbit/s guaranteed bandwidth, permit burst flow of 100 Kbytes, discard excess flow.

Figure 8-11 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 gigabitEthernet 1/1/3
Raisecom(config-gigabitEthernet1/1/3)#rate-limit ingress cir 30000 cbs 100
Raisecom(config-gigabitEthernet1/1/3)#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)
-----
gigabitEthernet1/1/1  ingress  25000          100          25024
101
    
```

gigaethernet1/1/2 101	ingress	30000	100	30016
gigaethernet1/1/3 101	ingress	30000	100	30016

9 Multicast

This chapter describes principles and configuration procedures of multicast, and provides related configuration examples, including the following sections:

- Introduction
- Basic functions of Layer 2 multicast
- IGMP Snooping
- IGMP MVR
- IGMP filtering
- MLD
- IGMP Querier
- Multicast VLAN copy

9.1 Introduction

With the continuous development of the Internet, more and more various interactive data, voice, and video services 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 have higher requirements for network bandwidth, data security, and the paid feature. Traditional unicast and broadcast cannot meet these requirements well but multicast can meet them timely.

Multicast is a point-to-multipoint data transmission method. The method can effectively solve point-to-multipoint problems. During transmission of packets on the network, multicast can save network resources and improve data security.

Comparison among unicast, broadcast, and multicast

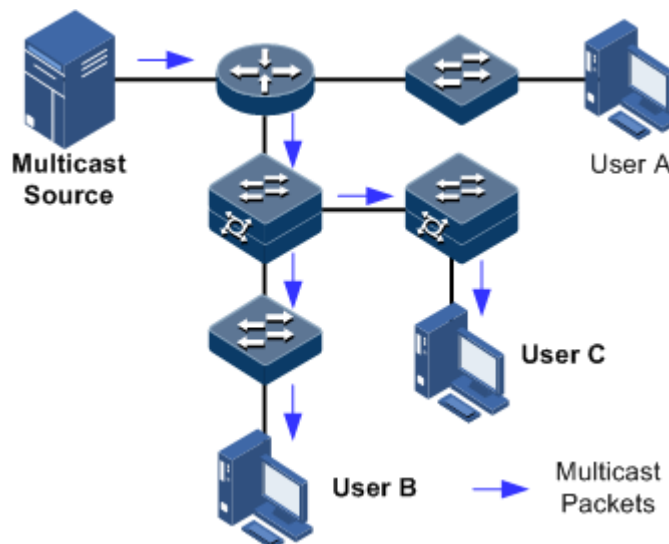
Multicast is a packet transmission method, which is parallel with unicast and broadcast.

- Unicast: the system establishes a data transmission path for each user who needs the data, and sends separate copied data for them. Through unicast, the amount of data 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 suitable to large-scale data transmission.

- Broadcast: the system sends data to all users regardless of whether they need or not, so all users will receive data. Through broadcast, the data source delivers data to all users in the network segment, which cannot guarantee data security and paid service. In addition, when the number of users who require the data decreases, the utilization of network resources will be low, and the bandwidth will be wasted seriously.
- Multicast: when some users on 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 9-1, assume that User B and User C need data, you can use multicast transmission to combine User B and User C into a receiver set. Then the data source just needs to send one copy of data. Each switch on the network will establish their multicast forwarding table according to IGMP packets, and finally transmits the data to the actual receivers User B and User C.

Figure 9-1 Multicast transmission networking



In summary, unicast is used on the sparsely-populated network while broadcast is used on densely-populated network. When the number of users on the network is uncertain, unicast and broadcast will be less efficient. When the number of users are doubled and redoubled, the multicast mode does not need to increase backbone bandwidth, but sends data to users in need. These advantages of multicast make itself a hotspot in study of the current network technology.

Advantages and applications of multicast

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

- Improve efficiency: reduce network traffic, and relieve server and CPU load.
- Optimize performance: reduce excess traffic and guarantee data security.
- Support distributed applications: solve the problem of point-point data transmission.

Multicast 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 the 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 the 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 packets. A multicast source can send data to multiple multicast groups. Multiple multicast sources can send data to a multicast group.

- Multicast router

A multicast router is a router that supports Layer 3 multicast. The multicast router supports multicast routing, manages multicast packet forwarding, and manages multicast group members to the edge network segment connected with users.

- Router interface

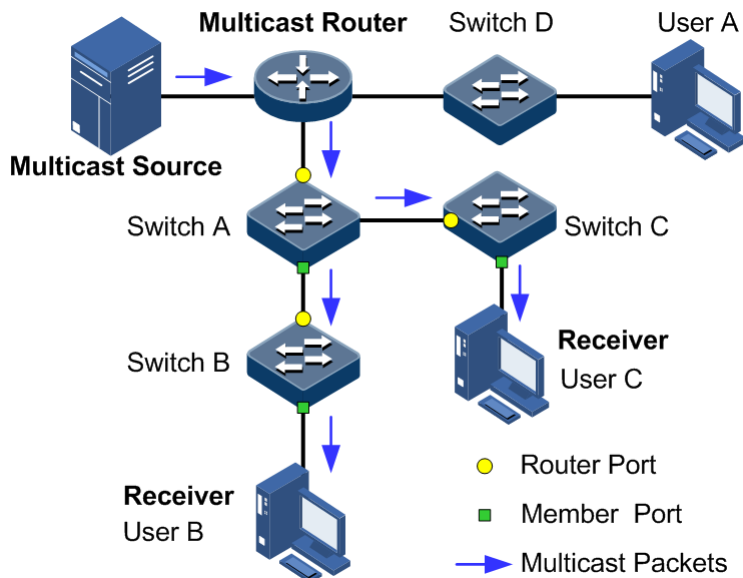
A router interface refers to the interface toward the multicast router between a multicast router and a host. The Gazelle S1512i-PWR receives multicast packets from this interface.

- Member interface

Known as the receiving interface, a member interface is the interface towards the host between the multicast router and the host. The Gazelle S1512i-PWR sends multicast packets from this interface.

Figure 9-2 shows basic concepts in multicast.

Figure 9-2 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

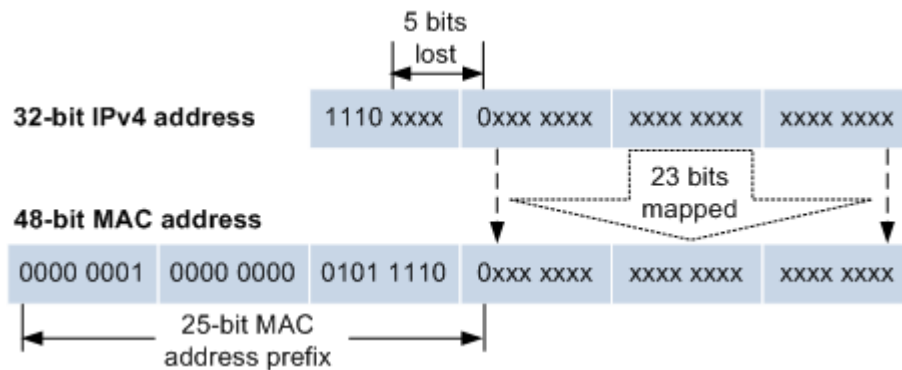
When the Ethernet transmits unicast IP packets, it uses the MAC address of the receiver as the destination MAC address. However, when multicast packets are transmitted, the destination is no longer a specific receiver, but a group with an uncertain number of members, so the Ethernet needs to use the multicast MAC address.

The multicast MAC address identifies receivers of the same multicast group at the link layer.

According to IANA, the first 24 bits of the multicast MAC address are 0x01005E, bit 25 is fixed at 0, and the last 23 bits correspond to the last 23 bits of the IPv4 multicast address.

Figure 9-3 shows mapping between the IPv4 multicast address and MAC address.

Figure 9-3 Mapping between IPv4 multicast address and multicast MAC address



The first 4 bits of the IP multicast address are 1110, indicating multicast. In the last 28 bits, only 23 bits are mapped into the multicast MAC address, and the missing 5 bits make 32 IP multicast addresses mapped into the same multicast MAC address. Therefore, at Layer 2, the Gazelle S1512i-PWR may receive extra data besides the IPv4 multicast group, and these extra multicast data needs to be filtered by the upper layer on the Gazelle S1512i-PWR.

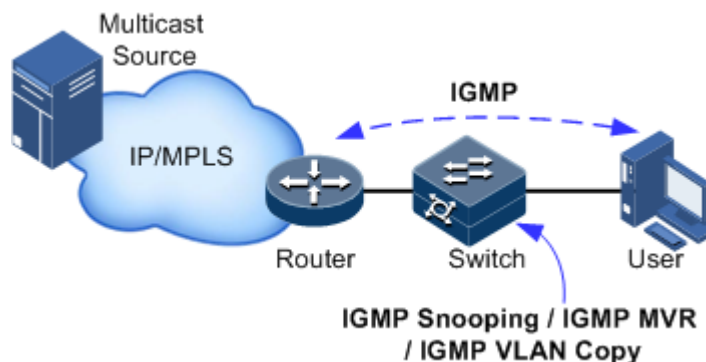
Basis of multicast protocol

To implement a complete set of multicast services, you need to deploy a variety of multicast protocols in various positions of the network and make them cooperate with each other.

Typically, IP multicast working at the network layer is called Layer 3 multicast, so the corresponding multicast protocol is called the Layer 3 multicast protocol, including Internet Group Management Protocol (IGMP). IP multicast working at the data link layer is called Layer 2 multicast, so the corresponding multicast protocol is called the Layer 2 multicast protocol, including Internet Group Management Protocol (IGMP) Snooping.

Figure 9-4 shows operating of IGMP and Layer 2 multicast features.

Figure 9-4 Operating positions of IGMP and Layer 2 multicast features



IGMP, a protocol in the TCP/IP protocol suite, is used to manage 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, and include 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 decides which multicast group packets to receive.
- The multicast router sends Query packets periodically, and receives Report packets and Leave packets from hosts to learn the multicast group members in connected network segment. The multicast data will be forwarded to the network 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 later version is fully compatible with the earlier version. Currently the most widely used version is IGMPv2 while the Leave packet does not support IGMPv1.

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 forward multicast data at Layer 2 and suppress multicast data diffusion at Layer 2.

Supported multicast features

The Gazelle S1512i-PWR supports the following multicast features:

- Basic functions of IGMP
- IGMP Snooping
- IGMP Multicast VLAN Registration (MVR)
- IGMP filtering
- VLAN copy



Note

- IGMP Snooping and IGMP MVR can be enabled concurrently, but IGMP Snooping works with higher priority. IGMP VLAN copy and IGMP Snooping cannot be enabled concurrently. Multicast VLAN copy and IGMP MVR cannot be enabled concurrently.
- The Gazelle S1512i-PWR supports IGMPv1, IGMPv2, and IGMPv3.

9.2 Basic functions of Layer 2 multicast

9.2.1 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 Gazelle S1512i-PWR 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

Only IGMPv2 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.

9.2.2 Preparing for configurations

Scenario

Basic functions of Layer 2 multicast provide common features of Layer 2 multicast, and must be used on the Gazelle S1512i-PWR enabled with IGMP Snooping or IGMP MVR.

Prerequisite

- Create VLANs.
- Add related interfaces to VLANs.

9.2.3 Default configurations of basic functions of Layer 2 multicast

Default configurations of basic functions of Layer 2 multicast are as below.

Function	Default value
IGMP immediate leave status	Disable
Aging time of multicast entries	260s
Interface IGMP ring network forwarding status	Disable

9.2.4 Configuring basic functions of Layer 2 multicast

Configure basic functions of Layer 2 multicast for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#igmp mrouter <i>vlan vlan-id interface-type</i> <i>interface-number</i>	(Optional) configure the multicast router interface.
3	Raisecom(config)#igmp immediate-leave { <i>interface-type interface-number [vlan vlan-list] based mac-address</i> }	(Optional) configure immediate leave.
4	Raisecom(config)#igmp report-suppression	(Optional) enable Report suppression.
5	Raisecom(config)#igmp ring <i>interface-type interface-number</i>	(Optional) enable IGMP ring network forwarding on the interface.
6	Raisecom(config)#igmp member-timeout { <i>seconds</i> infinite }	(Optional) configure the aging time of IGMP members.

9.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show igmp mrouter	Show configurations of the multicast router interface.
2	Raisecom# show igmp immediate-leave [<i>interface-type interface-number</i>]	Show configuration of immediate leave on Layer 2 multicast.
3	Raisecom# show igmp statistics [<i>interface-type interface-number</i>]	Show Layer 2 multicast statistics.

9.2.6 Maintenance

Maintain the Gazelle S1512i-PWR as below.

Command	Description
Raisecom(config)# clear igmp statistics [<i>interface-type interface-number</i>]	Clear statistics on Layer 2 multicast IGMP.
Raisecom(config)# no igmp member <i>interface-type interface-number</i>	Delete a specified multicast entry.

9.3 IGMP Snooping

9.3.1 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 Gazelle S1512i-PWR to monitor IGMP sessions between the host and multicast router. When monitoring the IGMP Report packet from the host to a group, the Gazelle S1512i-PWR will add host-related interface to the forwarding entry of this group. Similarly, when a forwarding entry reaches the aging time, the Gazelle S1512i-PWR will delete host-related interface from the forwarding table.

IGMP Snooping forwards multicast data through Layer 2 multicast entry. When receiving multicast data, the Gazelle S1512i-PWR will forward them directly according to the corresponding Rx interface of the multicast entry, instead of flooding them to all interfaces, to save bandwidth of the Gazelle S1512i-PWR effectively.

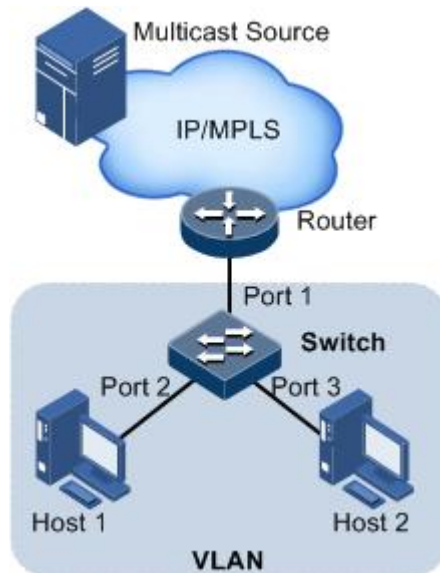
IGMP Snooping establishes a Layer 2 multicast forwarding table, of which entries can be learnt dynamically or configured manually.

9.3.2 Preparing for configurations

Scenario

As shown in Figure 9-5, 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 9-5 IGMP Snooping networking



Prerequisite

- Disable multicast VLAN copy on the Gazelle S1512i-PWR.
- Create VLANs.
- Add related interfaces to the VLANs.

9.3.3 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

9.3.4 Configuring IGMP Snooping

Configure IGMP Snooping for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#igmp snooping</code>	Enable global IGMP Snooping.
3	<code>Raisecom(config)#igmp member timeout { seconds infinite }</code>	(Optional) configure the aging time of IGMP members.
4	<code>Raisecom(config)#igmp snooping mrouter vlan <i>vlan-id</i> priority <i>priority-number</i></code>	(Optional) configure the CoS priority of the IGMP route VLAN.

9.3.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show igmp snooping [vlan <i>vlan-list</i>]</code>	Show configurations of IGMP Snooping.
2	<code>Raisecom#show igmp snooping member [<i>interface-type interface-number</i> vlan <i>vlan-id</i>]</code>	Show information about multicast group members of IGMP Snooping.
3	<code>Raisecom#show igmp snooping vlan <i>vlan-id</i></code>	Show configurations of IGMP Snooping in the specified VLAN.
4	<code>Raisecom#show igmp snooping mrouter <i>vlan-priority</i></code>	Show the CoS priority of the IGMP router VLAN.

9.3.6 Example for applying multicast on ring network

Networking requirements

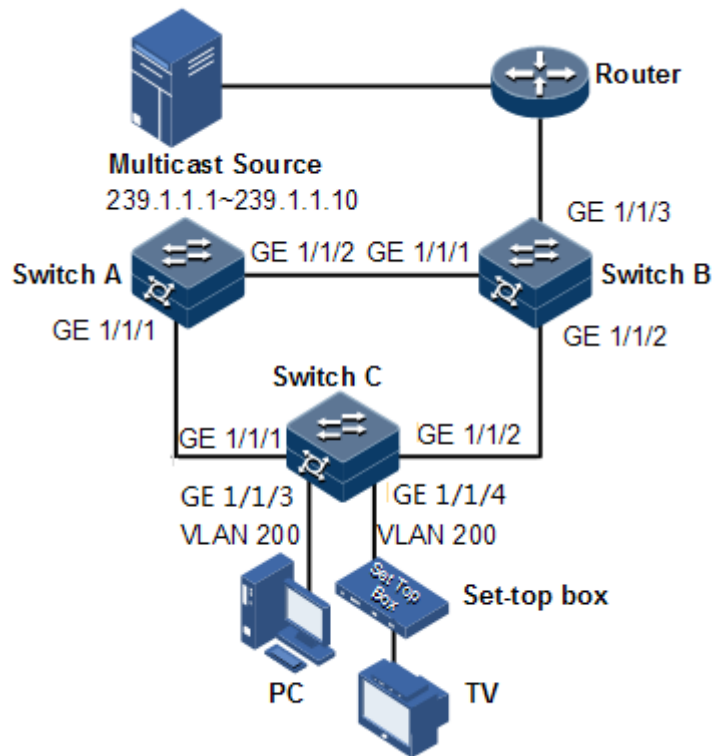
Configure IGMP ring forwarding on single Ethernet ring to make multicast service more stable and prevent multicast service from being disrupted by link failure.

As shown in Figure 9-6, 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. This networking does not affect the customer's on-demand multicast traffic whichever link fails on 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 9-6 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
```

Configure Switch B.

```
SwitchB(config)#igmp ring gigaethernet 1/1/1
SwitchB(config)#igmp ring gigaethernet 1/1/2
SwitchB(config)#igmp snooping
```

Configure Switch C.

```
SwitchC(config)#igmp ring gigaethernet 1/1/1
SwitchB(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.

9.4 IGMP MVR

9.4.1 Introduction

IGMP Multicast VLAN Registration (MVR) is multicast constraining mechanism running on Layer 2 devices, used for managing and controlling multicast group and implementing Layer 2 multicast.

IGMP MVR adds member interfaces belonging to different user VLAN on the switch to a multicast VLAN by configuring the multicast VLAN and makes users of different VLANs share one common multicast VLAN. In this case, the multicast data will be transmitted in only one multicast VLAN without being copied to each user VLAN, thus saving bandwidth. At the same time, multicast VLAN and user VLAN are completely isolated, thus enhancing security.

Both IGMP MVR and IGMP Snooping can implement Layer 2 multicast, but the difference is that the multicast VLAN in IGMP Snooping is the same as the customer VLAN while the multicast VLAN in IGMP MVR can be different from the customer VLAN.



Note

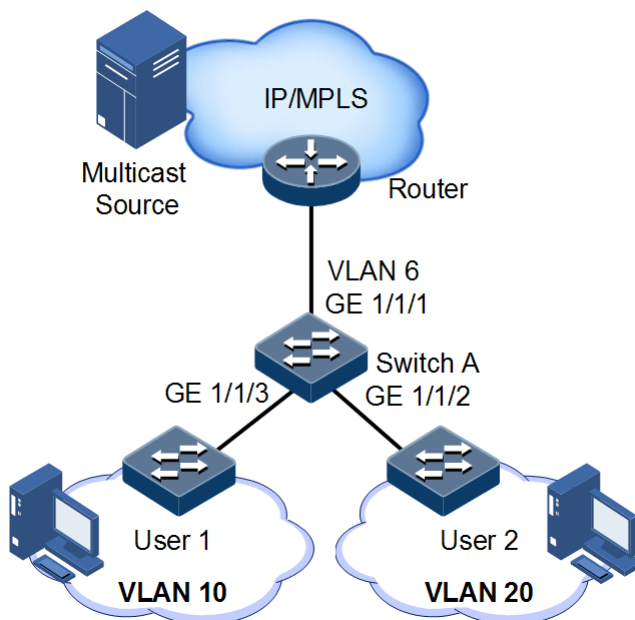
One switch can configure up to 10 multicast VLANs, at least one multicast VLAN and group addresses. The maximum number of supported multicast groups is 1024.

9.4.2 Preparing for configurations

Scenario

As shown in Figure 9-7, multiple users receive data from the multicast source. These users and the multicast router belong to different VLANs. Enable IGMP MVR on Switch A, and configure multicast VLAN. In this way, users in different VLANs can share a multicast VLAN to receive the same multicast data, and bandwidth waste is reduced.

Figure 9-7 IGMP MVR networking



Prerequisite

- Disable multicast VLAN copy.
- Create VLANs.
- Add related interfaces to VLANs.

9.4.3 Default configurations of IGMP MVR


Default configurations of IGMP 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

9.4.4 Configuring IGMP MVR

Configure IGMP MVR for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# igmp mvr	Enable global IGMP MVR.

Step	Command	Description
3	<pre>Raisecom(config)#igmp mvr mcast-vlan vlan-id group { start-ip-address [end-ip- address] any }</pre>	Configure the group address set for multicast VLAN.  Note 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	<pre>Raisecom(config)#interface interfacetype interfacenumber</pre>	Enter physical layer interface configuration mode.
5	<pre>Raisecom(config- gigaethernet1/1/port)#igmp mvr mcast-vlan vlan-id static ip-address</pre>	(Optional) configure static multicast members of MVR.
6	<pre>Raisecom(config- gigaethernet1/1/port)#igmp mvr user-vlan vlan-id</pre>	(Optional) configure the range for multicast inter-VLAN copy to take effect.

9.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<pre>Raisecom#show igmp mvr [interface- type interface-number]</pre>	Show configurations of IGMP MVR.
2	<pre>Raisecom#show igmp mvr members [interface-type interface-number user-vlan vlan-id]</pre>	Show information about multicast group members of IGMP MVR.
3	<pre>Raisecom#show igmp mvr vlan-group [mcast-vlan vlan-id]</pre>	Show multicast VLAN and its group address set.

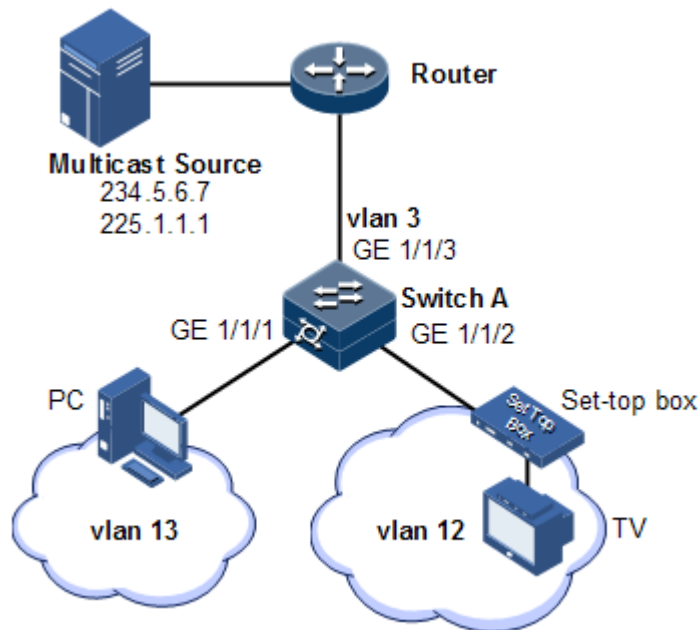
9.4.6 Example for configuring IGMP MVR

Networking requirements

As shown in Figure 9-8, 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 9-8 MVR networking



Configuration steps

Step 1 Create VLANs on Switch A and add interfaces to them.

```
Raisecom(config)#config
Raisecom(config)#creat 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 3
Raisecom(config-gigaethernet1/1/1)#switchport trunk untagged vlan 12,13
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
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 1/1/3
Raisecom(config-gigaethernet1/1/3)#switchport mode trunk
Raisecom(config-gigaethernet1/1/3)#switchport trunk native vlan 13
Raisecom(config-gigaethernet1/1/3)#switchport trunk untagged vlan 3
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)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#igmp mvr
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
Mcast-vlan   Start-group   End-group
vlan         Port           Age           Type
-----
3            225.1.1.1    225.1.1.1
3            234.5.6.7    234.5.6.7
```

9.5 IGMP filtering

9.5.1 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 the IGMP filtering profile to control the interface. One IGMP filtering 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 filtering profile is applied to the interface, the interface will discard the IGMP report packet from this group directly when receiving it and disallow the interface to receive this group of multicast data.

The IGMP filtering profile can be configured on an interface or interface+VLAN.

The IGMP filtering 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.

9.5.2 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 can also configure the maximum number of multicast groups jointed by users. IGMP Querier is generally used with IGMP Snooping or IGMP MVR.

Prerequisite

- Create VLANs.
- Add related interfaces to the VLANs.

9.5.3 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, with the largest group action of drop, no application filter profile

Function	Default value
IGMP filtering under interface+VLAN	No maximum group limit, with the largest group action of drop, no application filter profile

9.5.4 Enabling global IGMP filtering

Enable global IGMP filtering for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#igmp filter	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.

9.5.5 Configuring IGMP filtering profile

The IGMP filtering profile can be used to interface or interface+VLAN.

Configure the IGMP filtering profile for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#igmp filter profile profile-number	Create an IGMP filtering profile and enter Profile configuration mode.
3	Raisecom(config-igmp-profile)#{ permit deny }	Configure the IGMP filtering profile action.
4	Raisecom(config-igmp-profile)#range range-id start-ip-address [end-ip-address]	Configure the device to control IP multicast address access and range.
5	Raisecom(config-igmp-profile)#exit Raisecom(config)#interface interface-type interface-number	Enter physical layer interface configuration mode or LAG configuration mode.
6	Raisecom(config-gigaethernet1/1/1)#igmp filter profile profile-number [vlan vlan-list]	Configure the IGMP filtering profile on the physical interface or interface+VLAN.
	Raisecom(config-port-channel)#igmp filter profile profile-number [vlan vlan-list]	Configure the IGMP filtering profile on the LAG interface or interface+VLAN.



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.

9.5.6 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode or LAG configuration mode.
3	Raisecom(config-gigaetherne t1/1/port)#igmp filter max-groups <i>group-number</i> [vlan <i>vlan-list</i>]	Configure the maximum number of multicast groups to physical interface or interface+VLAN.
	Raisecom(config-port-channel) #igmp filter max- groups <i>group-number</i> [vlan <i>vlan-list</i>]	Configure the maximum number of multicast groups to LAG interface or interface+VLAN.
4	Raisecom(config-gigaetherne t1/1/port)#igmp filter max-groups action { drop replace } [vlan <i>vlan-list</i>]	(Optional) configure the action when the maximum number of multicast groups on the physical interface or interface+VLAN is exceeded.
	Raisecom(config-port-channel) #igmp filter max- groups action { drop replace } [vlan <i>vlan-list</i>]	(Optional) configure the action when the maximum number of multicast groups on the LAG interface or interface+VLAN is exceeded.

9.5.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show igmp filter [interface <i>interface-type</i> <i>interface-number</i> [vlan <i>vlan-id</i>]]	Show configurations of IGMP filtering.
2	Raisecom#show igmp filter profile [<i>profile-number</i>]	Show information about the IGMP profile.

9.5.8 Example for applying IGMP filtering on interface

Networking requirements

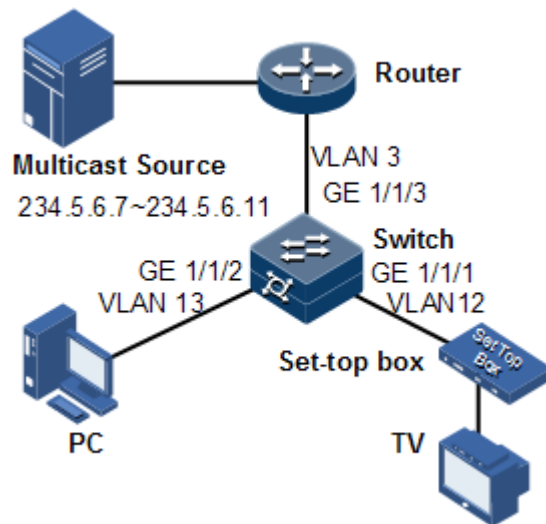
Enable IGMP filtering on the switch. Add filtering rules on the interface to filter multicast users.

As shown in Figure 9-9,

- 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 GE 1/1/2, 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 9-9 Applying IGMP filtering on interface



Configuration steps

Step 1 Create VLANs, and add interfaces to VLANs.

```
Raisecom#config
Raisecom(config)#creat 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 3
Raisecom(config-gigaethernet1/1/1)#switchport trunk untagged vlan 12,13
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 12
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 13
Raisecom(config-gigaethernet1/1/3)#switchport trunk untagged vlan 3
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)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#igmp mvr
Raisecom(config-gigaethernet1/1/2)#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 gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#igmp filter profile 1
```

Step 5 Configure the maximum number of multicast groups on the STB interface.

```
Raisecom(config-gigaethernet1/1/1)#igmp filter max-groups 1
Raisecom(config-gigaethernet1/1/1)#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 gigaethernet 1/1/1
```

```
igmp profile: 1
max group: 1
current group: 0
action: replace
```

9.6 MLD

9.6.1 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 Gazelle S1512i-PWR 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.

9.6.2 Configuring basic functions of MLD

Configure basic functions of MLD for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mld mrouter vlan <i>vlan-id</i> interface-type interface-number	Create a multicast router interface on the specified VLAN.
3	Raisecom(config)#mld ring interface-type interface-number	Enable MLD ring network forwarding on the interface.
4	Raisecom(config)#mld immediate- leave interface-type interface- number [vlan <i>vlan-list</i>]	(Optional) enable immediate leave on the interface or interface+VLAN.
5	Raisecom(config)#mld report- suppression	(Optional) enable Report suppression. When receiving multiple Report packets from the same group in a specified period, the Gazelle S1512i-PWR forwards only one Report packet to the router interface while it suppresses others.
6	Raisecom(config)#mld member- timeout { <i>second</i> infinite }	(Optional) configure the aging time of MLD members.
7	Raisecom(config)#mld version { 1 2 }	Configure the MLD version.

9.6.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show mld immediate-leave [<i>interface-type interface-number</i>]	Show configurations of immediate leave of MLD.
2	Raisecom# show mld mrouter	Show information about the multicast router interface of MLD.
3	Raisecom# show mld snooping [vlan <i>vlan-id</i>]	Show configurations of MLD Snooping.
4	Raisecom# show mld snooping member [count] [<i>interface-type interface-number</i> vlan <i>vlan-id</i>]	Show information about multicast group members of MLD Snooping.
5	Raisecom# show mld statistics [<i>interface-type interface-number</i>]	Show statistics of MLD statistics.

9.6.4 Maintenance

Maintain the Gazelle S1512i-PWR as below.

Command	Description
Raisecom(config)# clear mld statistics [<i>interface-type interface-number</i>]	Clear MLD statistics.

9.7 IGMP Querier

9.7.1 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

The interval 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

The interval 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.

9.7.2 Preparing for configurations

Scenario

On a network with multicast routing protocol widely applied, multiple hosts and client subnets receive multicast data. 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.

9.7.3 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	60s
Maximum response time for sending Query packets	10s
Interval for the last member to send Query packets	1s

9.7.4 Configuring IGMP Querier

Configure IGMP Querier for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#igmp querier	Enable IGMP Querier.

Step	Command	Description
3	<code>Raisecom(config)#igmp querier address ip-address</code>	(Optional) configure the source IP address for the IGMP querier to send Query packets.
4	<code>Raisecom(config)#igmp querier query-interval period</code>	(Optional) configure the IGMP query interval.
5	<code>Raisecom(config)#igmp querier query-max-response-time period</code>	(Optional) configure the maximum response time to send Query packets.
6	<code>Raisecom(config)#igmp querier last-member-query-interval period</code>	(Optional) configure the interval for the last member to send Query packets.



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.

9.7.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show igmp querier</code>	Show configurations of IGMP Querier.
2	<code>Raisecom#show igmp vlan-copy member count</code>	Show the number of multicast group members of multicast VLAN copy.

9.8 Multicast VLAN copy

9.8.1 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 9-10 while multicast VLAN copy transmits data in a way as shown in Figure 9-11.

Figure 9-10 Data transmission of IGMP MVR

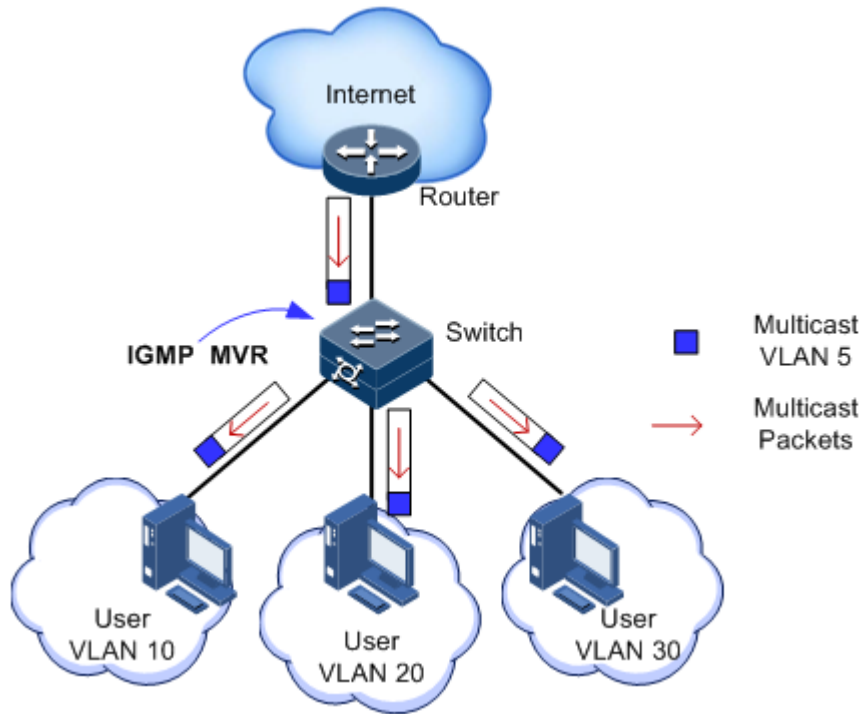
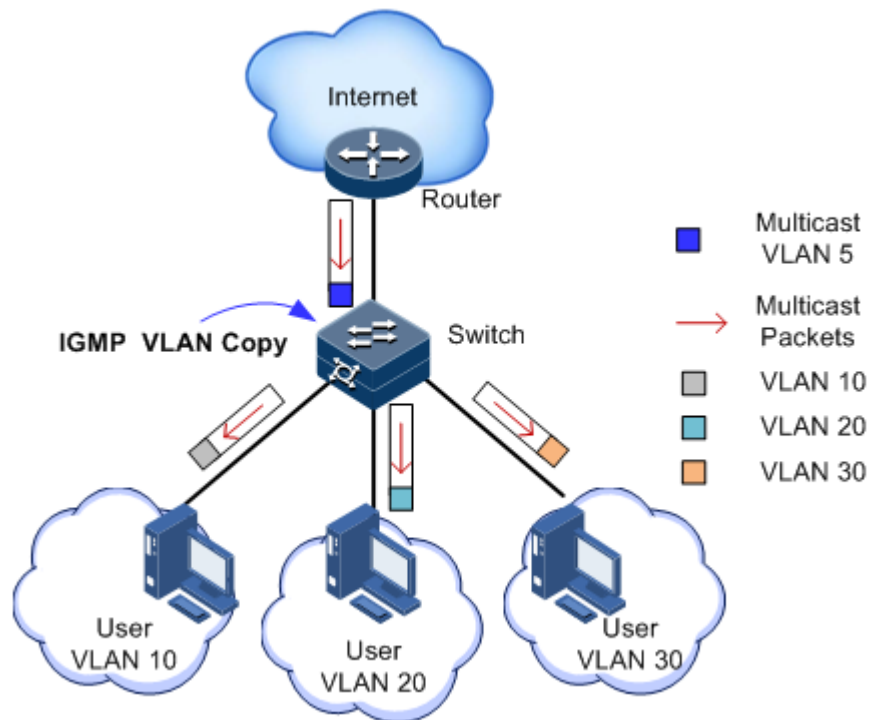


Figure 9-11 Data transmission of multicast VLAN copy



 **Note**

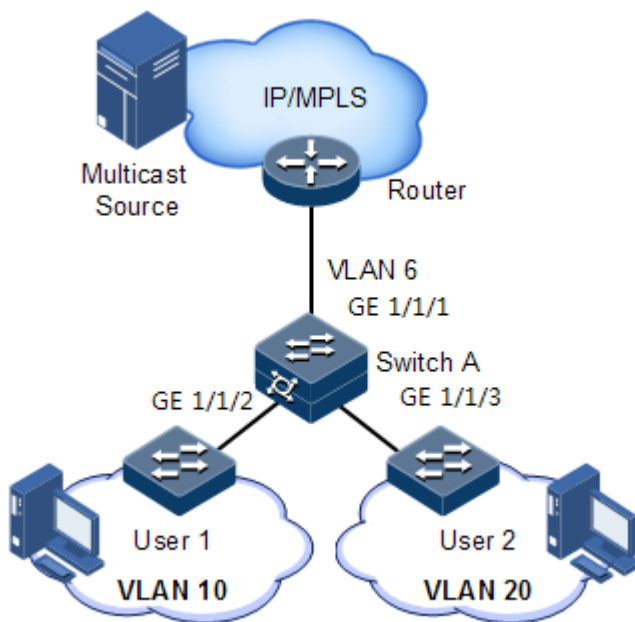
The Gazelle S1512i-PWR can be configured with 1–10 multicast VLANs and at least one multicast VLAN and corresponding group address set. It supports up to 1024 multicast groups.

9.8.2 Preparing for configurations

Scenario

As shown in Figure 9-12, 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 Rx 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 9-12 Multicast VLAN copy networking



Prerequisite

- Disable IGMP Snooping and IGMP MVR.
- Create VLANs, and add related interfaces to VLANs.

9.8.3 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 first and then configure N:1 VLAN mapping.
- To concurrently configure N:1 VLAN mapping and PIM, you must configure PIM first and then configure N:1 VLAN mapping.

9.8.4 Configuring multicast VLAN copy

Configure multicast VLAN copy for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#igmp vlan-copy	Enable global multicast VLAN copy.
3	Raisecom(config)#igmp vlan-copy mcast-vlan vlan- id group { start-ip [end- ip] any }	Configure the group address set of the multicast VLAN.  Note 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.

9.8.5 Configuring static multicast members of VLAN copy

Configure static multicast members of VLAN copy for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface interface-type interface-number	Enter physical layer interface configuration mode.
3	Raisecom(config- tengigabitethernet1/1/1)#igmp vlan- copy mcast-vlan vlan-id static ip- address user-vlan vlan-id	Configure static multicast members of VLAN copy.
4	Raisecom(config- gigaethernet1/1/port)#igmp vlan- copy user-vlan vlan-id	Configure the effective range of multicast VLAN copy.

9.8.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show igmp vlan- copy	Show configurations of multicast VLAN copy.
2	Raisecom#show igmp vlan- copy interface-type interface-number	Show configurations of multicast VLAN copy on the specified interface.
3	Raisecom#show igmp vlan- copy member	Show information about multicast group members of multicast VLAN copy.

No.	Command	Description
4	<code>Raisecom#show igmp vlan-copy member interface-type interface-number</code>	Show information about multicast group members of multicast VLAN copy on the specified interface.
5	<code>Raisecom#show igmp vlan-copy member user-vlan vlan-id</code>	Show information about multicast group members of multicast VLAN copy in the specified user VLAN.
6	<code>Raisecom#show igmp vlan-copy vlan-group [mcast-vlan vlan-id]</code>	Show the multicast VLAN and bound group address set of multicast VLAN copy.
7	<code>Raisecom#show igmp vlan-copy-table [vlan vlan-id] [count]</code>	Show the multicast VLAN copy table.

10 Security

This chapter describes principles and configuration procedures of security, and provides related configuration examples, including the following sections.

- ACL
- Port security MAC
- Dynamic ARP inspection
- RADIUS
- TACACS+
- Storm control
- 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 Gazelle S1512i-PWR 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 number of data packets. The Gazelle S1512i-PWR 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).
- **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.
- **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.
- **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).
- **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 ingress interface to egress interface
- ACL based on VLAN

Prerequisite

N/A

10.1.3 Configuring MAC ACL

Configure MAC ACL for the Gazelle S1512i-PWR as below.

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

Step	Command	Description
2	<pre>Raisecom(config)#access-list <i>acl-number</i> [name <i>acl-name</i>]</pre>	<p>Create an ACL, and enter ACL configuration mode.</p> <ul style="list-style-type: none"> • When the ACL number is between 1000 and 1999, this configuration enters basic IP ACL configuration mode. • When the ACL number is between 2000 and 2999, this configuration enters extended IP ACL configuration mode. • When the ACL number is between 3000 and 3999, this configuration enters MAC ACL configuration mode. • When the ACL number is between 5000 and 5999, this configuration enters User ACL configuration mode. • When the ACL number is between 6000 and 6999, this configuration enters IPv6 ACL configuration mode. • When the ACL number is between 7000 and 7999, this configuration enters advanced ACL configuration mode.
	<pre>Raisecom(config)#time-range <i>time-range name start-time to end-time</i> { <i>weekday-list</i> <i>mon</i> <i>tue</i> <i>wed</i> <i>thu</i> <i>fri</i> <i>sta</i> <i>sun</i> <i>off-day</i> <i>working-day</i> <i>daily</i> } [from <i>start-time start-day</i> [to <i>end-time end-day</i>] to <i>end-time end-day</i>]</pre> <pre>Raisecom(config)#time-range <i>time-range name</i> { from <i>start-time start-day</i> [to <i>end-time end-day</i>] to <i>end-time end-day</i> }</pre>	<p>Create a period which can be quoted by ACL.</p>
3	<pre>Raisecom(config-acl-ip-std)#rule [<i>rule-id</i>] { deny permit } { <i>source-ip-address source-ip-mask</i> any } [time-range <i>time-range name</i>]</pre>	<p>(Optional) configure the matching rule for basic IP ACL.</p>
4	<pre>Raisecom(config-acl-ipv4-ext)#rule [<i>rule-id</i>] { deny permit } { <i>protocol-id</i> icmp igmp ip } { <i>source-ip-address source-ip-mask</i> any } { <i>destination-ip-address destination-ip-mask</i> any } [dscp <i>dscp-value</i>] [ttl <i>ttl-value</i>] [fragment] [precedence <i>precedence-value</i>] [tos <i>tos-value</i>] [time-range <i>time-range name</i>]</pre>	<p>(Optional) configure the matching rule for extended IP ACL.</p>

Step	Command	Description
	<pre>Raisecom(config-acl-ipv4-ext)#rule [rule-id] { deny permit } icmp { source-ip-address source-ip-mask any } { destination-ip-address destination-ip-mask any } icmp-type icmp-message-type [icmp-message- code] [dscp dscp-value precedence precedence-value tos tos-value] [ttl ttl-value] [fragment] [time-range time-range name]</pre>	
	<pre>Raisecom(config-acl-ipv4-ext)#rule [rule-id] { deny permit } igmp { source-ip-address source-ip-mask any } { destination-ip-address destination-ip-mask any } igmp-type igmp-message--type [dscp dscp-value precedence precedence-value tos tos-value] [ttl ttl-value] [fragment] [time-range time-range name]</pre>	
	<pre>Raisecom(config-acl-ipv4-ext)#rule [rule-id] { deny permit } tcp { 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] [range minimu- destination-port maximum- destination-port] [ack ack-value] [dscp dscp-value] [fin fin-value] [fragment] [precedence precedence-value] [psh psh-value] [rst rst-value] [syn syn-value] [tos tos-value] [urg urg-value] [ttl ttl-value] [time-range time- range name]</pre>	
	<pre>Raisecom(config-acl-ipv4-ext)#rule [rule-id] { deny permit } 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] [range minimu- destination-port maximum- destination-port] [dscp dscp-value precedence precedence- value tos tos-value] [ttl ttl- value] [fragment] [time-range time-range name]</pre>	

Step	Command	Description
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 }] [svlan svlanid] [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 } 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.
7	<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]</pre>	(Optional) configure the matching rule for advanced ACL.
8	<pre>Raisecom(config-acl-ipv6)#rule [rule-id] { deny permit } { protocol-id ipv6 } { source-ipv6-address/prefix any } { destination-ipv6-address/prefix any } [dscp dscp-value] [fragment] [flow-label flow label-value] [time-range time-range name]</pre> <pre>Raisecom(config-acl-ipv6)#rule [rule-id] { deny permit } icmpv6 { source-ipv6-address/prefix any } { destination-ipv6-address/prefix any } [icmpv6-type icmpv6-type-value [icmpv6-message-code]] [dscp dscp-value] [flow-label flow label-value] [fragment] [time-range time-range name]</pre>	(Optional) configure the matching rule for IPv6 ACL.

Step	Command	Description
	<pre>Raisecom(config-acl-ipv6)#rule [rule-id] { deny permit } tcp { source-ipv6-address/prefix source- ip-mask any } [source-port] { 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>	
	<pre>Raisecom(config-acl-ipv6)#rule [rule-id] { deny permit } udp { source-ipv6-address/prefix source- ip-mask any } [source-port] { destination- ipv6-address/prefix any } [destination-port] [dscp dscp-value] [flow-label flow label- value] [fragment] [time-range time-range name]</pre>	



Note

When you use the **rule** parameter, the smaller the rule-id is, the higher its priority is.

10.1.4 Configuring filter

Configure the filter for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config- gigaethernet1/1/port)#filter ingress access-list <i>acl-number</i> [statistics]	Apply ACL on the interface.

10.1.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show access-list [<i>acl-number</i> name <i>acl-name</i>]	Show ACL configurations.

No.	Command	Description
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 statistics interface interface-type interface-number { ingress egress } [{ access-list acl-number name acl-name }]</code>	
	<code>Raisecom#show filter interface interface-type interface-number [ingress egress]</code>	
4	<code>Raisecom#show time-range [time-range name]</code>	Show the time range.
5	<code>Raisecom#show local-access access-list</code>	Show SNMP information about server authentication.

10.1.6 Maintenance

Maintain the Gazelle S1512i-PWR as below.

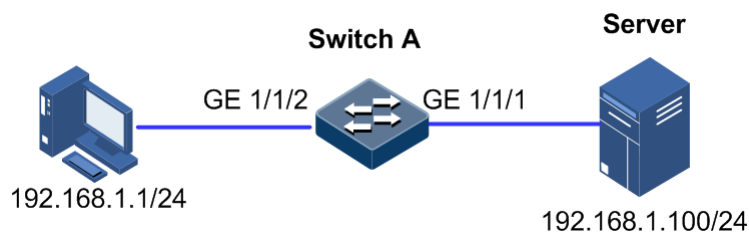
Command	Description
<code>Raisecom(config)#clear filter statistics interface { interface-type interface-number vlan vlan-id } { ingress egress } [access-list acl-number]</code>	Clear statistics on ACL filter configurations.

10.1.7 Example for configuring ACL

Networking requirements

As shown in Figure 10-1, to restrict the access of the user to the server, configure ACL on Switch A. In this way, only PC 192.168.1.1 can access server 192.168.1.100.

Figure 10-1 ACL networking



Configuration steps

Step 1 Configure IP ACL.


```
Raisecom#config
Raisecom(config)#access-list 1001
Raisecom(config-acl-ipv4-advanced)#rule 1 permit 192.168.1.1
255.255.255.255
Raisecom(config-acl-ipv4-advanced)#rule 10 deny any
```

Step 2 Apply ACL on GE 1/1/2 on Switch A.

```
Raisecom(config)#interface gig Ethernet 1/1/2
Raisecom(config-gig Ethernet1/1/2)#filter ingress access-list 1001
```

Checking configurations

Use the **show access-list** command to show IP ACL configurations.

```
Raisecom#show access-list 1001
ACL 1001, name --, 2 rules
ACL's step is 10
  rule 1 permit 192.168.1.1 255.255.255.255
  rule 10 deny any
```

Use the **show filter** command to show filter configurations.

```
Raisecom#show filter interface gig Ethernet 1/1/2
Interface          Direction  ACL-Num
gig Ethernet1/1/2  ingress   1001
```

10.2 Port security MAC

10.2.1 Introduction

Port security MAC is used on the switching device on the edge of the network user side, which can ensure the security of access data on an interface, control ingress packets according to the source MAC address.

You can enable port security MAC to limit and distinguish users which can access the network through secure interfaces. Only users with secure MAC addresses can access the network while users with unsecure MAC addresses will be processed as the configured interface access violation mode.

Secure MAC address classification

Secure MAC addresses supported by the device are divided into the following three types:

- Static secure MAC addresses

Static secure MAC addresses are configured by user on secure interfaces manually. These MAC addresses will take effect when port security MAC is enabled. Static secure MAC addresses are not aged and support loading configurations.

- Dynamic secure MAC addresses

Dynamic secure MAC addresses are learnt by the device. You can configure a learnt MAC address as a secure MAC address within the maximum number of learnt MAC address. Dynamic secure MAC addresses are aged and do not support loading configurations.

Dynamic secure MAC addresses can be converted to sticky secure MAC addresses so as not to be aged and support loading configurations.

- Sticky secure MAC addresses

Sticky secure MAC addresses are generated from the manual configuration of a user on secure interfaces or converted from dynamic secure MAC addresses. Different from static secure MAC addresses, Sticky secure MAC address need to be used with sticky learning and the system supports loading configurations:

- When sticky learning is enabled, sticky secure MAC addresses will take effect and these addresses will not be aged.
- When sticky learning is disabled, sticky secure MAC addresses will lose efficacy and be saved in the system only.



Note

- When sticky learning is enabled, all dynamic secure MAC addresses learnt from an interface will be converted into sticky secure MAC addresses.
- When sticky learning is disabled, all sticky secure MAC addresses on an interface will be converted into dynamic secure MAC addresses.

Processing mode for violating port security MAC

When the number of secure MAC addresses has already reached the maximum number, the input of packets from a new source MAC address will be regarded as violation. For the illegal user access, there are different processing modes for configuring the switch according to the secure MAC violation policy:

- Protect mode: for an illegal access user, 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 a MAC address is drifting, in other words, interface A is accessed by a user of a secure MAC address that already exists on secure interface B, secure interface A will take it as a 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 ingress packets according to the source MAC address. With port security MAC, you can configure the device to allow specified users to access the interface or specified number of users to access from this interface only. However, when the number of users exceeds the limit, accessed packets will be processed according to the port security MAC violation policy.

Prerequisite

N/A

10.2.3 Default configurations of secure MAC address

Default configurations of port security MAC are as below.

Function	Default value
Port secure MAC	Disable
Aging time of dynamic secure MAC addresses	5min
Aging type of dynamic secure MAC addresses	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 secure MAC addresses	1

10.2.4 Configuring basic functions of port security MAC



- 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 configuring them concurrently.
- Port security MAC and interface/interface+VLAN-based MAC address limit are mutually exclusive. We do not recommend configuring them concurrently.

Configure basic functions of port security MAC for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/port)#switchport port-security	Enable port security MAC.
4	Raisecom(config-gigaethernet1/1/port)#switchport port-security maximum <i>maximum</i>	(Optional) configure the maximum number of secure MAC addresses.
5	Raisecom(config-gigaethernet1/1/port)#switchport port-security violation { protect restrict shutdown }	(Optional) configure the port security MAC violation mode.
6	Raisecom(config-gigaethernet1/1/port)#no port-security shutdown Raisecom(config-gigaethernet1/1/port)#exit	(Optional) re-enable the interface which is shut down due to violating port security MAC.
7	Raisecom(config)#port-security recovery-time <i>second</i>	(Optional) configure the restoration time of port security MAC.



Note

When the secure MAC violation policy is Shutdown, 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 remain valid.

10.2.5 Configuring static secure MAC address

Configure the static secure MAC address for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/port)#switchport port-security	Enable port security MAC.
4	Raisecom(config-gigaethernet1/1/port)#switchport port-security mac-address <i>mac-address vlan vlan-id</i>	Configure the static secure MAC address.

10.2.6 Configuring dynamic secure MAC address

Configure dynamic secure MAC address for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#port-security aging-time <i>period</i>	(Optional) configure the aging time of dynamic secure MAC addresses.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
4	Raisecom(config-gigaethernet1/1/port)#switchport port-security aging-type { absolute inactivity }	(Optional) configure the aging type of secure MAC addresses.
5	Raisecom(config-gigaethernet1/1/port)#switchport port-security	(Optional) enable port dynamic security MAC learning.
6	Raisecom(config-gigaethernet1/1/port)#switchport port-security trap enable	(Optional) enable port security MAC Trap.
7	Raisecom(config-gigaethernet1/1/port)#switchport port-security trap period <i>period value</i>	(Optional) configure the period for sending Traps for port security MAC.



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 be abnormal.

Configure the sticky secure MAC address for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/port)#switchport port-security	Enable port security MAC.

Step	Command	Description
4	<code>Raisecom(config-gigaetherne1/1/port)#switchport port-security mac-address sticky</code>	Enable sticky secure MAC learning.
5	<code>Raisecom(config-gigaetherne1/1/port)#switchport port-security mac-address sticky mac-address vlan vlan-id</code>	(Optional) manually configure sticky secure MAC addresses.



Note

After sticky secure MAC address learning is enabled, dynamic secure MAC addresses will be converted into sticky secure MAC addresses; manually configured sticky secure MAC addresses 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-list]</code>	Show configurations of port security MAC.
2	<code>Raisecom#show port-security mac-address [interface-type interface-list]</code>	Show configurations of secure MAC address and secure MAC address learning.

10.2.9 Maintenance

Maintain the Gazelle S1512i-PWR as below.

Command	Description
<code>Raisecom(config-gigaetherne1/1/port)#clear port-security { all configured dynamic sticky }</code>	Clear a specified secure MAC address type on a specified interface.

10.2.10 Example for configuring port security MAC

Networking requirements

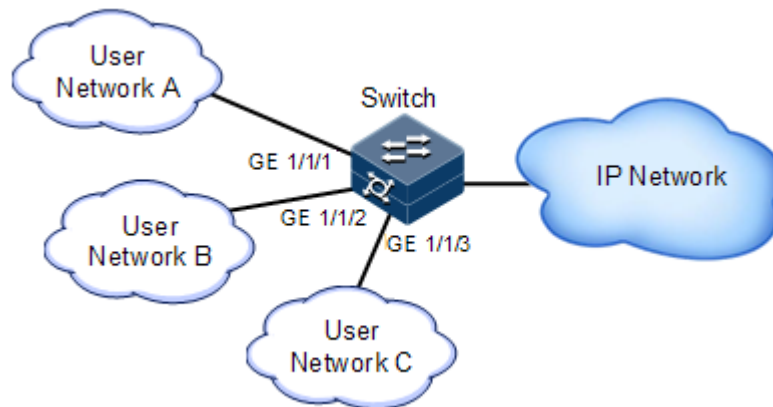
As shown in Figure 10-2, the Switch connects 3 user networks. To ensure security of data accessed from the interface, configure the Switch as below.

- 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 when 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; when 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 10-2 Port security MAC networking



Configuration steps

Step 1 Configure secure MAC address of GE 1/1/1.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport port-security
Raisecom(config-gigaethernet1/1/1)#switchport port-security maximum 3
Raisecom(config-gigaethernet1/1/1)#switchport port-security mac-address
0000.0000.0001 vlan 1
Raisecom(config-gigaethernet1/1/1)#switchport port-security violation
protect
Raisecom(config-gigaethernet1/1/1)#switchport port-security trap enable
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#port-security aging-time 10
```

Step 2 Configure the secure MAC address of GE 1/1/2.

```
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport port-security
Raisecom(config-gigaethernet1/1/2)#switchport port-security maximum 2
Raisecom(config-gigaethernet1/1/2)#switchport port-security mac-address
sticky
Raisecom(config-gigaethernet1/1/2)#switchport port-security violation
restrict
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 3 Configure the secure MAC address of 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 address.

```
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 avoids responding ARP packets which do not meet requirements, thus preventing ARP spoofing attacks on the network.

There are 2 modes for dynamic ARP inspection:

- Static binding mode: configure the binding manually.
- Dynamic binding mode: cooperate with the DHCP snooping to generate dynamic binding. When a DHCP Snooping entry is changed, dynamic ARP inspection will also update the 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 the 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 trusted status:

- Trusted interface: the interface will stop ARP inspection and performs no ARP protection on the interface. All ARP packets are allowed to pass.
- Untrusted interface: the interface performs ARP protection. Only ARP packets that match the binding table rules are allowed to pass, otherwise they are discarded.

Figure 10-3 Principles of dynamic ARP inspection

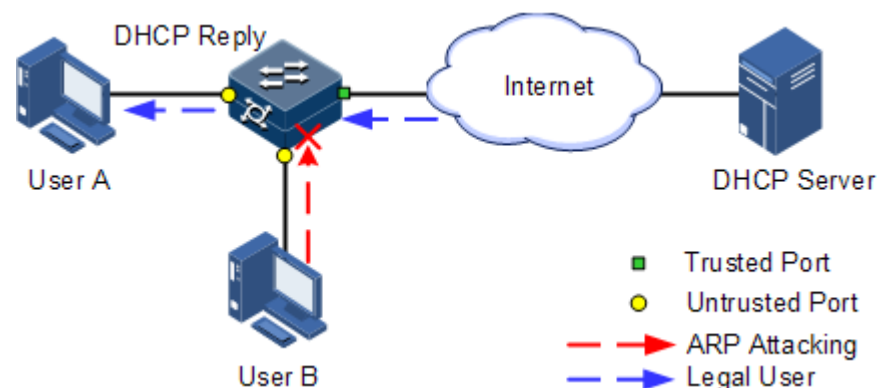


Figure 10-3 shows principles of dynamic ARP inspection. When the Gazelle S1512i-PWR receives an ARP packet, it compares the source IP address, source MAC address, interface ID, and VLAN information of the ARP packet with the DHCP Snooping entry information. If matched, it indicates that it is a legal 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 Gazelle S1512i-PWR by sending a large number of ARP packets to the Gazelle S1512i-PWR.

- When the number of ARP packets received by an interface every second exceeds the threshold, the system will regard that the interface is under an ARP attack, and then discard all received ARP packets to prevent the attack.
- 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
Interface trusted status of dynamic ARP inspection	Untrusted
Static binding of dynamic ARP inspection	Disable
Dynamic binding of dynamic ARP inspection	Disable
Static binding table of dynamic ARP inspection	N/A
Protection VLAN of dynamic ARP inspection	All VLANs
Rate limiting on ARP packets on the interface	Disable
Rate limit on ARP packets on the interface	60 pps
Restoration status of rate limiting on ARP packets	Disable
Restoration time for rate limiting on ARP packets	30s

10.3.4 Configuring trusted interfaces of dynamic ARP inspection

Configure trusted interfaces of dynamic ARP inspection for the Gazelle S1512i-PWR 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)#ip arp-inspection trust</code>	Configure the interface as a trusted interface. Use the no ip arp-inspection trust command to configure the interface as 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip arp-inspection static-config</code>	Enable global static ARP binding.
3	<code>Raisecom(config)#ip arp-inspection binding ip-address [mac-address] [vlan vlan-id] interface-type interface-number</code>	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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip arp- inspection dhcp-snooping</code>	Enable global dynamic ARP binding.

10.3.7 Configuring protection VLAN of dynamic ARP inspection

Configure protection VLAN of dynamic ARP inspection for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip arp-inspection dhcp-snooping	Enable global dynamic binding.
3	Raisecom(config)#ip arp-inspection vlan <i>vlan-list</i>	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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/port)#ip arp-rate-limit rate <i>rate-value</i>	Configure rate limiting on ARP packets on the interface.

10.3.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show ip arp-inspection	Show configurations of dynamic ARP inspection.
2	Raisecom#show ip arp-inspection binding [<i>interface-type interface-number</i>]	Show information about the dynamic ARP inspection binding table.
3	Raisecom#show ip arp-rate-limit	Show configurations of rate limiting on ARP packets.

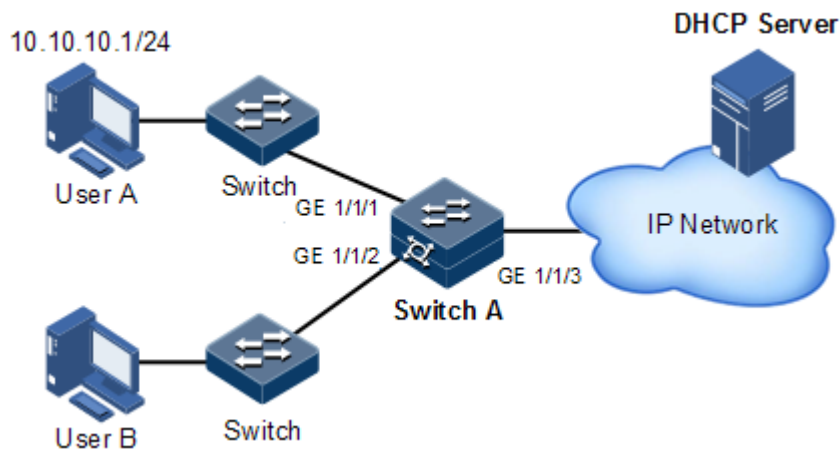
10.3.10 Example for configuring dynamic ARP inspection

Networking requirements

To prevent ARP attacks, configure dynamic ARP inspection on Switch A, as shown in Figure 10-4.

- 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 limit is configured to 20 pps and recovery time for rate limiting is configured to 15s.

Figure 10-4 Configuring dynamic ARP inspection



Configuration steps

Step 1 Configure GE 1/1/3 to the trusted interface.

```
Raisecom#config  
Raisecom(config)#interface gigaethernet 1/1/3  
Raisecom(config-gigaethernet1/1/3)#ip arp-inspection trust  
Raisecom(config-gigaethernet1/1/3)#exit
```

Step 2 Configure static binding.

```
Raisecom(config)#ip arp-inspection static-config  
Raisecom(config)#ip arp-inspection binding 10.10.10.1 gigaethernet 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)#ip arp-rate-limit enable
Raisecom(config-gigabitEthernet1/1/2)#exit
```

Step 5 Configure automatic recovery for rate limiting on ARP packets.

```
Raisecom(config)#ip arp-rate-limit recover time 15
Raisecom(config)#ip arp-rate-limit recover enable
```

Checking results

Use the **show ip arp-inspection** command to show configurations of interface trusted status 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
-----
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
arp rate limit auto recover    : enable
arp rate limit auto recover time : 15 second
Port                          Enable-Status  Rate(Num/Sec)  Overload
-----
--
gigaethernet1/1/1            Disabled      100             NO
gigaethernet1/1/2            Enabled       20              NO
gigaethernet1/1/3            Disabled      100             NO
gigaethernet1/1/4            Disabled      100             NO
gigaethernet1/1/5            Disabled      100             NO
gigaethernet1/1/6            Disabled      100             NO
.....
```

10.4 RADIUS

10.4.1 Introduction

Remote Authentication Dial In User Service (RADIUS) is a standard communication protocol that authenticates remote access users intensively. RADIUS uses UDP as the transmission protocol (port 1812 and port 1813) which has a good instantaneity; at the same time, RADIUS supports retransmission mechanism and standby server mechanism which has a good reliability.

RADIUS authentication

RADIUS adopts client/server mode, network access device is used as the client of the RADIUS server. RADIUS server receives user connecting requests and authenticates users, then reply configurations to all clients for providing services. Control user access device and network and improve network security.

Communication between client and RADIUS server is authenticated by sharing key, which will not be transmitted on network. Besides, all user directions need to be encrypted when transmitting between client device and RADIUS server to ensure security.

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 perform authentication and accounting to control users to access to the Gazelle S1512i-PWR and network. The Gazelle S1512i-PWR 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
IP address of the RADIUS accounting server	0.0.0.0
Port number of the RADIUS authentication server	1812
Port number 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#radius [backup] ip-address [auth-port port- id]</code>	Assign the IP address and port number for RADIUS authentication server. Configure the backup parameter to assign the backup RADIUS authentication server.
2	<code>Raisecom#radius-key string</code>	Configure the shared key for RADIUS authentication.

Step	Command	Description
3	<code>Raisecom#user login { local-radius local-user radius-local [server-no-response] radius-user local-tacacs tacacs-local [server-no-response] tacacs-user }</code>	Configure users to perform login authentication through RADIUS.

10.4.5 Configuring RADIUS accounting

Configure RADIUS accounting for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#aaa accounting login enable</code>	Enable RADIUS accounting.
2	<code>Raisecom#radius [backup] accounting-server ip-address [account-port]</code>	Assign IP address and UDP port number for RADIUS accounting server. Configure the backup parameter to assign the backup RADIUS accounting server.
3	<code>Raisecom#radius accounting-server key string</code>	Configure the shared key for communicating with the RADIUS accounting server. The shared key must be identical to the one configured on the RADIUS accounting server. Otherwise, accounting will fail.
5	<code>Raisecom#aaa accounting fail { offline online }</code>	Configure the processing policy for accounting failure.
6	<code>Raisecom#aaa accounting update minute</code>	Configure the period for sending Account-Update packets. If it is configured to 0, no Account-Update packet will be sent.  Note The RADIUS accounting server can record access time and operation for each user through Account-Start packets, Account-Update packets, and Account-Stop packets.

10.4.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show radius-server</code>	Show configurations of the RADIUS server.

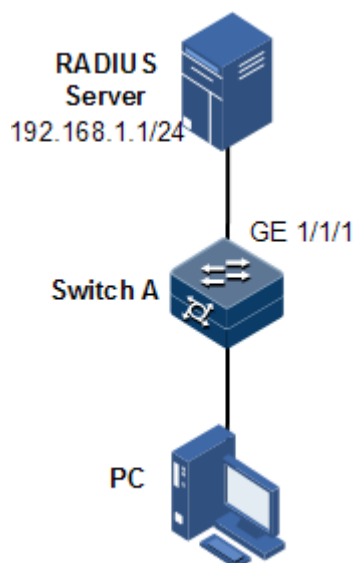
No.	Command	Description
2	<code>Raisecom#show aaa</code>	Show configurations of RADIUS accounting.

10.4.7 Example for configuring RADIUS

Networking requirements

As shown in Figure 10-5, 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 10-5 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
authentication server IP      :192.168.1.1
port                          :1812
Backup authentication server IP:
port                          :1812
Authentication server key    :gGOIjAJxkJKy
Backup authentication server Key:--
Accounting server IP        :192.168.1.1
port                          :1813
Backup accounting server IP   :
port                          :1813
Accounting server key        :gGOIjAJxkJKy
Backup Accounting server Key  :--
authorization fail policy    :15
NAS IP Address               :--
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 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 header of TACACS+, and there is a field to show whether the data packets are encrypted in the header 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 Gazelle S1512i-PWR and network. TACACS+ is safer and more reliable than RADIUS. The Gazelle S1512i-PWR 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+	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
Accounting failure processing policy	Online
Period for sending Account-Update packets	0

10.5.4 Configuring TACACS+ authentication

Configure TACACS+ authentication for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#tacacs-server [backup] ip-address</code>	Assign the IP address and port number for the TACACS+ authentication server. Configure the backup parameter to assign the backup TACACS+ authentication server.
2	<code>Raisecom#tacacs-server [backup] { key string encrypt-key string }</code>	Configure the shared key for TACACS+ authentication.

Step	Command	Description
3	<code>Raisecom#user login { local-tacacs tacacs-local [server-no-response] tacacs-user }</code>	Configure users to perform login authentication through TACACS+.
4	<code>Raisecom#aaa command authorize { enable disable }</code>	Enable command authorization.

10.5.5 Configuring TACACS+ accounting

Configure TACACS+ accounting for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#aaa accounting login enable</code>	Enable TACACS+ accounting.
2	<code>Raisecom#tacacs [backup] accounting-server ip-address</code>	Assign the IP address and UDP port number for the TACACS+ accounting server. Configure the backup parameter to assign the backup TACACS+ accounting server.
3	<code>Raisecom#tacacs-server key string</code>	Configure the shared key to communicate with the TACACS+ accounting server.
4	<code>Raisecom#aaa accounting fail { offline online }</code>	Configure the processing policy for accounting failure.
5	<code>Raisecom#aaa accounting update period</code>	Configure the period for sending accounting update packets. If it is configured to 0, no Account-Update packet will be sent.

10.5.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show tacacs-server</code>	Show configurations of the TACACS+ authentication server.
2	<code>Raisecom#show aaa</code>	Show configurations of TACACS+ accounting.

10.5.7 Maintenance

Maintain the Gazelle S1512i-PWR as below.

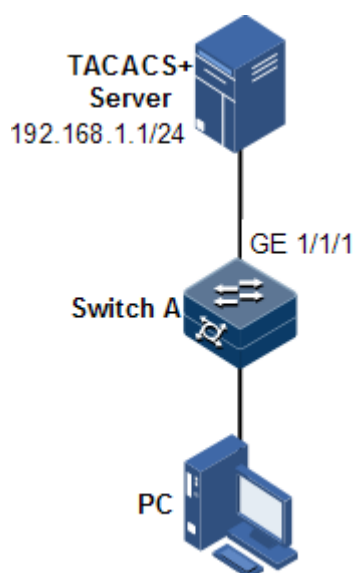
Command	Description
<code>Raisecom#clear tacacs statistics</code>	Clear TACACS+ statistics.

10.5.8 Example for configuring TACACS+

Networking requirements

As shown in Figure 10-6, configure TACACS+ authentication on Switch A to authenticate login user and control users from accessing the Gazelle S1512i-PWR.

Figure 10-6 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
```

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          : 48rTxZF0aWN6
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.

Generation of broadcast storm

Broadcast storm may occur under the following conditions:

- 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 Gazelle S1512i-PWR 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 preconfigured 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 preconfigured threshold, the broadcast packets are broadcasted to other interfaces of the switch properly.

Types of storm control

Storm control is performed in the following forms:

- Ratio (bandwidth ratio): the ratio of broadcast traffic, unknown multicast traffic, or unknown unicast traffic to total bandwidth of the interface
- 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 Gazelle S1512i-PWR 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
Storm control mode	bps
Number of allowed broadcast storm packets per second	1024 pps
DLF packet forwarding	Enable

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 Gazelle S1512i-PWR 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	<pre>Raisecom(config- gigaethernet1/1/port)#storm-control { broadcast unknown-multicast dlf all } pps value</pre>	Configure the storm control threshold.



Caution

The Gazelle S1512i-PWR does not support configuring multiple storm control modes. To change the storm control threshold for a type of packets, use the **no** form of the corresponding command to delete it, and then configure it to another value.

10.6.5 Configuring DLF packet forwarding

Configure DLF packet forwarding for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#dlf-forwarding enable</code>	Enable DLF packet forwarding on an interface.

10.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show storm-control interface [interface-type interface-number]</code>	Show configurations of storm control.
2	<code>Raisecom#show dlf-forwarding</code>	Show DLF packet forwarding status.

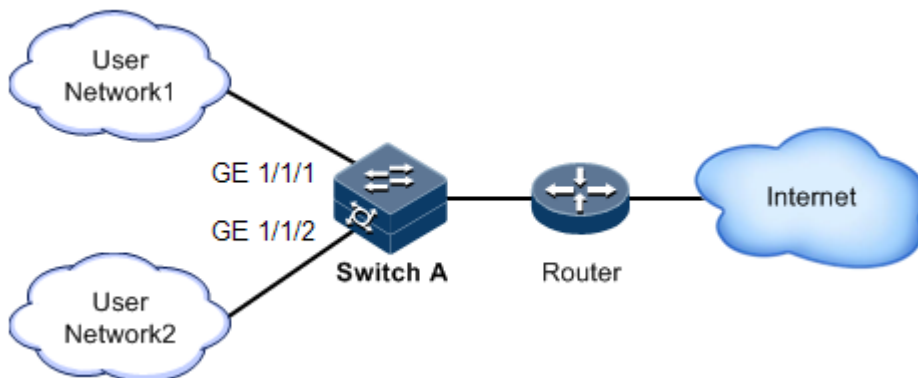
10.6.7 Example for configuring storm control

Networking requirements

As shown in Figure 10-7, 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 GE 1/1/1 and GE 1/1/2 on Switch A to control broadcast packets from user networks 1 and 2, with the threshold of 640 kbit/s.

Figure 10-7 Storm control networking



Configuration steps

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)
-----
GE1/1/1       Broadcast        --                640            4
              Multicast        --                0              0
              Dlf
```

10.7 IP Source Guard

10.7.1 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:

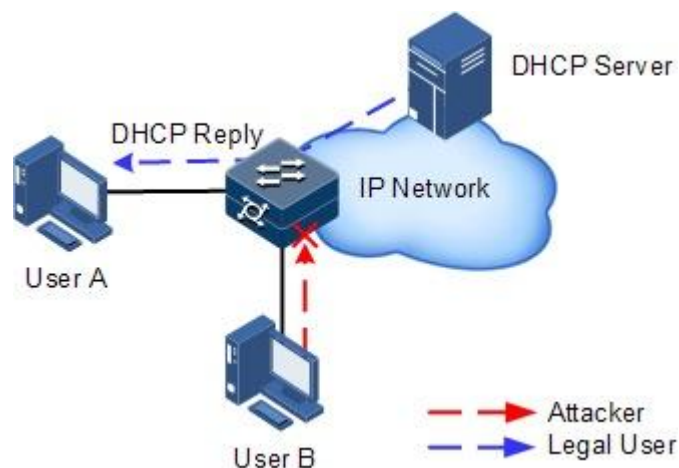
- Static binding: configure binding information manually and generate binding entry to complete the interface control, which fits for the case where the number of hosts is small or where you need to perform separate binding on a single host.
- Dynamic binding: obtain binding information automatically 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 Gazelle S1512i-PWR. The IP source binding table is taken as the basis for each interface to test received data packets. Figure 10-8 shows principles of IP Source Guard.

- If the received IP packets meet the relation 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 10-8 Principles of IP Source Guard



Before forwarding IP packets, the Gazelle S1512i-PWR 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.

10.7.2 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.

10.7.3 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 trusted status	Untrusted

10.7.4 Configuring interface trusted status of IP Source Guard

Configure the interface trusted status of IP Source Guard for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)# interface interface-type interface-number	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/p ort)#ip verify source trust	(Optional) configure the IPv4 interface as a trusted interface. Use the no ip verify source trust 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.

10.7.5 Configuring IP Source Guard binding

Configuring IP Source Guard static binding

Configure IP Source Guard static binding for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip verify source</code>	Enable IP Source Guard static binding.
3	<code>Raisecom(config)#ip source binding ip-address [ip-mask-address mac- address vlan vlan-id] interface- type interface-number</code>	Configure the static binding. Use the no ip source binding static-all command to delete the 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip verify source dhcp</code>	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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip verify source dhcp	Enable IP Source Guard dynamic binding.
3	Raisecom(config)#ip source binding dhcp static	Translate the dynamic binding to the static binding.

10.7.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show ip verify source	Show global binding status and interface trusted status.
2	Raisecom#show ip source binding [interface-type interface-number]	Show configurations of IP Source Guard binding, interface trusted status, and binding table.

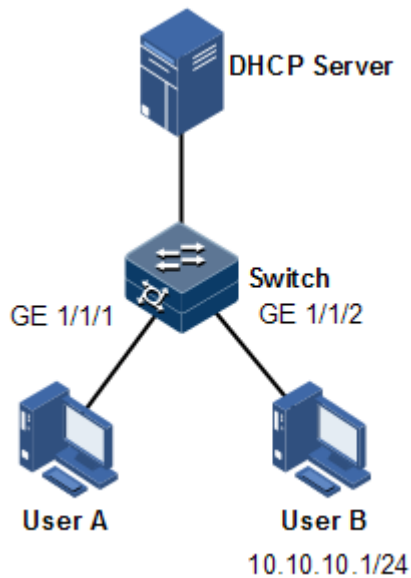
10.7.7 Example for configuring IP Source Guard

Networking requirements

As shown in Figure 10-9, to prevent IP address embezzlement, 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 10-9 Configuring IP Source Guard



Configuration steps

Step 1 Configure GE 1/1/1 to the trusted interface.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#ip verify source trust
Raisecom(config-gigaethernet1/1/1)#exit
```

Step 2 Configure static binding.

```
Raisecom(config)#ip verify source
Raisecom(config)#ip source binding 10.10.10.1 gigaethernet 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
.....
```

10.8 PPPoE+

10.8.1 Introduction

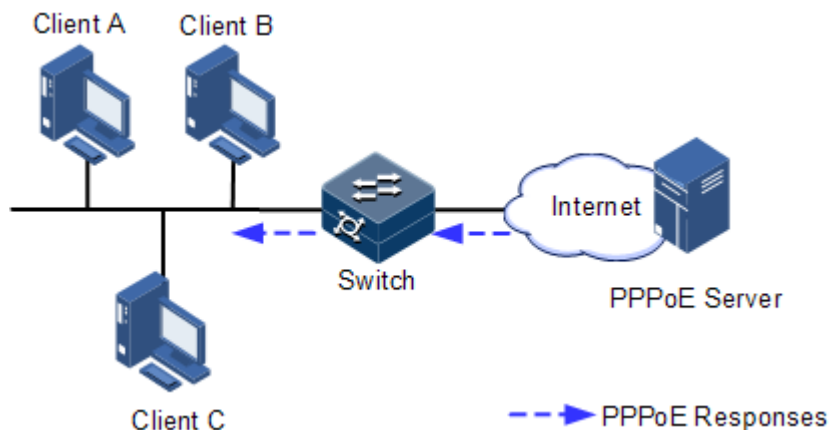
PPPoE Intermediate Agent (PPPoE+) is used to process authentication packets. PPPoE+ adds more information about access devices into the authentication packet to bind account and access device so that the account is not shared and stolen, and the carrier's and users' interests are protected. This provides 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 10-10. 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 10-10 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 judges 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.

10.8.2 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

10.8.3 Default configurations of PPPoE+

Default configurations of 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.

10.8.4 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#pppoeagent enable</code>	Enable global PPPoE+.
3	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
4	<code>Raisecom(config- gigaethernet1/1/port)#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 Gazelle S1512i-PWR 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)#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.

10.8.5 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/port)#pppoeagent circuit-id <i>string</i>	(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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)# pppoeagent circuit-id attach-string <i>string</i>	(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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/port)#pppoeagent remote-id { client-mac switch- mac }	(Optional) configure PPPoE+ Remote ID to be padded with the MAC address.
4	Raisecom(config- gigaethernet1/1/port)#pppoeagent remote-id format { ascii binary }	(Optional) configure the padding modes of the PPPoE+ Remote ID.
5	Raisecom(config- gigaethernet1/1/port)#pppoeagent remote-id user-define <i>string</i>	(Optional) configure the customized Remote ID.

Configuring Tag overriding

Tags of some fields may be forged by the client due to some reasons, so the original Tags need to be overridden. After Tag overriding is enabled, these Tags will be overridden if the PPPoE packets contain Tags of these fields; if not, Tags will be added to these PPPoE packets.

Configure Tag overriding for the Gazelle S1512i-PWR 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)#pppoeagent vendor-specific-tag overwrite enable</code>	Enable Tag overriding.

10.8.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show pppoeagent</code>	Show PPPoE+ configurations.
2	<code>Raisecom#show pppoeagent statistic</code>	Show PPPoE+ statistics.

10.8.7 Maintenance

Maintain the Gazelle S1512i-PWR as below.

Command	Description
<code>Raisecom(config)#clear pppoeagent statistic</code>	Clear PPPoE+ statistics.

10.8.8 Example for configuring PPPoE+

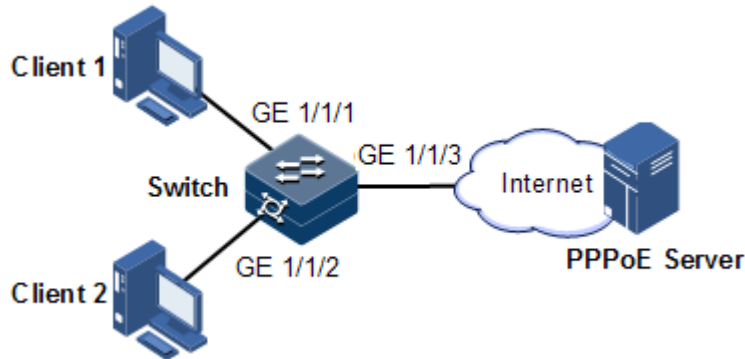
Networking requirements

As shown in Figure 10-11, 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 10-11 PPPoE+ networking



Configuration steps

Step 1 Configure GE 1/1/3 as the trusted interface.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#pppoeagent trust
Raisecom(config-gigaethernet1/1/3)#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 gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#pppoeagent circuit-id user01
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#pppoeagent remote-id client-mac
Raisecom(config-gigaethernet1/1/2)#pppoeagent remote-id format ascii
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 3 Enable Tag overwriting on GE 1/1/1 and GE 1/1/2.

```
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#pppoeagent vendor-specific-tag
overwrite enable
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#pppoeagent vendor-specific-tag
overwrite enable
```

```
Raisecom(config-gigaethernet1/1/2)#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 gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#pppoeagent enable
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#pppoeagent enable
```

Checking results

Use the **show pppoeagent** command to show PPPoE+ configurations.

```
Raisecom#show pppoeagent
Mac-format: hhhhhhhhhhhh
Global PPPoE+ status: enable
Attach-string: raisecom
Circuit ID padding mode: switch
      Port          State  Overwrite  Remote-ID  Format-rules
Circuit-ID
-----
-----
```

10.9 Configuring CPU protection

10.9.1 Preparing for configurations

Scenario

When the Gazelle S1512i-PWR 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 rate of packets which enters the CPU.

Prerequisite

N/A

10.9.2 Configuring global CPU CAR

Configure global CPU CAR for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#cpu-protect car { arp bpdu dhcp global icmp igmp } kbps cir cir cbs cbs</code>	Configure the protocol type, CIR, and BPS of global CPU packet protection.

10.9.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show cpu-protect car statistics</code>	Show CPU CAR statistics.

10.9.4 Maintenance

Maintain the Gazelle S1512i-PWR as below.

Command	Description
<code>Raisecom(config)# clear cpu-protect car { arp bpdu dhcp global icmp igmp } statistics</code>	Clear global CPU CAR statistics.

10.10 Configuring anti-ARP attack

10.10.1 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 Gazelle S1512i-PWR, they will cause the following harms:

- The Gazelle S1512i-PWR sends excessive ARP request packets to the destination network segment, so this network segment is overburdened.
- The Gazelle S1512i-PWR repeatedly resolve destination IP addresses, so the CPU is overburdened.

To prevent these harms due to attacks on IP packets, the Gazelle S1512i-PWR supports anti-ARP attack.

Prerequisite

N/A

10.10.2 Configuring ARP

Configure ARP for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#arp learning strict enable	Enable the device to learn ARP entries requested by itself.
4	Raisecom(config-vlan1)#arp check- destination-ip enable	Enable the check of ARP destination IP address.
5	Raisecom(config-vlan1)#arp filter { gratuitous mac-illegal tha- filled-request }	Configure ARP filtering.
6	Raisecom(config-vlan1)#arp anti- attack entry-check { fixed-all fixed-mac send-ack }	Configure the fixing of ARP entries.
7	Raisecom(config-vlan1)#ip arp-rate- limit rate <i>rate value</i>	Configure rate limiting of ARP.

10.10.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show arp	Show ARP information.
2	Raisecom#show ip arp filter	Show information about ARP filtering.
3	Raisecom#show ip arp-rate- limit	Show the rate limit on ARP packets.

11 Reliability

This chapter describes principles and configuration procedures of reliability, and provides related configuration examples, including the following sections:

- Link aggregation
- Interface backup
- Link-state tracking

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 the link between two devices, link aggregation helps gain higher bandwidth without upgrading hardware.

The Gazelle S1512i-PWR supports the following three link aggregation modes:

- 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 rate, 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.

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 these interfaces 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 Gazelle S1512i-PWR 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-channel1)#mode manual</code>	Configure manual link aggregation mode.

Step	Command	Description
4	<code>Raisecom(config-port-channel)#{ max-active min-active } links <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)#load-sharing mode { dst-ip dst-mac src-dst-ip src-dst-mac src-ip src-mac }</code>	(Optional) configure a load balancing mode for link aggregation. By default, the load balancing algorithm is configured to <code>sxordmac</code> . 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#lACP system-priority <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)#lACP timeout { fast slow }</code>	(Optional) configure LACP timeout mode. By default, it is slow.
4	<code>Raisecom(config)#interface port-channel <i>channel-number</i></code>	Enter LAG configuration mode.
5	<code>Raisecom(config-port-channel)#mode lACP [backup]</code>	Configure the working mode of the LAG to static LACP LAG.
6	<code>Raisecom(config-port-channel)#master-port <i>interface-type interface-number</i></code>	Configure the interface as the master interface in master/slave aggregation group mode.
7	<code>Raisecom(config-port-channel)#{ max-active min-active } links <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 number is 1.

Step	Command	Description
8	<code>Raisecom(config-port-channel1)#exit</code>	Return to global configuration mode.
9	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter Layer 2 physical interface configuration mode.
10	<code>Raisecom(config-gigaethernet1/1/port)#port-channel channel-number</code>	Add the Layer 2 interface to the LAG.
11	<code>Raisecom(config-port-channel1)#lACP 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.
12	<code>Raisecom(config-channel1)#lACP 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 rate, interface highest LACP priority, and interface minimum ID. The interface is in active status by default, the interface with identical rate, 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 Gazelle S1512i-PWR 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-channel1)#mode manual backup</code>	Configure the working mode of the LAG to manual backup LAG.
4	<code>Raisecom(config-port-channel1)#master-port interface-type interface-number</code>	Configure the active interface of the LAG.

Step	Command	Description
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.

11.1.6 Checking configurations

Use the following commands to check configuration results.

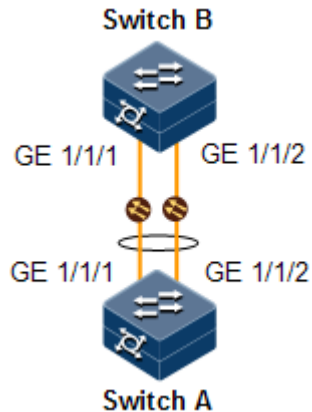
No.	Command	Description
1	<code>Raisecom#show lacp internal</code>	Show local system LACP interface status, flag, interface priority, administration key, operation key, and interface status machine status.
2	<code>Raisecom#show lacp neighbor</code>	Show information about LACP neighbors, including Tag, interface priority, device ID, Age, operation key value, interface ID, and interface status machine status.
3	<code>Raisecom#show lacp statistics</code>	Show statistics on 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.  Note The active member interface refers to the one whose interface status is Up.

11.1.7 Example for configuring static LACP link aggregation

Networking requirements

As shown in Figure 11-1, 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 into one LAG; GE 1/1/1 is used as the active interface and GE 1/1/2 as the standby interface.

Figure 11-1 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#name 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 port-channel 1
SwitchB(config-aggregator)#mode lacp-static
SwitchB(config-aggregator)#exit
```

```
SwitchB(config)#interface gig Ethernet 1/1/1
SwitchB(config-gig Ethernet1/1/1)#port-channel 1
SwitchB(config-gig Ethernet1/1/1)#exit
SwitchB(config)#interface gig Ethernet 1/1/2
SwitchB(config-gig Ethernet1/1/2)#port-channel 1
SwitchB(config-gig Ethernet1/1/2)#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    : 0                        Priority-Preemptive: Disable
Member Port: gig Ethernet1/1/1 gig Ethernet1/1/2
Efficient Port:
```

Use the **show lacp internal** command to show configurations of local LACP interface status, flag, interface priority, administration key, operation key, and interface status 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
-----
gig Ethernet1/1/1  Down      SA     1000           1          1
0x45
gig Ethernet1/1/2  Down      SA     32768          1          1
0x45
```

Use the **show lacp neighbor** command to show configurations of LACP interface status, flag, interface priority, administration key, operation key, and interface status machine of the peer system on Switch A.

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 links. 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.

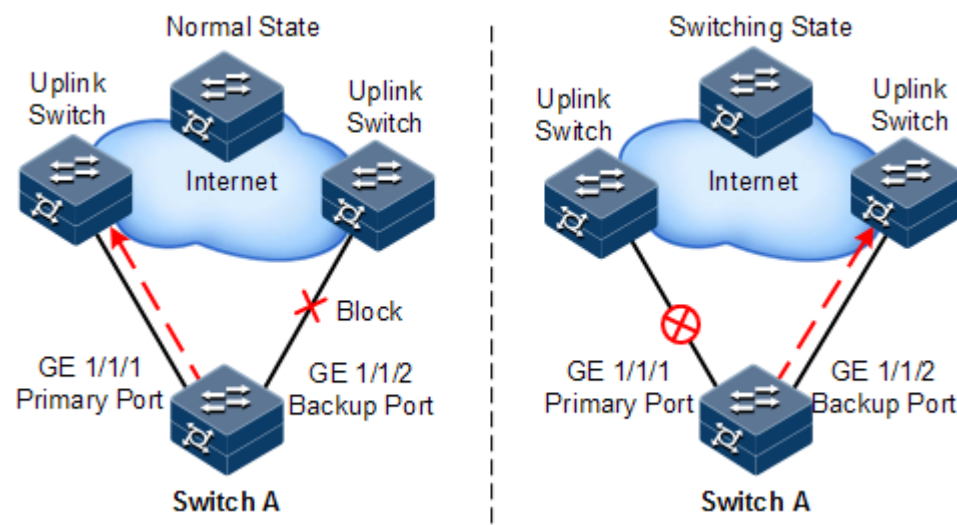
When the primary link fails, traffic is switched to the backup link. In this way, not only 50ms fast switching is ensured, but also configurations are simplified.

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 Up status, the other interface is in Standby status. At any time, only one interface is in Up status. When the Forward interface fails, the blocked interface is switched to the Up status.

Figure 11-2 Principles of interface backup



As shown in Figure 11-2, GE 1/1/1 and GE 1/1/2 on Switch A are connected to their uplink devices respectively. The interface forwarding status is shown as below:

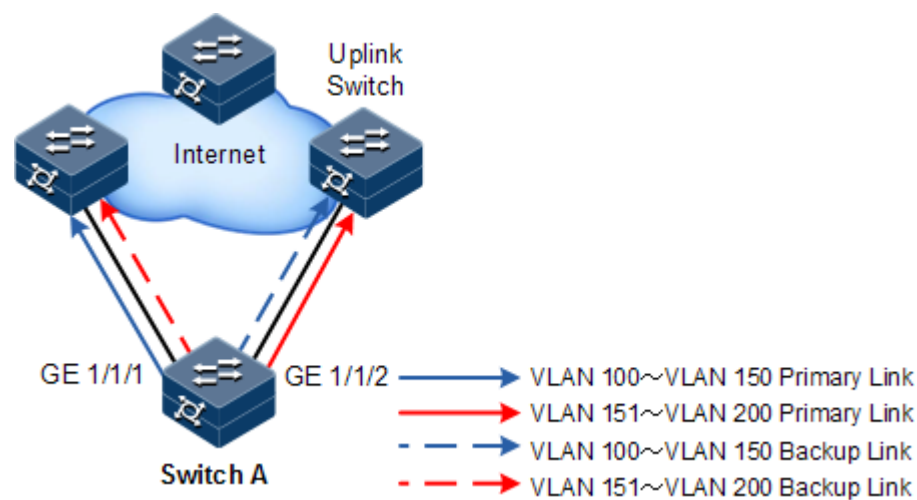
- Under normal conditions, GE 1/1/1 is the primary interface while GE 1/1/2 is the backup interface. GE 1/1/1 and the uplink device forward packet while GE 1/1/2 and the uplink device do not forward packets.
- When the link between GE 1/1/1 and its uplink device fails, the backup GE 1/1/2 and its uplink 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 11-3.

Figure 11-3 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 share 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 Gazelle S1512i-PWR 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	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type primary-interface-number</i>	Enter physical layer interface configuration mode or LAG configuration mode.
3	Raisecom(config-gigaethernet1/1/port)#port backup <i>interface-type backup-interface-number [vlanlist vlan-list]</i> Raisecom(config-port-channel)#port backup <i>interface-type backup-interface-number [vlanlist vlan-list]</i>	Configure the interface backup group. In the VLAN list, configure the <i>interface backup-interface-number</i> to the backup interface and configure the <i>interface primary-interface-number</i> to the primary interface. If no VLAN list is specified, the VLAN ranges from 1 to 4094.

Step	Command	Description
4	<code>Raisecom(config-gigaetherne1/1/port)#exit</code>	Return to global configuration mode.
	<code>Raisecom(config-port-channel1)#exit</code>	
5	<code>Raisecom(config-port)#port backup restore-mode { non-revertive revertive [restore-delay delay-time] }</code>	(Optional) configure the restoration mode and restoration delay of interface backup.
6	<code>Raisecom(config-port)#port backup fault-detect ll dp</code>	Configure the fault detection mode of interface backup.



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 Gazelle S1512i-PWR 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 LAG configuration mode.
3	<code>Raisecom(config-gigaetherne1/1/port)#port backup interface-type backup-interface-number [vlanlist vlan-list]</code>	Configure the interface backup group. In the VLAN list, configure interface <i>backup-interface-number</i> as the backup interface and interface <i>primary-interface-number</i> as the primary interface. If no VLAN list is specified to the interface backup group, the default VLAN range is VLANs 1–4094.
	<code>Raisecom(config-port-channel1)#port backup interface-type backup-interface-number [vlanlist vlan-list]</code>	

Step	Command	Description
4	<pre>Raisecom(config- gigaethernet1/1/port)#port backup interface-type backup- interface-number force-switch</pre> <pre>Raisecom(config-port- channel1)#port backup interface-type backup- interface-number force-switch</pre>	<p>Configure FS on the interface.</p> <p>Use the no port backup [<i>interface-type backup-interface-number</i>] force-switch command to cancel FS. Then, the principles of selecting the current link according to link status are as below:</p> <ul style="list-style-type: none"> • If the Up/Down status of the two interfaces is the same, the primary interface has higher priority. • If the Up/Down status of the two interfaces is different, the Up interface has higher priority.

11.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<pre>Raisecom#show switchport backup</pre>	Show basic information about interface backup.
2	<pre>Raisecom#show port backup group</pre>	Show the status of the interface backup group.

11.2.7 Example for configuring interface backup

Networking requirements

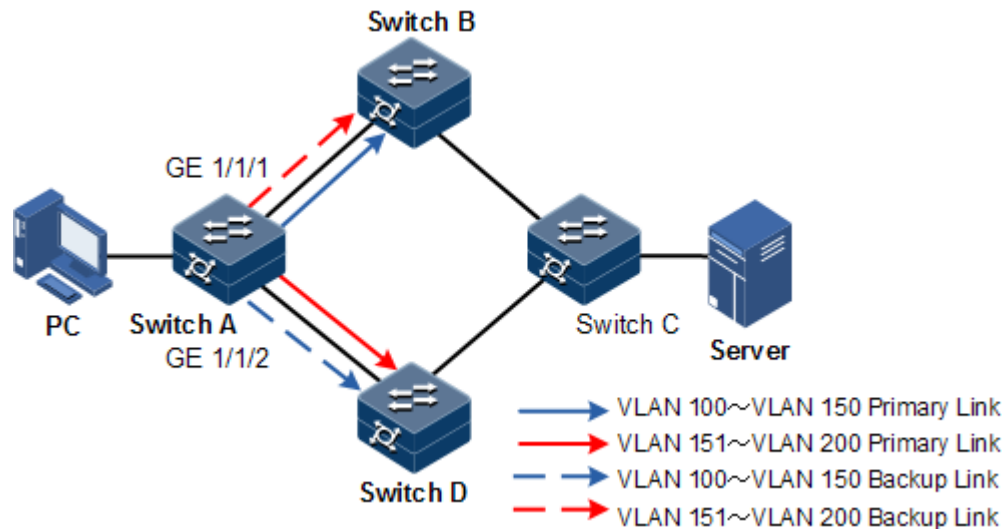
As shown in Figure 11-4, the PC accesses the server through the Switch. To implement a reliable remote access from the PC to the server, configure an interface backup group on Switch A and specify the VLAN list so that the two interfaces concurrently forward services in different VLANs and balance load. 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 11-4 Interface backup networking



Configuration steps

Step 1 Create VLANs 100–200, 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 gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk allowed vlan 100-200
confirm
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 allowed vlan 100-200
confirm
Raisecom(config-gigaethernet1/1/2)#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 gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#port backup gigaethernet 1/1/2
vlanlist 100-150
Raisecom(config-gigaethernet1/1/1)#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 gigaethernet 1/1/2
```

```
Raisecom(config-gigaethernet1/1/2)#port backup gigaethernet 1/1/1  
vlanlist 151-200
```

Checking results

Use the **show port backup group** command to show the 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 Block, 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(Block)	GE1/1/2(Forward)	NO	100-150
GE1/1/2(Forward)	GE1/1/1(Block)	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.

11.3 Link-state tracking

11.3.1 Introduction

Link-state tracking is used to provide port 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, faults of uplink devices can be informed to the downlink devices to trigger switching. Link-state tracking can be used to prevent traffic loss when the uplink fault fails to be sensed by the downstream device.

When all uplink interfaces fail, down link interfaces are configured to Down status. When at least one uplink interface recovers, downlink interfaces will recover to Up status. Therefore, faults of uplink devices can be informed to the downstream devices immediately. Uplink interfaces are not influenced when downlink interfaces fail.

11.3.2 Preparing for configurations

Scenario

When the uplink of an intermediate device fails, traffic will fail to be switched to the standby link and traffic will be interrupted if the uplink fails to notify the downstream device in time.

Link-state tracking can be used to add downlink interfaces and uplink interfaces of the intermediate device to a link-state group and monitor uplink interfaces. When all uplink interfaces fails, faults of uplink devices can be sent to the downstream devices to trigger switching from the active link to the standby link.

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

11.3.4 Configuring link-state tracking



Note

Link-state tracking supports the physical interface or LAG interface.

Configure link-state tracking for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#link-state-tracking group group-number</code>	Create a link-state group, and enable link-state tracking.
3	<code>Raisecom(config)#link-state-tracking group group-number action { block-vlan delete-vlan flush-erps modify-pvid suspend-vlan }</code>	Configure the fault processing mode on the link-state group.
4	<code>Raisecom(config)#link-state-tracking group group-number trap { enable disable }</code>	Configure Trap sending on link-state tracking.
5	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.

Step	Command	Description
6	<code>Raisecom(config-gigaethernet1/1/port)#link-state-tracking group <i>group-number</i> { downstream upstream }</code>	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.



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* { downstream | upstream }** 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* { downstream | upstream }** command to delete an interface. In this case, if there is no interface in the link-state group and link-state tracking is disabled, this command will delete both the interface and the link-state group.

11.3.5 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	<code>Raisecom#show link-state-tracking group <i>group-number</i> [detail]</code>	Show configurations and status of the link-state group.

12 OAM

This chapter describes principles and configuration procedures of OAM and provide related configuration examples, including the following sections:

- Introduction
- Configuring EFM

12.1 Introduction

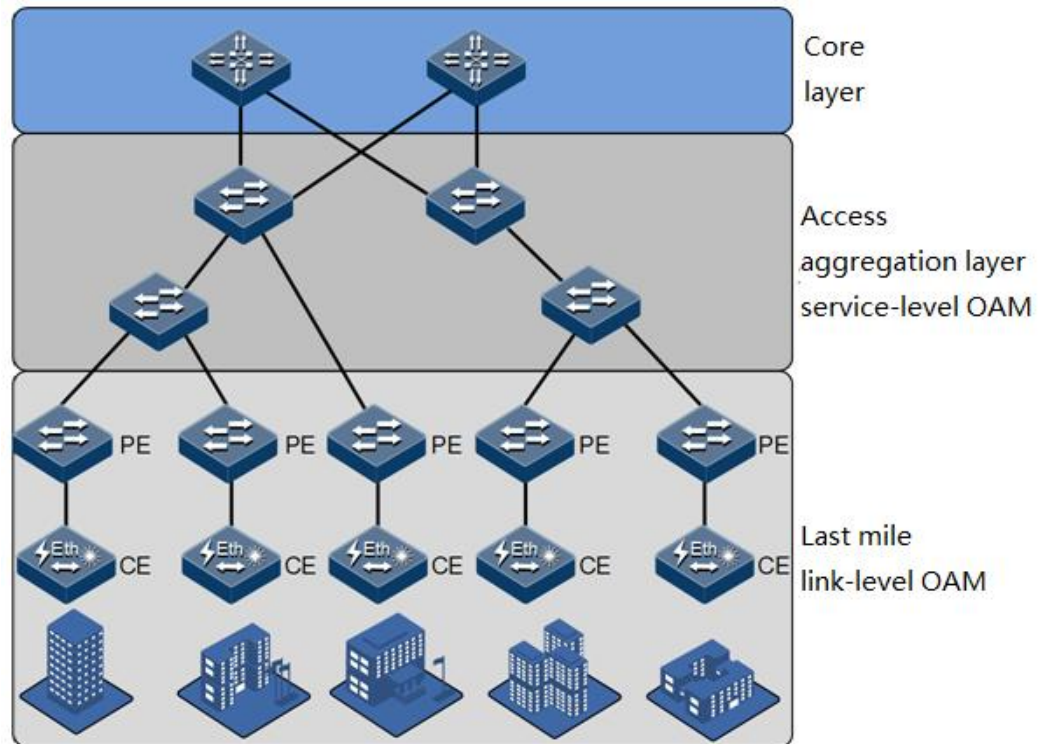
Initially, Ethernet is designed for LAN. Operation, Administration, and Maintenance (OAM) is weak for its small scale and a NE-level administrative system. With constant development of Ethernet technology, the application scale of Ethernet in telecom network becomes wider and wider. Compared with LAN, the link length and network scale for telecom network is bigger and bigger. The lack of effective management and maintenance mechanism has seriously obstructed Ethernet technology to be applied to the telecom network.

To confirm connectivity of Ethernet virtual connection, effectively detect, confirm and locate faults on Ethernet layer, balance network utilization, measure network performance, and provide service according Service Level Agreement (SLA), implementing OAM on Ethernet has becoming an inevitable developing trend.

Ethernet OAM is implemented in different levels, as show in Figure 12-1, and there are two levels:

- **Link-level Ethernet OAM:** it is applied in Ethernet physical link (that is the first mile) between Provider Edge (PE) and Customer Edge (CE), which is used to monitor link state between the user network and carrier network, and the typical protocol is Ethernet in the First Mile (EFM) OAM protocol.
- **Business-level Ethernet OAM:** it is applied in access aggregation layer of network, which is used to monitor connectivity of the whole network, locate connectivity fault of network, monitor and control performance of link, and the typical protocol is Connectivity Fault Management (CFM) OAM protocol.

Figure 12-1 OAM classification



Complying with IEEE 802.3ah protocol, Ethernet in the First Mile (EFM) is a link-level Ethernet OAM technology. It provides the link connectivity detection, link fault monitor, and remote fault notification, etc. for a link between two directly connected devices.

"The first mile" in EFM is the connection between the local device of the telecom carrier and client device. The target is that Ethernet technology will be extended to access network market of telecom users, to improve network performance, and reduce cost of device and running. EFM is used in Ethernet link of user access network edge.

The Gazelle S1512i-PWR provides EFM with IEEE 802.3ah standard.

12.2 Configuring EFM

12.2.1 Preparing for configurations

Scenario

To improve the management and maintenance capability of Ethernet links and ensure network running smoothly, deploy EFM between directly connected devices.

Prerequisite

Connect interfaces and configure physical parameters on interfaces. Make the physical layer Up.

12.2.2 Configuring basic functions of EFM

Configure basic functions of EFM for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	raisecom#config	Enter global configuration mode.
2	raisecom(config)#interface gigaethernet interface-number	Enter physical layer interface configuration mode.
3	raisecom(config)#oam send-period period-number timeout time	(Optional) configure the sending period and timeout for OAM PDUs. By default, the period for sending OAM PDU is 1s (namely, the <i>period-number</i> is 10; 10 × 100ms = 1s), and the link timeout is 5s.
4	raisecom(config-gigaethernet1/1/port)#oam { active passive }	(Optional) configure the working mode of EFM. By default, it is passive mode.
5	raisecom(config-gigaethernet1/1/port)#oam enable	Enable link EFM OAM. By default, it is disabled.

12.2.3 Configuring active functions of EFM



Note

The active EFM must be configured when the Gazelle S1512i-PWR is in active mode.

(Optional) configuring device to initiate EFM remote loopback



Note

- You can discover network faults in time by periodically detecting loopbacks. By detecting loopbacks in segments, you can locate exact areas where faults occur and you can troubleshoot these faults.
- When a link is in a loopback status, the Gazelle S1512i-PWR detects all packets but OAM packets received by the link. In this case, data packets of the user fail to be forwarded normally. Therefore, disable this function immediately when no detection is needed.

Configure the Gazelle S1512i-PWR to initiate EFM remote loopback as below.

Step	Command	Description
1	raisecom#config	Enter global configuration mode.
2	raisecom(config)#interface interface-type interface-number	Enter physical interface configuration mode.

Step	Command	Description
3	<code>Raisecom(config-gigaethernet1/1/port)#oam remote-loopback</code>	Enable the physical interface to initiate EFM remote loopback.
4	<code>Raisecom(config-gigaethernet1/1/port)#oam loopback timeout time</code>	(Optional) configure remote loopback timeout on the physical interface. By default, it is 3s.
5	<code>Raisecom(config-gigaethernet1/1/port)#oam loopback retry times</code>	Configure remote loopback retry times on the physical interface. By default, it is 2.
6	<code>Raisecom(config-gigaethernet1/1/port)#no oam remote-loopback</code>	(Optional) disable remote loopback. After detection, disable remote loopback immediately.

(Optional) configuring peer OAM event alarm

Configure peer OAM event alarm for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)# interface gigaethernet interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/port)#oam peer event trap enable</code>	Enable peer OAM event trap and then link monitoring event can be reported to NMS center in time.

(Optional) showing current variable information about peer device



- 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 Gazelle S1512i-PWR supports obtaining OAM information and interface statistics.
- Peer variable cannot be obtained until EFM is connected.

Show current variable information about the peer device for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#show oam peer { link-statistic oam-info } [interface-type interface-number]</code>	Obtain EFM OAM information or variable values about the peer device.

12.2.4 Configuring passive functions of EFM



Note

The passive EFM can be configured regardless of whether the Gazelle S1512i-PWR is in active or passive mode.

(Optional) configuring device to respond to EFM remote loopback



Note

The peer OAM remote loopback will not take effect until the remote loopback response is configured on the local device.

Configure the Gazelle S1512i-PWR to respond to EFM remote loopback as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface gigabitEthernet interface-number</code>	Enter Layer 2 physical interface configuration mode.
3	<code>Raisecom(config-gigabitEthernet1/1/port)#oam loopback { ignore process }</code>	Configure the Layer 2 physical interface to respond to/ignore OAM remote loopback. By default, the Layer 2 physical interface ignores OAM remote loopback.

12.2.5 Configuring link monitoring and fault indication

(Optional) configuring OAM link monitoring



Note

- OAM link monitoring is used to detect and report link errors in different conditions. When detecting a fault on a link, the Gazelle S1512i-PWR provides the peer with the generated time, window, and threshold through OAM event notification packets. The peer receives event notification and reports it to the NMS through SNMP Trap. Besides, the local device can directly report events to the NMS through SNMP Trap.
- By default, the system configures default values of the error generated time, window, and threshold.

Configure OAM link monitoring for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface gigaethernet <i>interface-number</i>	Enter Layer 2 physical interface configuration mode.
3	Raisecom(config- gigaethernet1/1/port)#oam errored- frame window <i>framewindow</i> threshold <i>framethreshold</i>	Configure the monitor window and threshold for an errored frame event. By default, they are 1s and 1 respectively.
4	Raisecom(config- gigaethernet1/1/port)#oam errored- frame-period window <i>frameperiodwindow</i> threshold <i>frameperiodthreshold</i>	Configure the monitor window and threshold for an errored frame period event. By default, they are 1000ms and 1 respectively.
5	Raisecom(config- gigaethernet1/1/port)#oam errored- frame-seconds window <i>framesecwindow</i> threshold <i>framesecsthreshold</i>	Configure the monitor window and threshold for an errored frame second event. By default, they are 60s and 1s respectively.
6	Raisecom(config- gigaethernet1/1/port)#oam errored- symbol-period window <i>sympriodwindow</i> threshold <i>sympriodthreshold</i>	Configure the monitor window and threshold for an errored symbol period event. By default, they are 1s and 1 respectively.

(Optional) configuring OAM fault indication

Configure OAM fault indication for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface gigaethernet <i>interface-number</i>	Enter Layer 2 physical interface configuration mode.
3	Raisecom(config- gigaethernet1/1/port)#oam notify { critical-event dying-gasp errored-frame errored-frame-period errored-frame-seconds errored-symbol-period } enable	Enable OAM fault notification By default, is is enabled.

Step	Command	Description
4	<code>Raisecom(config-gigaetherne t1/1/port)#oam event trap enable</code>	Enable local OAM link event Trap. By default, it is disabled.
5	<code>Raisecom(config-gigaetherne t1/1/port)#oam peer event trap { enable disable }</code>	Enable peer OAM link event Trap. By default, it is disabled.

(Optional) configuring local OAM event alarm

Configure local OAM event alarm for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)# interface gigaetherne t interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config-gigaetherne t1/1/port)#oam event trap enable</code>	Enable local OAM event alarm and then link monitoring event can be reported to NMS in time.

12.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show oam [interface-type interface-number]</code>	Show basic configurations of EFM OAM.
2	<code>Raisecom#show oam loopback [interface-type interface-number]</code>	Show remote loopback configurations of EFM OAM.
3	<code>Raisecom#show oam notify [interface-type interface-number]</code>	Show configurations of link monitoring and fault indication of EFM OAM.
4	<code>Raisecom#show oam statistics [interface-type interface-number]</code>	Show statistics on EFM OAM packets.
5	<code>Raisecom#show oam trap [interface-type interface-number]</code>	Show configurations of EFM OAM event alarm.
6	<code>Raisecom#show oam event [interface-type interface-number] [critical]</code>	Show information about local critical faults detected by the EFM OAM interface.

No.	Command	Description
7	Raisecom# show oam peer event [<i>interface-type interface-number</i>] [critical]	Show information about link events or critical faults sent from the EFM OAM peer device to the local interface.
8	Raisecom# show oam peer [<i>interface-type interface-number</i>]	Show information about the peer EFM OAM device.
9	Raisecom# show oam peer { link-statistic oam-info } [<i>interface-type interface-number</i>]	Show information about the peer EFM OAM and interface statistical variable.

12.2.7 Maintenance

Maintain the Gazelle S1512i-PWR as below.

Command	Description
Raisecom(config-gigaethernet1/1/1)# clear oam statistics	Clear statistics on links of the EFM OAM interface.
Raisecom(config-gigaethernet1/1/1)# clear oam event	Clear EFM OAM link events.
Raisecom(config)# clear oam config	Clear EFM OAM configurations.

13 System management

This chapter describes principles and configuration procedures of system management and maintenance, and provides related configuration examples, including the following sections:

- SNMP
- KeepAlive
- RMON
- LLDP
- Optical module DDM
- System log
- Alarm management
- Hardware environment monitoring
- CPU monitoring
- Cable diagnosis
- Memory monitoring
- Ping
- Traceroute

13.1 SNMP

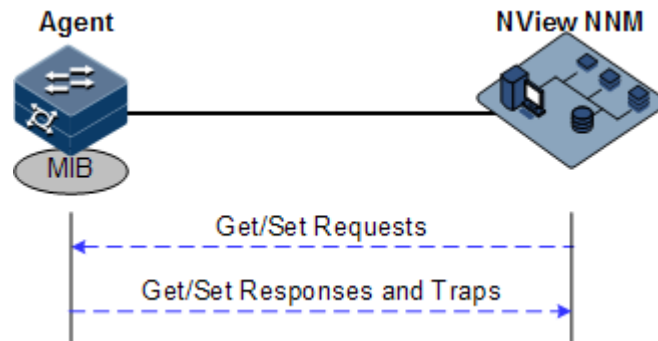
13.1.1 Introduction

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 13-1 shows the SNMP principle.

Figure 13-1 Principles of SNMP



The Raisecom NView NNM system can provide friendly Human Machine Interface (HMI) to facilitate network management. It has the following functions:

- 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 Gazelle S1512i-PWR when conditions are satisfied; replying module sends Trap packets to the NView NNM system through agent to report current status of the Gazelle S1512i-PWR.

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.

Protocol versions

Till now, SNMP has three versions: v1, v2c, and v3, described as below.

- SNMPv1 uses the 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 Gazelle S1512i-PWR, the packet will be discarded.
- Compatible with SNMPv1, SNMPv2c also uses the community name authentication mechanism. SNMPv2c supports more operation types, data types, and errored codes, and thus better identifying errors.
- SNMPv3 uses the 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 Gazelle S1512i-PWR 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 Gazelle S1512i-PWR.

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 packets can access network devices by checking the nodes in MIB tree directory.

The Gazelle S1512i-PWR supports standard MIB and Raisecom-customized MIB.

13.1.2 Preparing for configurations

Scenario

Before logging in to the Gazelle S1512i-PWR through NMS, configure SNMP basic functions for the Gazelle S1512i-PWR.

Prerequisite

Configure the routing protocol and ensure that the route between the Gazelle S1512i-PWR and NMS is reachable.

13.1.3 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) Index CommunityName ViewName Permission 1 public internet ro 2 private internet rw
SNMP access group	initialnone and initial access groups (default)
SNMP user	none, md5nopriv, shapriv, md5priv, and shanopriv users (default)

Function	Default value																								
Mapping between SNMP user and access group	<table border="1"> <thead> <tr> <th>Index</th> <th>GroupName</th> <th>UserName</th> <th>SecModel</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>initialnone</td> <td>none</td> <td>usm</td> </tr> <tr> <td>1</td> <td>initial</td> <td>md5priv</td> <td>usm</td> </tr> <tr> <td>2</td> <td>initial</td> <td>shapriv</td> <td>usm</td> </tr> <tr> <td>3</td> <td>initial</td> <td>md5nopriv</td> <td>usm</td> </tr> <tr> <td>4</td> <td>initial</td> <td>shanopriv</td> <td>usm</td> </tr> </tbody> </table>	Index	GroupName	UserName	SecModel	0	initialnone	none	usm	1	initial	md5priv	usm	2	initial	shapriv	usm	3	initial	md5nopriv	usm	4	initial	shanopriv	usm
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 administrator	support@Raisecom.com																								
Device physical location	world china raisecom																								
Trap	Enable																								
SNMP target host address	N/A																								
SNMP engine ID	800022B603000E5E000016																								

13.1.4 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 Gazelle S1512i-PWR 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#snmp-server view view-name oid-tree [mask] { excluded included }</code>	(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.
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 view view-name option is empty.

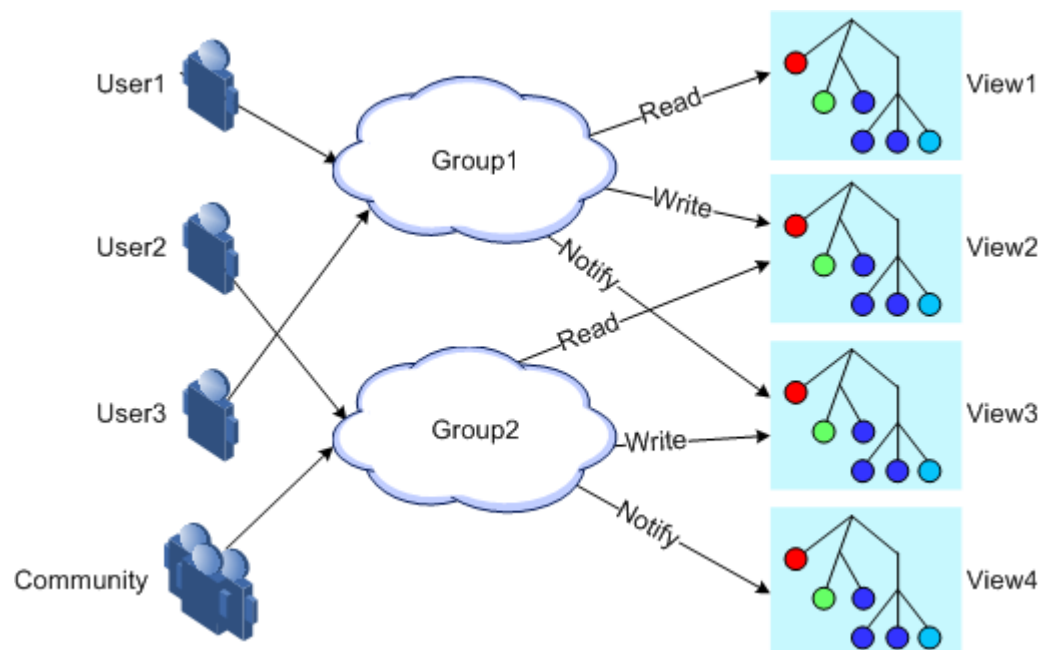
13.1.5 Configuring basic functions of SNMPv3

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 requests must have permission corresponding to the request, otherwise the request will not be accepted.

As shown in Figure 13-2, 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 13-2 Principles of SNMPv3 authentication



Configure basic functions of SNMPv3 for the Gazelle S1512i-PWR as below.

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

Step	Command	Description
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.

13.1.6 Configuring IP address authentication by SNMP server

Configure IP address authentication by SNMP server for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#snmp-server server-auth enable</code>	Enable 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.
4	<code>Raisecom(config)#snmp-server access-list { ipv4-acl-number ipv6-acl-number }</code>	Configure the SNMP ACL IP list.

13.1.7 Configuring other information about SNMP


Other information about SNMP includes:

- Logo and contact method of the administrator: used to identify and contact the administrator
- Physical location of the device: device location

SNMPv1, SNMPv2c, and SNMPv3 support configuring this information.

Configure other information about SNMP for the Gazelle S1512i-PWR as below.

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

Step	Command	Description
2	<code>Raisecom(config)#snmp-server contact <i>contact</i></code>	(Optional) configure the logo and contact method of the administrator.  Note For example, configure the Email to the logo and contact method of the administrator.
3	<code>Raisecom(config)#snmp-server location <i>location</i></code>	(Optional) specify the physical location of the device.

13.1.8 Configuring Trap



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 Gazelle S1512i-PWR 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. For SNMPv1/v2c, configure the community name; for SNMPv3, configure the user name and SNMP view.
- Configure the routing protocol and ensure that the route between the Gazelle S1512i-PWR and NMS is available.

Configure Trap of SNMP for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#snmp-server host <i>ip-address</i> version 3 { authnopriv authpriv noauthnopriv } <i>user-name</i> [udpport <i>udpport</i>]</code>	(Optional) configure the SNMPv3 Trap target host.
3	<code>Raisecom(config)#snmp-server host <i>ip-address</i> version { 1 2c } <i>community-name</i> [udpport <i>udpport</i>]</code>	(Optional) configure the SNMPv1/SNMPv2c Trap target host.
4	<code>Raisecom(config)#snmp-server enable traps</code>	Enable Trap.

13.1.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show snmp access</code>	Show configurations of SNMP access groups.
2	<code>Raisecom#show snmp community</code>	Show configurations of SNMP communities.
3	<code>Raisecom#show snmp config</code>	Show basic configurations of SNMP, including the local SNMP engine ID, logo and contact method of the administrator, physical location of the device, and Trap status.
4	<code>Raisecom#show snmp group</code>	Show the mapping between SNMP users and the access group.
5	<code>Raisecom#show snmp host</code>	Show information about the Trap target host.
6	<code>Raisecom#show snmp statistics</code>	Show SNMP statistics.
7	<code>Raisecom#show snmp user</code>	Show information about SNMP users.
8	<code>Raisecom#show snmp view</code>	Show information about SNMP views.
9	<code>Raisecom#show snmp server-auth</code>	Show configurations of the SNMP server authentication.
10	<code>Raisecom# show snmp access-list</code>	Show information about access and authentication by the SNMP server.

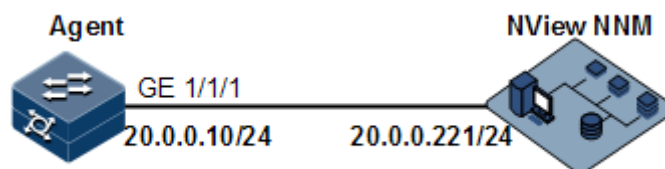
13.1.10 Example for configuring SNMPv1/SNMPv2c and Trap

Networking requirements

As shown in Figure 13-3, the route between the NView NNM system and the Gazelle S1512i-PWR is available. The NView NNM system can check the MIB under view corresponding to the remote Switch by SNMPv1/SNMPv2c, and the Gazelle S1512i-PWR can send Trap automatically to the NView NNM system in emergency.

By default, there is VLAN 1 on the Gazelle S1512i-PWR and all physical interfaces belong to VLAN 1.

Figure 13-3 SNMPv1/SNMPv2c networking



Configuration steps

Step 1 Configure the IP address of the Gazelle S1512i-PWR.

```
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  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
```

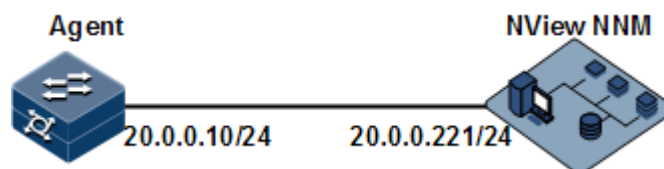
13.1.11 Example for configuring SNMPv3 and Trap

Networking requirements

As shown in Figure 13-4, the route between the NView NNM system and Gazelle S1512i-PWR is available, the NView NNM system monitors the Agent through SNMPv3, and the Gazelle S1512i-PWR can send Trap automatically to the NView NNM system when the Agent is in emergency.

By default, there is VLAN 1 on the Gazelle S1512i-PWR and all physical interfaces belong to VLAN 1.

Figure 13-4 SNMPv3 and Trap networking



Configuration steps

Step 1 Configure the IP address of the Gazelle S1512i-PWR.

```
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 into 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
```

13.2 KeepAlive

13.2.1 Introduction

The KeepAlive packet is a kind of KeepAlive mechanism running in High-level Data Link Control (HDLC) link layer protocol. The Gazelle S1512i-PWR will send a KeepAlive packet to confirm whether the peer is online periodically to implement the neighbor detection mechanism.

Trap is the unrequested information sent by the Gazelle S1512i-PWR actively to the NView NNM system, used to report some urgent and important events.

The Switch sends KeepAlive Trap actively which includes the basic information about RC551E (device name, device OID, MAC address and IP address) to the NView NNM system. Network management synchronizes device information by IP to make the NView NNM system discover fault in a short time, improve working efficiency and reduce working load of administrators.

13.2.2 Preparing for configurations

Scenario

The Gazelle S1512i-PWR sends KeepAlive packet to make network management discover segment in a short time, improve working efficiency, and reduce the working load of administrators. You can configure the switch to enable or disable the KeepAlive transmission and its period. When enabled with KeepAlive Trap switch, configure with the **snmp enable traps** command and Layer 3 IP address, the Switch will send a KeepAlive Trap alarm message to all target hosts with Bridge Trap every KeepAlive Trap Interval.

Prerequisite

- Configure basic functions of SNMP. For SNMPv1/v2c, configure the community name; for SNMPv3, configure the user name and SNMP view.
- Configure the routing protocol and ensure that the route between the Gazelle S1512i-PWR and NMS is reachable.

13.2.3 Default configurations of KeepAlive

Default configurations of KeepAlive are as below.

Function	Default value
KeepAlive Trap	Disable
KeepAlive Trap period	300s

13.2.4 Configuring KeepAlive

Configure KeepAlive for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	raisecom#config	Enter global configuration mode.
2	raisecom(config)#snmp-server keepalive-trap enable	Enable KeepAlive Trap.
3	raisecom(config)#snmp-server keepalive-trap interval <i>period</i>	(Optional) configure the period for sending KeepAlive Trap.



Caution

To avoid multiple devices sending KeepAlive Trap at the same time according to the same period and causing heavy network management load, configure the real transmission period for sending KeepAlive Trap in random transmission of period+5s period.

13.2.5 Checking configurations

Use the following commands to check configuration results.

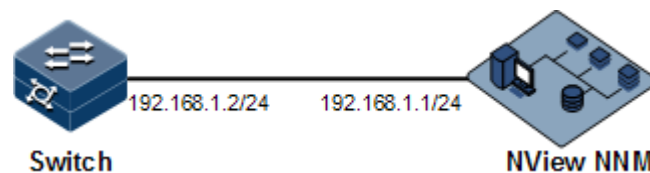
No.	Command	Description
1	<code>Raisecom#show keepalive</code>	Show KeepAlive configurations.

13.2.6 Example for configuring KeepAlive

Networking requirements

As shown in Figure 13-5, the IP address of the Switch is 192.168.1.2, the IP address of the SNMPv2c Trap target host is 192.168.1.1, the name of the read-write community is public, and the SNMP version is v2c. Configure the interval for sending KeepAlive Trap from the Switch to SNMP network management station as 120s, and enable sending KeepAlive Trap.

Figure 13-5 KeepAlive networking



Configuration steps

Step 1 Configure the IP address of the Switch.

```
Raisecom#config  
Raisecom(config)#interface vlan 1  
Raisecom(config-vlan1)#ip address 192.168.1.2 255.255.255.0  
Raisecom(config-vlan1)#exit
```

Step 2 Configure the IP address of the Trap target host for SNMP.

```
Raisecom(config)#snmp-server host 192.168.1.1 version 2c public
```

Step 3 Configure sending KeepAlive Trap.

```
Raisecom(config)#snmp-server keepalive-trap enable  
Raisecom(config)#snmp-server keepalive-trap interval 120
```

Checking results

Use the **show keepalive** command to show KeepAlive configurations.

```
Raisecom#show keepalive
Keepalive Admin State:Enable
keepalive trap interval:120s
keepalive trap count:2
```

13.3 RMON

13.3.1 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 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.

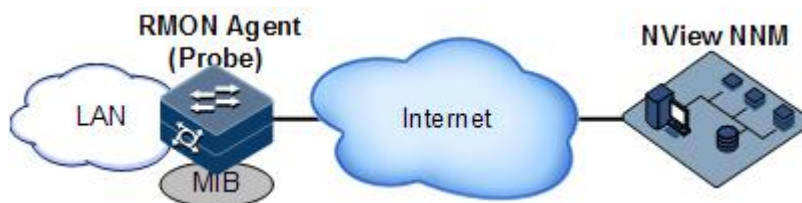
The RMON Agent is commonly referred to as the probe program. RMON Probe can gather the communication subnet statistics and performance analysis. Whenever it finds network failure, RMON Probe can report the NView NNM system, and describes the capture information under unusual circumstances so that the 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 as below:

- Distributed RMON. The NMS 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. The NMS will collect network management information through the basic operation of SNMP and the exchange data information about RMON Agent.

The Raisecom Gazelle S1512i-PWR is embedded with RMON. As shown in Figure 13-6, the Gazelle S1512i-PWR implements RMON Agent function. Through this function, the management station can obtain the overall flow, error statistics and performance statistics on this segment connected to the managed network device interface so as to achieve the monitoring to one segment.

Figure 13-6 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:** gather statistics about each interface, including receiving packets accounts and size distribution statistics.
- **History group:** similar with statistic group, it only gather statistics in an assigned detection period.
- **Alarm group:** monitor an assigned MIB object, configure upper threshold and lower threshold in assigned time interval, and trigger an event if the monitor object receives threshold value.
- **Event group:** cooperating with the alarm group. When an alarm triggers an event, it records the event, such as sending Trap, and writes the event into log.

13.3.2 Preparing for configurations

Scenario

RMON helps monitor and account network traffic.

Compared with SNMP, RMON is a more high-efficient monitoring method. After you specifying the alarm threshold, the Gazelle S1512i-PWR actively sends alarms when the threshold is exceeded without obtaining variable information. This helps reduce traffic of the Central Office (CO) and managed devices and facilitates network management.

Prerequisite

The route between the Gazelle S1512i-PWR and the NView NNM system is reachable.

13.3.3 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

13.3.4 Configuring RMON statistics

RMON statistics is used to gather statistics about 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#rmon statistics interface-type interface-list [owner owner-name]</code>	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.

13.3.5 Configuring RMON historical statistics

Configure RMON historical statistics for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#rmon history interface-type interface-list [shortinterval short-period] [longinterval long-period] [buckets buckets-number] [owner owner-name]</code>	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.

13.3.6 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 Gazelle S1512i-PWR as below.

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

13.3.7 Configuring RMON event group

Configure the RMON event group for the Gazelle S1512i-PWR 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.

13.3.8 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.

No.	Command	Description
4	<code>Raisecom#show rmon statistics [interface-type interface-list]</code>	Show information about the RMON statistics group.
5	<code>Raisecom#show rmon history interface-type interface-list</code>	Show information about the RMON history group.

13.3.9 Maintenance

Maintain the Gazelle S1512i-PWR as below.

Command	Description
<code>Raisecom(config)#clear rmon</code>	Clear all RMON configurations.

13.3.10 Example for configuring RMON alarm group

Networking requirements

As shown in Figure 13-7, the Gazelle S1512i-PWR 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 1/1/1. When packets received on GE 1/1/1 exceeds the threshold in a period, logs are recorded and Trap is sent.

Figure 13-7 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 event 1 log description High-ifOutErrors owner
system
    
```

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 messages 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 Gazelle S1512i-PWR.

```
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 Gazelle S1512i-PWR.

```
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.

13.4 LLDP

13.4.1 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. The NMS 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 the NMS querying and judging link communication.

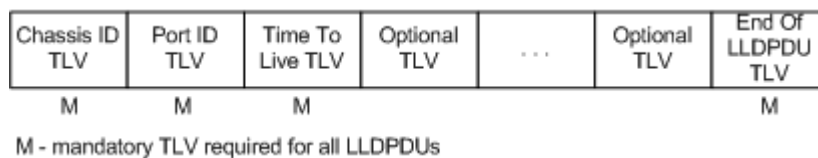
LLDP packet

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 13-8, LLDPDU is made by several TLV, including 4 mandatory TLV and several optional TLV.

Figure 13-8 Structure of a LLDPDU



As shown in Figure 13-9, each TLV denotes a piece of information about the local device. For example the device ID and interface ID correspond with the Chassis ID TLV and Port ID TLV, which are fixed TLVs.

Figure 13-9 Structure of a TLV packet

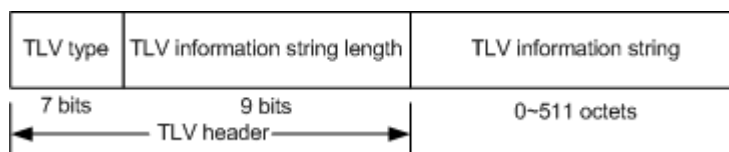


Table 13-1 lists TLV types. At present only types 0-8 are used.

Table 13-1 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

TLV type	Description	Optional/Required
7	System capabilities	Optional
8	Management address	Optional

Principles

LLDP is a 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 Gazelle S1512i-PWR sends a LLDP packet to the peer. To avoid sending LLDP packet continuously because of frequency change of device status, you can configure a delay timer for sending the LLDP packet.

The aging time of Time To Live (TTL) of local device information in the neighboring node can be adjusted by modifying the parameter values of aging coefficient, sends LLDP packets to neighboring node, after receiving LLDP packets, neighboring node will adjust the aging time of its neighboring 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 neighboring node.
- Hold-multiplier refers to the aging coefficient of device information in neighboring node.

13.4.2 Preparing for configurations

Scenario

When you obtain connection information between devices through NView NNM system for topology discovery, the Gazelle S1512i-PWR 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

13.4.3 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 packet	0180.c200.000e

13.4.4 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 Gazelle S1512i-PWR 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#lldp enable</code>	Enable global LLDP.

13.4.5 Enabling interface LLDP

Enable interface LLDP for the Gazelle S1512i-PWR 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)#lldp enable</code>	Enable LLDP on an interface.

13.4.6 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 Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#lldp message-transmission interval <i>period</i>	(Optional) configure the period timer of the LLDP packet.
3	Raisecom(config)#lldp message-transmission delay <i>period</i>	(Optional) configure the delay timer of the LLDP packet.
4	Raisecom(config)#lldp message-transmission hold-multiplier <i>hold-multiplier</i>	(Optional) configure the aging coefficient of the LLDP packet.
5	Raisecom(config)#lldp restart-delay <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.

13.4.7 Configuring LLDP Trap

When the network changes, you need to enable LLDP alarm notification function to send topology update Trap to the NView NNM system immediately.

Configure LLDP Trap for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#lldp trap-interval <i>period</i>	(Optional) configure the period of the timer for sending LLDP Trap.

13.4.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show lldp local config	Show local configurations of LLDP.

No.	Command	Description
2	Raisecom# show lldp local system-data [<i>interface-type interface-number</i>]	Show information about the LLDP local system.
3	Raisecom# show lldp remote [<i>interface-type interface-number</i>] [detail]	Show information about the LLDP neighbor.
4	Raisecom# show lldp statistic [<i>interface-type interface-number</i>]	Show statistics on LLDP packets.

13.4.9 Maintenance

Maintain the Gazelle S1512i-PWR as below.

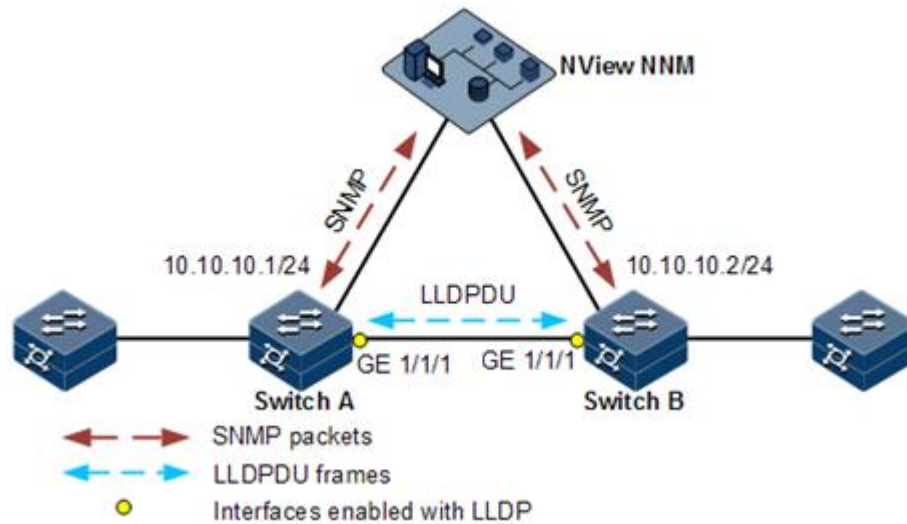
Command	Description
Raisecom(config)# clear lldp statistic <i>interface-type interface-number</i>	Clear LLDP statistics.
Raisecom(config)# clear lldp remote-table [<i>interface-type interface-number</i>]	Clear LLDP neighbor information.
Raisecom(config)# clear lldp global statistic	Clear global LLDP statistics.

13.4.10 Example for configuring LLDP

Networking requirements

As shown in Figure 13-10, 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 13-10 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 gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport access vlan 1024
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface vlan 1
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 1
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.C200.000E
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

.....

```
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				

.....

13.5 Optical module DDM

13.5.1 Introduction

Optical module Digital Diagnostics Monitoring (DDM) on the Gazelle S1512i-PWR 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 analyzes 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.

13.5.2 Preparing for configurations

Scenario

Fault diagnostics of optical modules provide a detection method to 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

N/A

13.5.3 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

13.5.4 Enabling optical module DDM

Enable optical module DDM for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#transceiver ddm enable</code>	Enable SFP DDM globally.
3	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.

Step	Command	Description
4	<code>Raisecom(config-gigaethernet1/1/port)#transceiver ddm enable</code>	Enable interface optical module DDM. Only when global optical DDM is enabled, the optical module, where interface optical module DDM is enabled, can the Gazelle S1512i-PWR perform DDM.

13.5.5 Enabling optical module DDM Trap

Enable optical module DDM Trap for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#snmp-server trap transceiver enable</code>	Enable optical module DDM Trap globally.
3	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
4	<code>Raisecom(config-gigaethernet1/1/port)#transceiver trap enable</code>	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 Gazelle S1512i-PWR send Traps.

13.5.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show transceiver</code>	Show global optical module DDM and interface optical module DDM configurations.
2	<code>Raisecom#show transceiver ddm interface-type interface-list [detail]</code>	Show optical module DDM performance parameters.
3	<code>Raisecom#show transceiver interface-type interface-list history [15m 24h]</code>	Show historical information about optical module DDM.
4	<code>Raisecom#show transceiver information interface-type interface-list</code>	Show basic information about the optical module.
5	<code>Raisecom#show transceiver threshold-violations interface-type interface-list</code>	Show the information when the optical module parameters exceed the thresholds.

13.6 System log

13.6.1 Introduction

The system log refers that the Gazelle S1512i-PWR records the system information and debugging information in a log and sends the log to the specified destination. When the Gazelle S1512i-PWR 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 process. According to the configuration, the system will send the log to various destinations. The destinations that receive the system log are divided into:

- Console: send the log message to the local console through Console interface.
- Host: send the log message to the host.
- Monitor: send the log message to the monitor, such as Telnet terminal.
- 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 13-2.

Table 13-2 Log levels

Severity	Level	Description
Emergency	0	The system cannot be used.
Alert	1	Need to process 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, namely, the severity ranges from emergencies to errors, can be sent.

13.6.2 Preparing for configurations

Scenario

The Gazelle S1512i-PWR generates the 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

13.6.3 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"> • Debug: no timestamp to debug level (7) Syslog information. • Log: The timestamp to 0–6 levels Syslog information is absolute time.

13.6.4 Configuring basic information of system log

Configure basic information of system log for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#logging on</code>	(Optional) enable system log.

Step	Command	Description
3	<code>Raisecom(config)#logging time-stamp { debug log } { datetime none uptime }</code>	(Optional) configure timestamp for system log. The optional parameter debug is used to assign debug level (7) system log timestamp; by default, this system log does not have timestamp The optional parameter log is used to assign debug level 0–6 system log timestamp; by default, this system log adopts date-time as timestamp.
4	<code>Raisecom(config)#logging rate-limit log-num</code>	(Optional) configure transmitting rate of system log.
5	<code>Raisecom(config)#logging sequence-number</code>	(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	<code>Raisecom(config)#logging discriminator discriminator-number { facility mnemonics msg-body } { { drops includes } key none }</code>	(Optional) create and configure system log filter. The filter can filter output log from the console, monitor, log file and log buffer.
7	<code>Raisecom(config)#logging buginf [high normal low none]</code>	(Optional) configure the sending of Debug-level logs.

13.6.5 Configuring system log output

Configure system log output for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#logging console [log-level alerts critical debugging emergencies errors informational notifications warnings discriminator discriminator-number]</code>	(Optional) output system logs to the console.
3	<code>Raisecom(config)#logging host ip-address [log-level alerts critical debugging emergencies errors informational notifications warnings discriminator discriminator-number]</code>	(Optional) output system logs to the log host. Up to 10 log hosts are supported.

Step	Command	Description
	<code>Raisecom(config)#logging [host ip-address] facility { alert audit auth clock cron daemon ftp kern local0 local1 local2 local3 local4 local5 local6 local7 lpr mail news ntp security syslog user uucp }</code>	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 Gazelle S1512i-PWR.
4	<code>Raisecom(config)#logging monitor [log-level alerts critical debugging emergencies errors informational notifications warnings discriminator discriminator-number]</code>	(Optional) output system logs to the monitor.
5	<code>Raisecom(config)#logging file [discriminator discriminateor-number]</code>	(Optional) output system logs to the Flash of the Gazelle S1512i-PWR. Only warning-level logs are available.
6	<code>Raisecom(config)#logging buffered [log-level alerts critical debugging emergencies errors informational notifications warnings discriminator discriminator-number]</code>	(Optional) output system logs to the buffer.
	<code>Raisecom(config)#logging buffered size size</code>	(Optional) configure the system log buffer size.
7	<code>Raisecom(config)#logging history</code>	(Optional) output system logs to the log history list. The level of the output logs is the one of the translated Trap.
	<code>Raisecom(config)#logging history size size</code>	(Optional) configure the log history list size.
	<code>Raisecom(config)#logging trap [log-level alerts critical debugging emergencies errors informational notifications warnings discriminator discriminator-number]</code>	(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.

13.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show logging	Show configurations of system log.
2	Raisecom#show logging buffer	Show information about the system log buffer.
3	Raisecom#show logging discriminator	Show filter information.
4	Raisecom#show logging file	Show contents of system log.
5	Raisecom#show logging history	Show information about the system log history list.

13.6.7 Maintenance

Maintain the Gazelle S1512i-PWR as below.

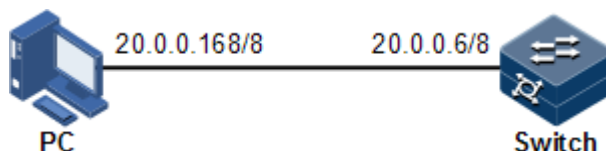
Command	Description
Raisecom(config)#clear logging buffer	Clear log information in the buffer.
Raisecom(config)#clear logging statistics	Clear log statistics.

13.6.8 Example for configuring outputting system logs to log host

Networking requirements

As shown in Figure 13-11, configure system log, and output device log information to log host for user to check.

Figure 13-11 Networking of outputting system log to log host



Configuration steps

Step 1 Configure the IP address of the Gazelle S1512i-PWR.

```
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
```

13.7 Alarm management

13.7.1 Introduction

Alarm means when a fault is generated on the Gazelle S1512i-PWR or some working condition changes, the system will generate alarm information 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 information is generated to log information. If a Network Management System (NMS), the alarm information will be sent to the NMS through SNMP. The information sent to the NMS is called Trap information.

Alarm classification

Alarms can be divided into three types by property:

- 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 by function:

- 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 information output modes:

- Alarm buffer: alarm information is recorded in tabular form, including the current alarm table and history alarm table.
 - Current alarm table, recording alarm information which is not cleared, acknowledged or restored.
 - History alarm table, consisting of acknowledged and restored alarm information, recording the cleared, auto-restored or manually acknowledged alarm information.
- Log: alarm information is generated to system log when recorded in the alarm buffer, and stored in the alarm log buffer.
- Trap information: alarm information sent to NMS when the NMS is configured.

Alarm will be broadcasted according to various terminals configured by the Gazelle S1512i-PWR, including CLI terminal and NMS.

Log output of alarm information starts with the symbol "#", and the output format is as below:

#Index TimeStamp HostName ModuleName/Severity/name:Arise From Description.

Table 13-3 lists alarm fields.

Table 13-3 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 13-4.

Table 13-4 Alarm levels

Level	Description	Syslog
Critical (3)	This alarm has affected system services and requires immediate troubleshooting. Restore the device or source immediately if they are completely unavailable, even it is not during working time.	1 (Alert)
Major (4)	This alarm has affected the service quality and requires immediate troubleshooting. Restore the device or source service quality if they decline; or take measures immediately during working hours to restore all performances.	2 (Critical)
Minor (5)	This alarm has not influenced the existing service yet, which needs further observation and take measures at appropriate time 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 Gazelle S1512i-PWR 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 Gazelle S1512i-PWR can effectively reduce the number of alarms.

Alarm A and alarm B will be recorded on the Gazelle S1512i-PWR 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 Gazelle S1512i-PWR.

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 information, or report the alarm when there is no alarm information. 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 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 status 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.

- Auto-reverse mode

Configure the alarm reverse mode as auto-reverse mode. If the interface has not actual reverse alarm currently, the configuration will return fail; if the interface has actual reverse alarm, the configuration is success and enter reverse mode, i.e. the interface reported alarm status is changed opposite to the actual alarm status immediately. After the alarm is finished, the enabling status of interface alarm reverse will ends automatically and changes to non-reverse alarm mode so that the alarm status can be reported normally in next alarm.

- Alarm delay

Alarm delay refers that the Gazelle S1512i-PWR 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 when 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 information and take rolling records.

Process new generated alarm information in configured storage mode 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 information directly on the Gazelle S1512i-PWR. If the Gazelle S1512i-PWR is configured with the NView NNM system, the administrator can monitor alarms on the NView NNM system.

13.7.2 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 information 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 information 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.

13.7.3 Default configurations of alarm management

Default configurations of alarm management are as below.

Function	Default value
Alarm monitoring	Enable
Alarm delay	0s
Alarm storage mode	stop
Alarm auto-reporting	Enable
Alarm clearance delay	0s
Alarm inhibition	Enable
Relativity alarm inhibition	Enable
Alarm reverse mode	Non-reverse
Output alarms to system logs	Disable

13.7.4 Configuring basic functions of alarm management

Configure basic information of alarm management for the Gazelle S1512i-PWR as below.

All following steps are optional and in any sequence.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#alarm inhibit enable</code>	(Optional) Enable alarm inhibition. By default, it is enabled.

Step	Command	Description
3	Raisecom(config)#alarm auto-report all enable	Enable alarm auto-reporting.
	Raisecom(config)#alarm auto-report alarm-restype alarm-restype-value enable	Enable alarm auto-reporting of a specified alarm source.
	Raisecom(config)#alarm auto-report type alarm-type enable	Enable alarm auto-reporting of a specified alarm type.
	Raisecom(config)#alarm auto-report type alarm-type alarm-restype alarm-restype-value enable	Enable alarm auto-reporting of a specified alarm source and type.
4	Raisecom(config)#alarm monitor all enable	Enable alarm monitoring.
	Raisecom(config)#alarm monitor alarm-restype alarm-restype-value enable	Enable alarm monitoring of a specified alarm source.
	Raisecom(config)#alarm monitor type alarm-type enable	Enable alarm monitoring of a specified alarm type.
	Raisecom(config)#alarm monitor type alarm-type alarm-restype alarm-restype-value enable	Enable alarm monitoring of a specified alarm source and type.
5	Raisecom(config)#alarm inverse interface-type interface-number { none auto manual }	Configure alarm reverse modes. By default, it is none; in other words, alarm reverse is disabled.
6	Raisecom(config)#alarm { active cleared } delay second	Configure alarm delay. By default, it is 0s.
7	Raisecom(config)#alarm active storage-mode { loop stop }	Configure alarm storage modes. By default, it is stop.
8	Raisecom(config)#alarm clear all	(Optional) clear all current alarms.
	Raisecom(config)#alarm clear index index	(Optional) clear current alarms of the specified alarm index.
	Raisecom(config)#alarm clear alarm-restype alarm-restype-value	(Optional) clear current alarms of the specified alarm source.
	Raisecom(config)#alarm clear type alarm-type	(Optional) clear current alarms of the specified alarm type.
	Raisecom(config)#alarm clear type alarm-type alarm-restype alarm-restype-value	(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.

13.7.5 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 on alarm management module.
4	<code>Raisecom#show alarm active</code>	Show information about current alarms.

13.8 Hardware environment monitoring

13.8.1 Introduction

Hardware environment monitoring mainly refers to monitor the running environment of the Gazelle S1512i-PWR. The monitoring alarm events include:

- Power supply status alarm
- Temperature beyond threshold alarm
- Abnormal interface status 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.
- Output alarms to the relay indication LED.

You can take appropriate measures to prevent failure when alarm events happen.

Alarm events

- Power supply monitoring alarms

Power supply status alarms include 2 types.

- Power supply voltage anomaly alarm

An alarm is generated when the power supply voltage is 20% greater than the preconfigured voltage (12 V) or is 20% smaller than the preconfigured voltage (12 V). In addition, an alarm is generated when the voltage value returns to normal status. The Gazelle S1512i-PWR 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.

- Power supply status change alarms

Power supply status change refers that unplugged power supply is plugged into the device and vice versa. The Gazelle S1512i-PWR supports dual power supplies. Therefore, power supply status change alarms are divided into the single power supply status change alarm and device dying gasp alarm.

- Dual power supply status change alarm: notify uses that power supply 1/power supply 2 changes. The Gazelle S1512i-PWR 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, namely, two power modules are out of position. The Gazelle S1512i-PWR 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 Gazelle S1512i-PWR 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 Gazelle S1512i-PWR 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.

- Interface status alarm

Each interface has two alarm events:

- Interface link-fault alarm: link failure alarm refers to the peer link signal loss. The alarm event only aims at optical port, but not power port.
- Interface link-down alarm: interface status Down alarm.

The Gazelle S1512i-PWR supports saving these two types of alarm events 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 information 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 information 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 13-5 describes Trap information.

Table 13-5 Trap information

Field	Description
Alarm status	<ul style="list-style-type: none"> • asserted (current alarm) • cleared (alarm recovery) • clearall (clear all alarm information)
Alarm source	<ul style="list-style-type: none"> • device (global alarm) • Interface number (interface status alarm)
Timestamp	Alarm time, in the form of absolute time
Alarm event type	<ul style="list-style-type: none"> • dev-power-down (power-down alarm) • power-abnormal (power-abnormal alarm, one of two powers is power down.) • high-temperature (high-temperature alarm) • low-temperature (low-temperature alarm) • high-volt (high-voltage alarm) • low-volt (low-voltage alarm) • link-down (interface LinkDown alarm) • link-falut (interface LinkFault alarm) • all-alarm (clear all alarm information)

- Syslog output

Record alarm information to Syslog.

Syslog output has global switch and all monitored alarm events still have their own Syslog alarm output switches. When enabling the global switch and monitored alarm events switches simultaneously, the alarm will generate Syslog output.

Table 13-6 describes Syslog information.

Table 13-6 Syslog information

Field	Description
Facility	The module name generating alarm, the hardware environment monitoring module is fixed at alarm.
Severity	Level, the same as defined in system logs. For details, see Table 13-2.
Mnemonics	Alarm event type. For details, see Table 13-5.
Msg-body	Main body, describing alarm event contents.

- Relay output

Outputting to relay or outputting from relay indicates outputting alarms to the relay and fault indication LED simultaneously. The relay and fault indication LED are bound together. Relay output and fault indication LED output are controlled by the relay alarm output switch. As a public fault output mode for all alarms, the relationship among all alarms is logical OR.

If any alarm is generated on the Gazelle S1512i-PWR, the device outputs the alarm from the relay. The relay cannot work properly unless all alarms are cleared.

Relay output cannot be enabled globally. Relay output is enabled for every monitored alarm.

13.8.2 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 information to the system log host, please configure system log host IP address for the device.
- In Trap output mode: please configure the NMS IP address for the device.
- In relay output mode: relay alarm output switch is enabled for every alarm.

13.8.3 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	<ul style="list-style-type: none"> • Enable Trap output. • Enable Syslog system log output. • Enable relay output.
Temperature alarm output	
Interface link-down event alarm output	<ul style="list-style-type: none"> • Enable Trap output. • Enable Syslog system log output. • Disable relay output.
Interface link-fault event alarm output	<ul style="list-style-type: none"> • Disable Trap output. • Disable Syslog system log output. • Disable relay output.
High temperature alarm threshold	102 °C
Low temperature alarm threshold	-40 °C

13.8.4 Enabling global hardware environment monitoring

Enable global hardware environment monitoring for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#logging alarm</code>	(Optional) enable global hardware environment monitoring alarm Syslog output.
3	<code>Raisecom(config)#snmp-server alarm-trap enable</code>	(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.
- When enabling global hardware environment monitoring alarm Relay output, alarm event can generate Relay only when Relay output under alarm event is also enabled.

13.8.5 Configuring temperature monitoring alarm

Configure temperature monitoring alarm for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)# alarm temperature { high high-value low low-value notifies syslog relay }</code>	Enable temperature monitoring alarm output and configure temperature monitoring alarm output modes. <ul style="list-style-type: none"> • The high temperature threshold (high-value) must be greater than the low temperature threshold (low-value). • The low temperature threshold (low-value) must be smaller than the high temperature threshold (high-value).


13.8.6 Configuring power supply alarm

Configure power supply alarm for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)# alarm power- supply { notifies syslog relay }</code>	Enable power supply alarm output, and configure power supply alarm output mode.

13.8.7 Clearing all hardware environment monitoring alarms manually

Clear all hardware environment monitoring alarms manually for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#conf ig</code>	Enter global configuration mode.
2	<code>Raisecom(conf ig)#clear alarm</code>	Clear alarms manually. <div style="margin-top: 10px;">  Note Use this command to clear all alarms in current alarm list and generate an all-alarm alarm in history alarm list. 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. </div>

13.8.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show alarm</code>	Show global hardware environment monitoring alarm configurations.
2	<code>Raisecom#show alarm current</code>	Show current alarms of hardware environment monitoring.
3	<code>Raisecom#show alarm history</code>	Show history alarms of hardware environment monitoring.
4	<code>Raisecom#show environment [temperature voltage power]</code>	Show current power supply, temperature, voltage alarms, and current environment information.

13.9 CPU monitoring

13.9.1 Introduction

The Gazelle S1512i-PWR supports CPU monitoring. It can monitor status, 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.

13.9.2 Preparing for configurations

Scenario

CPU monitoring can give realtime monitoring to task status, CPU utilization rate and stack usage in the system, provide CPU utilization rate threshold alarm, detect and eliminate hidden dangers, or help the administrator for locating faults.

Prerequisite

When the CPU monitoring alarm needs to be output in Trap mode, configure the IP address of the Trap output target host, which is the IP address of the NView NNM system.

13.9.3 Default configurations of CPU monitoring

Default configurations of CPU monitoring are as below.

Function	Default value
Rising threshold of CPU utilization alarm	99%
Restoration threshold of CPU utilization alarm	79%
Sampling period of CPU utilization	60s

13.9.4 Showing CPU monitoring information

Show CPU monitoring information for the Gazelle S1512i-PWR 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 [dead sorted { priority name } taskname]</code>	Show the status of all tasks.
3	<code>Raisecom#show process cpu [sorted [10min 1min 5sec invoked]]</code>	Show CPU utilization of all tasks.

13.9.5 Configuring CPU monitoring alarm

Configure CPU monitoring alarm for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#cpu threshold falling <i>falling-threshold-value</i> rising <i>rising-threshold-value</i></code>	(Optional) configure the recovering threshold and rising threshold for CPU alarms.
3	<code>Raisecom(config)#cpu interval <i>interval-value</i></code>	(Optional) configure the interval for sampling CPU alarms.

13.9.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	raisecom#show cpu-utilization	Show CPU utilization and related configurations.

13.10 Cable diagnosis

13.10.1 Introduction

The Gazelle S1512i-PWR supports cable diagnosis, which helps you detect lines.

Cable diagnosis contains the following results:

- Detection result of the Tx cable
- Errored location of the Tx cable
- Detection result of the Rx cable
- Errored location of the Rx cable

13.10.2 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

13.10.3 Configuring cable diagnosis

Configure cable diagnosis for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	raisecom#test cable-diagnostics <i>interface-type interface-number</i>	Enable cable diagnosis.

13.10.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	raisecom#show cable-diagnostics [<i>interface-type interface-number</i>]	Show results of cable diagnosis on the interface.

13.11 Memory monitoring

13.11.1 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.

13.11.2 Configuring memory monitoring

Configure memory monitoring for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	<code>Raisecom(config)#memory threshold recovering recovering-threshold-value rising rising-threshold-value</code>	(Optional) configure the recovering threshold and rising threshold for memory utilization alarms.
2	<code>Raisecom(config)#memory interval observation- interval-value</code>	(Optional) configure the interval for sampling memory alarms.

13.11.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show memory</code>	Show the memory utilization.
2	<code>Raisecom#show memory [module { value bufferpool diff }]</code>	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.

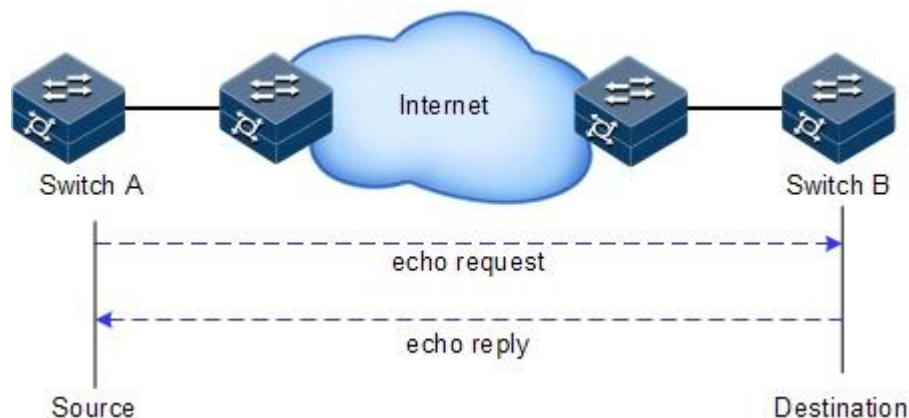
13.12 Ping

13.12.1 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 13-12 shows principles of Ping.

Figure 13-12 Principles of Ping



13.12.2 Configuring Ping

Configure Ping for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# ping <i>ip-address</i> [count <i>count</i>] [size <i>size</i>] [waittime <i>period</i>] [source <i>source-ip-address</i>]	(Optional) test the connectivity of the IPv4 network by the ping command.
2	Raisecom# ping ipv6 <i>ipv6-address</i> [count <i>count</i>] [size <i>size</i>] [waittime <i>period</i>]	(Optional) test the connectivity of the IPv6 network by the ping command.



Note

The Gazelle S1512i-PWR 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**.

13.13 Traceroute

13.13.1 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

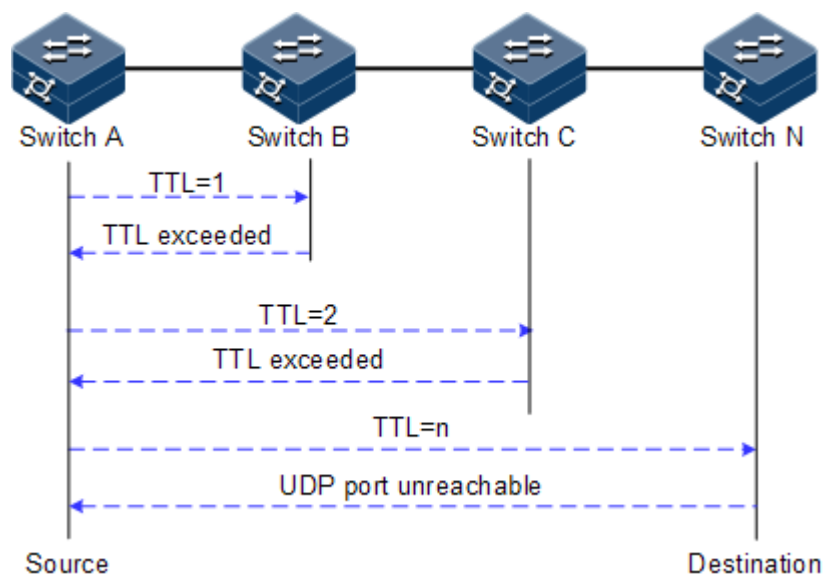
Traceroute works as below:

- Step 1 Send a piece of TTL1 sniffer packet (where the UDP port number 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 number of the destination host is not 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 13-13 shows principles of Traceroute.

Figure 13-13 Principles of Traceroute



13.13.2 Configuring Traceroute

Before using Traceroute, you should configure the IP address and default gateway of the Gazelle S1512i-PWR.

Configure Traceroute for the Gazelle S1512i-PWR as below.

Step	Command	Description
1	Raisecom# traceroute <i>ip-address</i> [firstttl <i>first-ttl</i>] [maxttl <i>max-ttl</i>] [port <i>port-number</i>] [waittime <i>period</i>] [count <i>times</i>] [size <i>size</i>]	(Optional) test the connectivity of the IPv4 network and view nodes passed by the packet by the traceroute command.
2	Raisecom# traceroute ipv6 <i>ipv6-address</i> [firstttl <i>first-ttl</i>] [maxttl <i>max-ttl</i>] [port <i>port-id</i>] [waittime <i>second</i>] [count <i>times</i>] [size <i>size</i>]	(Optional) test the connectivity of the IPv6 network and view nodes passed by the packet by the traceroute command.

14 Appendix

This chapter lists terms, acronyms, and abbreviations involved in this document, including the following sections:

- Terms
- Acronyms and abbreviations

14.1 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, 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, namely, 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 on 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 on 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 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.

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 on 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 rate, bit error rate, and signal-to-noise ratio.

R

Rapid Spanning Tree Protocol (RSTP) Evolution of the Spanning Tree Protocol (STP), which provides improvements in the rate of convergence for bridged networks

Remote Authentication Dial In User Service (RADIUS) RADIUS refers to a protocol used to authenticate and account users on 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 on 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.

14.2 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
C	
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
D	
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
E	

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
F	
FCS	Frame Check Sequence
FE	Fast Ethernet
FIFO	First Input First Output
FTP	File Transfer Protocol
G	
GARP	Generic Attribute Registration Protocol
GE	Gigabit Ethernet
GMRP	GARP Multicast Registration Protocol
GPS	Global Positioning System
GVRP	Generic VLAN Registration Protocol
H	
HDLC	High-level Data Link Control
HTTP	Hyper Text Transfer Protocol
I	
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
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
V	
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol
W	
WAN	Wide Area Network
WRR	Weight Round Robin

