



SNR-S212i-8POE
Configuration Guide (CLI)
(Rel_01)

NAG LLC provides customers with comprehensive technical support and services. For any assistance, please contact office

Website: <http://www.shop.nag.ru>

Tel: +7 343 3799838

Email: support@nag.com

Address: 57/2 Predelnaya st., Ekaterinburg, Russia

Postal code: 620016

Preface

Objectives

This guide describes features supported by the SNR-S212i-8POE, and related configurations, including basic principles and configuration procedure of Ethernet, reliability, OAM, security, and QoS, and related configuration examples.

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

By reading this guide, you can master principles and configurations of the SNR-S212i-8POE, and how to network with the SNR-S212i-8POE.

Versions




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


Product name	Product version	Software version	Hardware version
SNR-S212i-8POE	P100R001	V2.1.1 or later	A.00 or later

Conventions

Symbol conventions

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

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

Symbol	Description
 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	Names of files, directories, folders, and users are in boldface . For example, log in as user root .
<i>Italic</i>	Book titles are in <i>italics</i> .
Luci da Consol e	Terminal display is in Luci da Consol e.

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.

Change history

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

Issue 01 (2016-01-30)

Initial commercial release

Contents

1 Overview of features.....	1
2 Basic configurations.....	3
2.1 Accessing device	3
2.1.1 Introduction.....	3
2.1.2 Accessing through Console interface	4
2.1.3 Accessing through Telnet	5
2.1.4 Accessing through SSH.....	7
2.1.5 Checking configurations	8
2.2 CLI	9
2.2.1 Introduction.....	9
2.2.2 Levels.....	9
2.2.3 Modes	9
2.2.4 Shortcut keys	11
2.2.5 Acquiring help	13
2.2.6 Display information	15
2.2.7 Command history	16
2.2.8 Restoring default value of command line.....	16
2.2.9 Logging command lines.....	17
2.3 Managing users	17
2.3.1 Introduction.....	17
2.3.2 Preparing for configurations.....	18
2.3.3 Default configurations of user management.....	18
2.3.4 Creating user basic information.....	19
2.3.5 Managing user login	19
2.3.6 Managing user commands.....	19
2.3.7 Checking configurations	20
2.3.8 Example for configuring user management.....	20
2.4 Web network management	22
2.4.1 Introduction.....	22
2.4.2 Preparing for configuraitons.....	22
2.4.3 Default configurations of Web network management	22
2.4.4 Configuring Web network management.....	23

2.4.5 Checking configurations	23
2.5 Managing files.....	23
2.5.1 Managing BootROM files.....	23
2.5.2 Managing system files	24
2.5.3 Managing configuration files	25
2.5.4 Checking configurations	26
2.6 System upgrade	26
2.6.1 Upgrading system software through BootROM	27
2.6.2 Upgrading system software through CLI	28
2.6.3 Checking configurations	29
2.7 Configuring time management.....	29
2.7.1 Configuring time and time zone	29
2.7.2 Configuring DST	29
2.7.3 Configuring NTP	30
2.7.4 Configuring SNTP.....	31
2.7.5 Checking configurations	33
2.8 Configuring interface management	33
2.8.1 Introduction.....	33
2.8.2 Default configurations of interface management.....	34
2.8.3 Configuring basic attributes of interfaces.....	34
2.8.4 Configuring interface rate statistics	35
2.8.5 Configuring flow control on interfaces	36
2.8.6 Enabling/Disabling interfaces.....	36
2.8.7 Configuring L2Protocol Peer STP.....	37
2.8.8 Checking configurations	37
2.9 Configuring basic information	38
2.10 Task scheduling	38
2.11 Watchdog.....	39
2.11.1 Introduction	39
2.11.2 Preparing for configurations.....	40
2.11.3 Default configurations of watchdog.....	40
2.11.4 Configuring Watchdog	40
3 Ethernet.....	41
3.1 MAC address table	41
3.1.1 Introduction.....	41
3.1.2 Preparing for configurations.....	43
3.1.3 Default configurations of MAC address table	43
3.1.4 Configuring static MAC address	43
3.1.5 Configuring blackhole MAC address.....	44
3.1.6 Filtering unknown multicast packets	44
3.1.7 Configuring MAC address learning.....	44

3.1.8 Configuring MAC address limit	44
3.1.9 Configuring aging time of MAC addresses	45
3.1.10 Checking configurations	45
3.1.11 Maintenance	45
3.1.12 Example for configuring MAC address table	46
3.2 VLAN	47
3.2.1 Introduction	47
3.2.2 Preparing for configurations	48
3.2.3 Default configurations of VLAN	49
3.2.4 Configuring VLAN attributes	49
3.2.5 Configuring interface mode	50
3.2.6 Configuring VLAN on Access interface	50
3.2.7 Configuring VLAN on Trunk interface	51
3.2.8 Checking configurations	52
3.3 QinQ	52
3.3.1 Introduction	52
3.3.2 Preparing for configurations	53
3.3.3 Default configurations of QinQ	54
3.3.4 Configuring basic QinQ	54
3.3.5 Configuring selective QinQ	54
3.3.6 Configuring egress interface toTrunk mode	55
3.3.7 Checking configurations	55
3.3.8 Example for configuring basic QinQ	55
3.3.9 Example for configuring selective QinQ	58
3.4 VLAN mapping	60
3.4.1 Introduction	60
3.4.2 Preparing for configurations	61
3.4.3 Default configurations of VLAN mapping	61
3.4.4 Configuring 1:1 VLAN mapping	62
3.4.5 Checking configurations	62
3.5 STP/RTSTP	62
3.5.1 Introduction	62
3.5.2 Preparing for configurations	65
3.5.3 Default configurations of STP	65
3.5.4 Enabling STP	66
3.5.5 Configuring STP parameters	66
3.5.6 Checking configurations	67
3.5.7 Example for configuring STP	67
3.6 MSTP	70
3.6.1 Introduction	70
3.6.2 Preparing for configurations	73
3.6.3 Default configurations of MSTP	73

3.6.4 Enabling MSTP	74
3.6.5 Configuring MST domain and its maximum number of hops	74
3.6.6 Configuring root bridge/backup bridge	75
3.6.7 Configuring interface priority and system priority	76
3.6.8 Configuring network diameter for switching network	77
3.6.9 Configuring inner path cost for interface	77
3.6.10 Configuring external path cost on interface	78
3.6.11 Configuring maximum transmission rate on interface	78
3.6.12 Configuring MSTP timer	78
3.6.13 Configuring edge interface	79
3.6.14 Configuring BPDU filtering	79
3.6.15 Configuring BPDU Guard	80
3.6.16 Configuring STP/RSTP/MSTP mode switching	80
3.6.17 Configuring link type	81
3.6.18 Configuring root interface protection	81
3.6.19 Configuring interface loopguard	82
3.6.20 Checking configurations	82
3.6.21 Maintenance	82
3.6.22 Example for configuring MSTP	83
3.7 GARP	88
3.7.1 Introduction	88
3.7.2 Preparing for configurations	90
3.7.3 Default configurations of GARP	90
3.7.4 Configuring basic functions of GARP	91
3.7.5 Configuring GVRP	91
3.7.6 Configuring GMRP	92
3.7.7 Checking configurations	92
3.7.8 Maintenance	93
3.7.9 Example for configuring GVRP	93
3.7.10 Example for configuring GMRP	97
3.8 Loopback detection	100
3.8.1 Introduction	100
3.8.2 Preparing for configurations	102
3.8.3 Default configurations of loopback detection	102
3.8.4 Configuring loopback detection	102
3.8.5 Configuring uplink interface for loopback detection	103
3.8.6 Checking configurations	103
3.8.7 Maintenance	104
3.8.8 Example for configuring internal loopback detection	104
3.8.9 Example for configuring external loop for loopback detection	106
3.9 Line detection	108
3.9.1 Introduction	108

3.9.2	Preparing for configurations.....	108
3.9.3	Configuring line detection.....	108
3.9.4	Checking configurations	109
3.9.5	Example for configuring line detection.....	109
3.10	Interface protection	110
3.10.1	Introduction	110
3.10.2	Preparing for configurations.....	110
3.10.3	Default configurations of interface protection	110
3.10.4	Configuring interface protection.....	111
3.10.5	Checking configurations	111
3.10.6	Example for configuring interface protection.....	111
3.11	Port mirroring.....	113
3.11.1	Introduction	113
3.11.2	Preparing for configurations.....	114
3.11.3	Default configurations of port mirroring	114
3.11.4	Configuring port mirroring on local port.....	114
3.11.5	Checking configurations.....	115
3.11.6	Example for configuring port mirroring	115
3.12	Layer 2 protocol transparent transmission.....	116
3.12.1	Introduction	116
3.12.2	Preparing for configurations.....	117
3.12.3	Default configurations of Layer 2 protocol transparent transmission	117
3.12.4	Configuring transparent transmission parameters.....	117
3.12.5	Checking configurations	118
3.12.6	Maintenance	118
3.12.7	Example for configuring Layer 2 protocol transparent transmission	118
4	PoE.....	122
4.1	Introduction.....	122
4.1.1	PoE principle.....	122
4.1.2	PoE modules.....	122
4.1.3	PoE advantages.....	122
4.1.4	PoE concepts	123
4.2	Configuring PoE.....	123
4.2.1	Preparing for configurations.....	123
4.2.2	Default configurations of PoE	124
4.2.3	Enabling interface PoE.....	124
4.2.4	Configuring power supply modes.....	124
4.2.5	Configuring maximum output power of PoE	124
4.2.6	Configuring priority of PoE	125
4.2.7	Configuring identifying non-standard PDs.....	125
4.2.8	Configuring PSE power utilization ratio threshold	125

4.2.9 Enabling non-standard PD identification	126
4.2.10 Enabling forcible power supply on interface	126
4.2.11 Enabling overtemperature protection	126
4.2.12 Enabling global Trap.....	127
4.2.13 Checking configurations	127
4.3 Example for configuring PoE power supply	127
5 Ring network protection	130
5.1 G.8032	130
5.1.1 Introduction.....	130
5.1.2 Preparing for configurations.....	130
5.1.3 Default configurations of G.8032	131
5.1.4 Creating G.8032 ring	131
5.1.5 (Optional) creating G.8032 sub-ring.....	133
5.1.6 (Optional) configuring G.8032 switching control.....	135
5.1.7 Enabling association between ERPS and RSTP	135
5.1.8 Checking configurations	136
5.1.9 Maintenance	136
5.1.10 Example for configuring single ring G.8032	136
5.1.11 Example for configuring intersecting G.8032.....	139
5.2 RRPS	143
5.2.1 Introduction.....	143
5.2.2 Preparing for configurations.....	147
5.2.3 Default configurations of RRPS	147
5.2.4 Creating RRPS	147
5.2.5 Configuring basic functions of RRPS	148
5.2.6 Checking configurations	149
5.2.7 Maintenance	149
5.2.8 Example for configuring RRPS	149
6 IP services.....	152
6.1 Layer 3 interface.....	152
6.1.1 Introduction.....	152
6.1.2 Preparing for configurations.....	152
6.1.3 Default configurations of Layer 3 interface.....	153
6.1.4 Configuring Layer 3 interface	153
6.1.5 Configuring mapping between Layer 3 interface and VLAN.....	153
6.1.6 Configuring mapping between Layer 3 interface and physical interface	154
6.1.7 Configuring management VLAN attributes	154
6.1.8 Checking configurations	155
6.1.9 Example for configuring Layer 3 interface to interconnect with host	155
6.2 Loopback interface	157
6.2.1 Introduction.....	157

6.2.2	Preparing for configurations.....	157
6.2.3	Default configurations of loopback interface	157
6.2.4	Configuring IP address of loopback interface.....	157
6.2.5	Checking configurations	158
6.3	ARP	158
6.3.1	Introduction.....	158
6.3.2	Preparing for configurations.....	159
6.3.3	Default configurations of ARP	159
6.3.4	Configuring static ARP entries	159
6.3.5	Configuring dynamic ARP entries	159
6.3.6	Checking configurations	160
6.3.7	Maintenance	160
6.3.8	Configuring ARP	160
6.4	DHCP Client	162
6.4.1	Introduction.....	162
6.4.2	Preparing for configurations.....	164
6.4.3	Default configurations of DHCP Client	165
6.4.4	Configuring DHCP Client.....	165
6.4.5	Checking configurations	166
6.4.6	Example for configuring DHCP Client	166
6.5	DHCP Server.....	167
6.5.1	Introduction.....	167
6.5.2	Preparing for configurations.....	168
6.5.3	Default configurations of DHCP Server	168
6.5.4	Configuring DHCP Server	169
6.5.5	Configuring address pool	169
6.5.6	Configuring DHCP Server on IP interface	170
6.5.7	(Optional) configuring trusted DHCP relay device.....	171
6.5.8	Checking configurations	171
6.5.9	Example for configuring DHCP Server	171
6.6	DHCP Relay.....	173
6.6.1	Introduction.....	173
6.6.2	Preparing for configurations.....	174
6.6.3	Default configurations of DHCP Relay.....	174
6.6.4	Configuring global DHCP Relay	175
6.6.5	Configuring DHCP Relay on interface.....	175
6.6.6	Configuring destination IP address for forwarding packets.....	175
6.6.7	(Optional) configuring DHCP Relay to support Option 82	175
6.6.8	Checking configurations	176
6.7	DHCP Snooping	176
6.7.1	Introduction.....	176
6.7.2	Preparing for configurations.....	177

6.7.3 Default configurations of DHCP Snooping.....	178
6.7.4 Configuring DHCP Snooping.....	178
6.7.5 Checking configurations	179
6.7.6 Example for configuring DHCP Snooping.....	179
6.8 DHCP Options.....	181
6.8.1 Introduction.....	181
6.8.2 Preparing for configurations.....	182
6.8.3 Default configurations of DHCP Option	182
6.8.4 Configuring DHCP Option fields	182
6.8.5 Checking configurations	183
7 IP routing.....	184
7.1 Routing management.....	184
7.1.1 Introduction.....	184
7.1.2 Preparing for configurations.....	184
7.1.3 Default configurations	184
7.1.4 Configuring routing management.....	184
7.1.5 Showing routing table	185
7.2 Static routing.....	185
7.2.1 Introduction.....	185
7.2.2 Preparing for configurations.....	186
7.2.3 Default configurations of static routing.....	186
7.2.4 Configuring static routing	186
7.2.5 Checking configurations	186
7.2.6 Examples for configuring static routing.....	187
8 QoS.....	189
8.1 Introduction.....	189
8.1.1 ACL	189
8.1.2 Service model.....	190
8.1.3 Priority trust	190
8.1.4 Traffic classification	191
8.1.5 Traffic policy	192
8.1.6 Priority mapping.....	193
8.1.7 Congestion management	193
8.1.8 Rate limiting based on interface and VLAN	195
8.2 ACL.....	195
8.2.1 Preparing for configurations.....	195
8.2.2 Default configurations of ACL.....	196
8.2.3 Configuring IP ACL.....	196
8.2.4 Configuring MAC ACL	197
8.2.5 Configuring MAP ACL.....	197
8.2.6 Applying ACL	199

8.2.7	Checking configurations	201
8.2.8	Maintenance	201
8.3	Configuring basic QoS.....	202
8.3.1	Preparing for configurations.....	202
8.3.2	Default configurations of basic QoS	202
8.3.3	Enabling global QoS	203
8.3.4	Configuring priority type of interface trust	203
8.3.5	Configuring mapping from CoS to local priority.....	203
8.3.6	Configuring mapping from DSCP to local priority.....	204
8.3.7	Checking configurations	204
8.4	Configuring congestion management	205
8.4.1	Preparing for configurations.....	205
8.4.2	Default configurations of congestion management.....	205
8.4.3	Configuring SP queue scheduling.....	205
8.4.4	Configuring WRR or SP+WRR queue scheduling	205
8.4.5	Configuring DRR or SP+DRR queue scheduling.....	206
8.4.6	Configuring queue bandwidth guarantee.....	206
8.4.7	Checking configurations	206
8.5	Configuring traffic classification and traffic policy	207
8.5.1	Preparing for configurations.....	207
8.5.2	Default configurations of traffic classification and traffic policy	207
8.5.3	Creating traffic classification.....	207
8.5.4	Configuring traffic classification rules.....	208
8.5.5	Creating rate limit rule and shapping rule	208
8.5.6	Creating traffic policy	209
8.5.7	Defining traffic policy mapping	209
8.5.8	Defining traffic policy operation	210
8.5.9	Applying traffic policy to interfaces	211
8.5.10	Checking configurations	211
8.5.11	Maintenance	212
8.6	Configuring rate limiting based on interface and VLAN	212
8.6.1	Preparing for configurations.....	212
8.6.2	Default configurations of rate limiting based on interface and VLAN.....	212
8.6.3	Configuring rate limiting based on interface	212
8.6.4	Configuring rate limiting based on VLAN.....	213
8.6.5	Configuring rate limiting based on QinQ.....	213
8.6.6	Checking configurations	213
8.6.7	Maintenance	214
8.7	Configuring examples.....	214
8.7.1	Example for configuring ACL.....	214
8.7.2	Example for configuring congestion management.....	215
8.7.3	Example for configuring rate limiting based on traffic policy.....	217

8.7.4 Example for configuring rate limiting based on interface	220
9 Multicast	223
9.1 Overview	223
9.1.1 Multicast overview	223
9.1.2 Basic functions of Layer 2 multicast	228
9.1.3 IGMP Snooping	229
9.2 Configuring IGMP basis	230
9.2.1 Preparing for configurations	230
9.2.2 Default configurations of Layer 2 multicast basic functions	230
9.2.3 Configuring basic functions of Layer 2 multicast	230
9.2.4 Checking configurations	231
9.3 Configuring IGMP Snooping	231
9.3.1 Preparing for configurations	231
9.3.2 Default configurations of IGMP Snooping	232
9.3.3 Configuring IGMP Snooping	232
9.3.4 Checking configurations	233
9.4 Configuration examples	233
9.4.1 Example for configuring IGMP Snooping	233
9.4.2 Example for configuring ring network multicast	235
10 Security	239
10.1 Secure MAC address	239
10.1.1 Introduction	239
10.1.2 Preparing for configurations	240
10.1.3 Default configurations of secure MAC address	241
10.1.4 Configuring basic functions of secure MAC address	241
10.1.5 Configuring static secure MAC address	242
10.1.6 Configuring dynamic secure MAC address	242
10.1.7 Configuring Sticky secure MAC address	243
10.1.8 Checking configurations	244
10.1.9 Maintenance	244
10.1.10 Example for configuring secure MAC address	244
10.2 Dynamic ARP inspection	246
10.2.1 Introduction	246
10.2.2 Preparing for configurations	248
10.2.3 Default configurations of dynamic ARP inspection	248
10.2.4 Configuring trusted interfaces of dynamic ARP inspection	248
10.2.5 Configuring static binding of dynamic ARP inspection	249
10.2.6 Configuring dynamic binding of dynamic ARP inspection	249
10.2.7 Configuring protection VLAN of dynamic ARP inspection	249
10.2.8 Configuring rate limiting on ARP packets on interface	249
10.2.9 Configuring auto-recovery time for rate limiting on ARP packets	250

10.2.10	Checking configurations.....	250
10.2.11	Example for configuring dynamic ARP inspection	250
10.3	RADIUS.....	253
10.3.1	Introduction	253
10.3.2	Preparing for configurations.....	253
10.3.3	Default configurations of RADIUS	254
10.3.4	Configuring RADIUS authentication.....	254
10.3.5	Configuring RADIUS accounting.....	255
10.3.6	Checking configurations	256
10.3.7	Example for configuring RADIUS	256
10.4	TACACS+.....	257
10.4.1	Introduction	257
10.4.2	Preparing for configurations.....	258
10.4.3	Default configurations of TACACS+.....	258
10.4.4	Configuring TACACS+ authentication	258
10.4.5	Configuring TACACS+ accounting.....	259
10.4.6	Checking configurations	259
10.4.7	Maintenance	259
10.4.8	Example for configuring TACACS+.....	260
10.5	Storm control.....	261
10.5.2	Preparing for configurations.....	262
10.5.3	Default configurations of storm control	262
10.5.4	Configuring storm control	262
10.5.5	Configuring DLF packet forwarding.....	262
10.5.6	Checking configurations	263
10.5.7	Example for configuring storm control	263
10.6	802.1x	264
10.6.1	Introduction	264
10.6.2	Preparing for configurations.....	267
10.6.3	Default configurations of 802.1x	267
10.6.4	Configuring basic functions of 802.1x	267
10.6.5	Configuring 802.1x re-authentication	268
10.6.6	Configuring 802.1x timers	268
10.6.7	Checking configurations	269
10.6.8	Maintenance	269
10.6.9	Example for configuring 802.1x	270
10.7	IP Source Guard.....	271
10.7.1	Introduction	271
10.7.2	Preparing for configurations.....	273
10.7.3	Default configurations of IP Source Guard	273
10.7.4	Configuring interface trust status of IP Source Guard.....	273
10.7.5	Configuring IP Source Guide binding	274

10.7.6	Checking configurations	275
10.7.7	Example for configuring IP Source Guard	275
10.8	PPPoE+	277
10.8.1	Introduction	277
10.8.2	Preparing for configurations	278
10.8.3	Default configurations of PPPoE+	278
10.8.4	Configuring basic functions of PPPoE+	279
10.8.5	Configuring PPPoE+ packet information	280
10.8.6	Checking configurations	282
10.8.7	Maintenance	282
10.8.8	Example for configuring PPPoE+	282
11	Reliability	285
11.1	Link aggregation	285
11.1.1	Introduction	285
11.1.2	Preparing for configurations	287
11.1.3	Default configurations of link aggregation	288
11.1.4	Configuring manual link aggregation	288
11.1.5	Configuring static LACP link aggregation	289
11.1.6	Configuring dynamic LACP link aggregation	290
11.1.7	Checking configurations	291
11.1.8	Maintenance	292
11.1.9	Example for configuring manual link aggregation	292
11.1.10	Example for configuring static LACP link aggregation	294
11.1.11	Example for configuring dynamic LACP link aggregation	296
11.2	Interface backup	298
11.2.1	Introduction	298
11.2.2	Preparing for configurations	299
11.2.3	Default configurations of interface backup	300
11.2.4	Configuring basic functions of interface backup	300
11.2.5	(Optional) configuring FS on interfaces	301
11.2.6	Checking configurations	301
11.2.7	Example for configuring interface backup	302
11.3	Failover	304
11.3.1	Introduction	304
11.3.2	Preparing for configurations	304
11.3.3	Default configurations of failover	304
11.3.4	Configuring failover	304
11.3.5	Checking configurations	305
11.3.6	Example for configuring failover	306
12	System management	309
12.1	SNMP	309

12.1.1 Introduction	309
12.1.2 Preparing for configurations	311
12.1.3 Default configurations of SNMP	311
12.1.4 Configuring basic functions of SNMP v1/v2c	312
12.1.5 Configuring basic functions of SNMP v3.....	313
12.1.6 Configuring IP authentication by SNMP server.....	314
12.1.7 Configuring other information of SNMP	314
12.1.8 Configuring Trap	315
12.1.9 Checking configurations	316
12.1.10 Example for configuring SNMP v1/v2c and Trap.....	316
12.1.11 Example for configuring SNMP v3 and Trap	318
12.2 KeepAlive	320
12.2.1 Introduction	320
12.2.2 Preparing for configurations	321
12.2.3 Default configurations of KeepAlive	321
12.2.4 Configuring KeepAlive.....	321
12.2.5 Checking configurations	321
12.2.6 Example for configuring KeepAlive	322
12.3 RMON	323
12.3.1 Introduction	323
12.3.2 Preparing for configurations	324
12.3.3 Default configurations of RMON	324
12.3.4 Configuring RMON statistics.....	325
12.3.5 Configuring RMON historical statistics	325
12.3.6 Configuring RMON alarm group.....	325
12.3.7 Configuring RMON event group	326
12.3.8 Checking configurations	326
12.3.9 Maintenance	327
12.3.10 Example for configuring RMON alarm group.....	327
12.4 Cluster management	328
12.4.1 Introduction	328
12.4.2 Preparing for configurations	331
12.4.3 Default configurations of cluster management	331
12.4.4 Configuring RNDP	331
12.4.5 Configuring RTDP.....	332
12.4.6 Configuring cluster management on commander devices	332
12.4.7 (Optional) configuring auto-activation for candidate device	334
12.4.8 Checking configurations	334
12.4.9 Example for providing remote access through cluster management	335
12.5 LLDP	338
12.5.1 Introduction	338
12.5.2 Preparing for configurations.....	340

12.5.3 Default configurations of LLDP	340
12.5.4 Enabling global LLDP	340
12.5.5 Enabling interface LLDP	341
12.5.6 Configuring basic functions of LLDP	341
12.5.7 Configuring LLDP alarm	342
12.5.8 Configuring destination MAC address of LLDP packets	342
12.5.9 Checking configurations	342
12.5.10 Maintenance	343
12.5.11 Example for configuring basic functions of LLDP	343
12.6 Optical module DDM	346
12.6.1 Introduction	346
12.6.2 Preparing for configurations	346
12.6.3 Default configurations of optical module DDM	346
12.6.4 Enabling optical module DDM	347
12.6.5 Enabling optical module DDM Trap	347
12.6.6 Enabling optical DDM module password check	348
12.6.7 Checking configurations	348
12.7 System log	348
12.7.1 Introduction	348
12.7.2 Preparing for configurations	349
12.7.3 Default configurations of system log	349
12.7.4 Configuring basic information of system log	350
12.7.5 Configuring system log output	351
12.7.6 Checking configurations	352
12.7.7 Maintenance	353
12.7.8 Example for outputting system logs to log host	353
12.8 Alarm management	354
12.8.1 Introduction	354
12.8.2 Preparing for configurations	358
12.8.3 Default configurations of alarm management	359
12.8.4 Configuring basic functions of alarm management	359
12.8.5 Checking configurations	360
12.9 Hardware environment monitoring	360
12.9.1 Introduction	360
12.9.2 Preparing for configurations	363
12.9.3 Default configurations of hardware environment monitoring	363
12.9.4 Enabling global hardware environment monitoring	364
12.9.5 Configuring power supply monitoring alarm	364
12.9.6 Configuring temperature monitoring alarm	364
12.9.7 Configuring interface status monitoring alarm	365
12.9.8 Clearing all hardware environment monitoring alarms manually	365
12.9.9 Checking configurations	366

12.10 CPU monitoring.....	366
12.10.1 Introduction	366
12.10.2 Preparing for configurations	367
12.10.3 Default configurations of CPU monitoring	367
12.10.4 Showing CPU monitoring information	367
12.10.5 Configuring CPU monitoring alarm.....	367
12.10.6 Checking configurations.....	368
12.11 CPU protection	368
12.11.1 Introduction	368
12.11.2 Preparing for configurations	368
12.11.3 Default configurations of CPU protection	369
12.11.4 Configuring CPU protection on interfaces	369
12.11.5 Checking configurations.....	370
12.11.6 Example for configuring CPU protection	370
12.12 Ping.....	371
12.12.1 Introduction	371
12.12.2 Configuring Ping	372
12.13 Traceroute.....	372
12.13.1 Introduction	372
12.13.2 Configuring Traceroute	373
13 Appendix	374
13.1 Terms	374
13.2 Acronyms and abbreviations	378

Figures

Figure 2-1 Accessing device through PC connected with RJ45 Console interface.....	4
Figure 2-2 Configuring communication parameters in Hyper Terminal	5
Figure 2-3 Networking with device as Telnet server	5
Figure 2-4 Networking with device as Telnet client	6
Figure 2-5 User management networking.....	20
Figure 3-1 MAC networking.....	46
Figure 3-2 Partitioning VLANs.....	47
Figure 3-3 Principle of basic QinQ	52
Figure 3-4 Basic QinQ networking	56
Figure 3-5 Selective QinQ networking	58
Figure 3-6 Principle of VLAN mapping	61
Figure 3-7 Network storm due to loopback	63
Figure 3-8 Loop networking with STP	64
Figure 3-9 VLAN packet forward failure due to RSTP	65
Figure 3-10 STP networking.....	67
Figure 3-11 Basic concepts of MSTI network.....	71
Figure 3-12 MSTI concepts	72
Figure 3-13 Networking of multiple spanning trees instances in MST domain	73
Figure 3-14 MSTP networking.....	83
Figure 3-15 GVRP working principle.....	89
Figure 3-16 GVRP networking	94
Figure 3-17 GMRP networking.....	97
Figure 3-18 Loopback detection networking	100
Figure 3-19 Loopback detection networking	104
Figure 3-20 Networking with external loopback for loopback detection.....	106
Figure 3-21 Line detection networking	109

Figure 3-22 Interface protection networking.....	112
Figure 3-23 Port mirroring principle	113
Figure 3-24 Port mirroring networking	115
Figure 3-25 Layer 2 protocol transparent transmission networking	119
Figure 4-1 PoE switch power supply networking.....	128
Figure 5-1 Single ring G.8032 networking	137
Figure 5-2 Intersecting ring G.8032 networking.....	140
Figure 5-3 RRPS normal status.....	144
Figure 5-4 RRPS switching status.....	145
Figure 5-5 RRPS link restoration	146
Figure 5-6 RRPS networking.....	150
Figure 6-1 Layer 3 interface configuration networking.....	155
Figure 6-2 Configuring ARP networking.....	161
Figure 6-3 DHCP typical networking	162
Figure 6-4 Structure of DHCP packet.....	163
Figure 6-5 DHCP Client networking	164
Figure 6-6 DHCP client networking.....	166
Figure 6-7 DHCP Server networking	168
Figure 6-8 DHCP Server networking	172
Figure 6-9 Principle of DHCP Relay.....	174
Figure 6-10 DHCP Snooping networking.....	177
Figure 6-11 DHCP Snooping networking	179
Figure 7-1 Configuring static routing	187
Figure 8-1 Traffic classification	191
Figure 8-2 Structure of IP packet head	191
Figure 8-3 Structure of packets with IP priority and DSCP priority	191
Figure 8-4 Structure of VLAN packets.....	192
Figure 8-5 Structure of packets with CoS priority.....	192
Figure 8-6 SP scheduling.....	194
Figure 8-7 WRR scheduling	194
Figure 8-8 DRR scheduling	195
Figure 8-9 ACL networking.....	214
Figure 8-10 Queue scheduling networking.....	216

Figure 8-11 Rate limiting based on traffic policy	218
Figure 8-12 Rate limiting based on interface	221
Figure 9-1 Multicast transmission networking.....	224
Figure 9-2 Basic concepts in multicast	226
Figure 9-3 Mapping between IPv4 multicast address and multicast MAC address.....	227
Figure 9-4 Operating of IGMP and Layer 2 multicast features	227
Figure 9-5 IGMP Snooping networking	232
Figure 9-6 IGMP Snooping networking	234
Figure 9-7 Ring network multicast networking.....	236
Figure 10-1 Configuring secure MAC address	245
Figure 10-2 Principle of dynamic ARP inspection	247
Figure 10-3 Configuring dynamic ARP inspection	251
Figure 10-4 Configuring RADIUS	256
Figure 10-5 Configuring TACACS+	260
Figure 10-6 Storm control networking	263
Figure 10-7 802.1x structure.....	265
Figure 10-8 Configuring 802.1x.....	270
Figure 10-9 Principle of IP Source Guard.....	272
Figure 10-10 Configuring IP Source Guard.....	276
Figure 10-11 Accessing the network through PPPoE authentication.....	278
Figure 10-12 Configuring PPPoE+	283
Figure 11-1 Link aggregation.....	285
Figure 11-2 Configuring manual link aggregation	292
Figure 11-3 Configuring static LACP link aggregation	294
Figure 11-4 Configuring dynamic LACP link aggregation.....	297
Figure 11-5 Principles of interface backup	298
Figure 11-6 Networking with interface backup in different VLANs	299
Figure 11-7 Configuring interface backup.....	302
Figure 11-8 Configuring failover	306
Figure 12-1 Principle of SNMP	310
Figure 12-2 SNMP v3 authentication mechanism.....	313
Figure 12-3 Configuring SNMP v1/v2c and Trap	316
Figure 12-4 Configuring SNMP v3 and Trap.....	318

Figure 12-5 Configuring KeepAlive.....	322
Figure 12-6 RMON	324
Figure 12-7 Configuring RMON alarm group	327
Figure 12-8 Cluster management	330
Figure 12-9 Providing remote access through cluster management	335
Figure 12-10 LLDPDU structure	338
Figure 12-11 Basic TLV structure	339
Figure 12-12 Configuring basic functions of LLDP.....	343
Figure 12-13 Outputting system logs to log hosts	353
Figure 12-14 Configuring CPU protection	370
Figure 12-15 Principle of Ping.....	371
Figure 12-16 Principles of Traceroute	373

Tables

Table 1-1 Features, standards, and specifications.....	1
Table 2-1 Shortcut keys for display features.....	15
Table 3-1 Interface mode and packet processing.....	48
Table 6-1 Fields of DHCP packet.....	163
Table 6-2 Common DHCP options.....	181
Table 8-1 Default mapping of local priority, DSCP, and CoS.....	193
Table 8-2 Mapping between local priority and queue.....	193
Table 8-3 Default mapping from CoS to local priority.....	203
Table 8-4 Default mapping from DSCP to local priority.....	203
Table 12-1 TLV types.....	339
Table 12-2 Log levels.....	349
Table 12-3 Alarm fields.....	355
Table 12-4 Alarm levels.....	356
Table 12-5 Trap information.....	362
Table 12-6 Syslog information.....	362

1 Overview of features

The network-manageable guide-rail Layer 2 industrial Ethernet switch SNR-S212i-8POE (hereinafter referred to as the SNR-S212i-8POE) supports features, standards, and specifications, as listed in Table 1-1.

Table 1-1 Features, standards, and specifications

Feature	Description
Basic configurations	<ul style="list-style-type: none"> • Accessing the device (RJ45 Console/Telnet/SSH) • CLI • Web network management • Managing files (BootROM/system files/configuration files) • Load and upgrade (TFTP auto-loading, BootROM upgrade, FTP/SFTP/TFTP upgrade) • Time management • Interface management • Basic information about the device (device name, language mode, saving/deleting configurations, and reboot) • Task scheduling
Ethernet	<ul style="list-style-type: none"> • MAC address (16×1024) • VLAN (4094 VLANs) • PVLAN • Basic QinQ • Selective QinQ (1000) • VLAN mapping (680 in ingress) • STP/RSTP/MSTP • GARP (GVRP and GMRP) • Loopback detection • Line detection • Interface protection • Port mirroring • Layer 2 protocol transparent transmission (Dot1x packets, BPDU packets, LACP packets, CDP packets, PVST packets, and VTP packets)
PoE	<ul style="list-style-type: none"> • IEEE 802.3af standard (PoE) • IEEE 802.3at standard (PoE+)
Ring protection switching	<ul style="list-style-type: none"> • ERPS (ITU-T G.8032) • RRPS

Feature	Description
IP services	<ul style="list-style-type: none"> • ARP • Layer 3 interface • DHCP Client/DHCP Server/DHCP Relay/DHCP Snooping/DHCP Option
IP route	<ul style="list-style-type: none"> • Route management • Static routing
QoS	<ul style="list-style-type: none"> • ACL (1000) • Priority trust • Traffic classification (IP priority, DSCP priority, CoS priority), and traffic policy (rate limiting, redirection, re-marking based on traffic policy) • Local priority mapping and queue scheduling (SP, DRR, and SP+DRR) • Interface-based and VLAN-based rate limiting
Multicast	<ul style="list-style-type: none"> • Multicast forwarding entries (1024 entries) • IGMP Snooping (v1 and v2)
Security	<ul style="list-style-type: none"> • Port security MAC • Dynamic ARP detection • RADIUS authentication • 802.1x • TACACS+ • Storm control • IP Source Guard • PPPoE+
Reliability	<ul style="list-style-type: none"> • Link aggregation (14 LAGs) • Interface backup • Failover
System management	<ul style="list-style-type: none"> • SNMP • KeepAlive • RMON • Cluster management • LLDP • Optical module DDM • System log • Alarm management • Hardware environment monitoring • CPU monitoring • CPU protection • Ping and Traceroute



Note

Interface backup, STP, loopback detection, G.8032, and RRPS may interfere with each other. We recommend not configuring two or more of them concurrently.

2 Basic configurations

This chapter describes the basic configuration and configuration process about the SNR-S212i-8POE, and provides related configuration examples, including the following sections:

- Accessing device
- CLI
- Managing users
- Web network management
- Managing files
- System upgrade
- Configuring time management
- Configuring interface management
- Configuring basic information
- Task scheduling
- Watchdog



Note

The configuration steps in this manual are in command line mode.

2.1 Accessing device

2.1.1 Introduction

The SNR-S212i-8POE can be configured and managed in the Command Line Interface (CLI) mode or NView NNM network management mode.

The SNR-S212i-8POE CLI mode has a variety of configuration modes:

- Console mode: you must use Console mode in the first configuration. It supports the RJ45 Console interface.
- Telnet mode: log in to the SNR-S212i-8POE in Console mode, enable the Telnet service on the switch, configure the IP address of Layer 3 interface, set the user name and password, and then conduct remote Telnet configuration.

- Security Shell (SSH) mode: before accessing the SNR-S212i-8POE through SSH, you need to log in to the SNR-S212i-8POE and start the SSH service through the Console interface.

When configuring the SNR-S212i-8POE in network management mode, you must first configure the IP address of Layer 3 interface through CLI, and then configure the SNR-S212i-8POE through NView NNM system or in Web mode.

2.1.2 Accessing through Console interface

Introduction

The Console interface is an interface which is commonly used for network device to connect the terminal emulation program with a PC. You can use this interface to configure and manage local device. This management method can communicate directly without a network, so it is called out-of-band management. You can also perform configuration and management on the SNR-S212i-8POE through the Console interface when the network fails.

In the below two conditions, you can only log in to the SNR-S212i-8POE and configure it through the Console interface:

- The SNR-S212i-8POE is powered on to start for the first time.
- You cannot access the SNR-S212i-8POE through Telnet.

The SNR-S212i-8POE supports the RJ45 Console interface, which is marked "Console".

Accessing device through RJ45 Console interface

If you wish to access the SNR-S212i-8POE on a PC through RJ45 Console interface, connect the Console interface on the SNR-S212i-8POE to the RS-232 serial interface on the PC, as shown in Figure 2-1. Run the terminal emulation program such as Windows XP Hyper Terminal on the PC to configure communication parameters as shown in Figure 2-2, and then log in to the SNR-S212i-8POE.

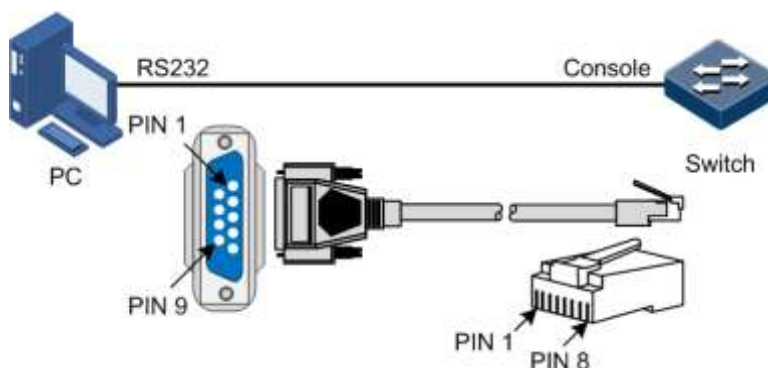


Figure 2-1 Accessing device through PC connected with RJ45 Console interface

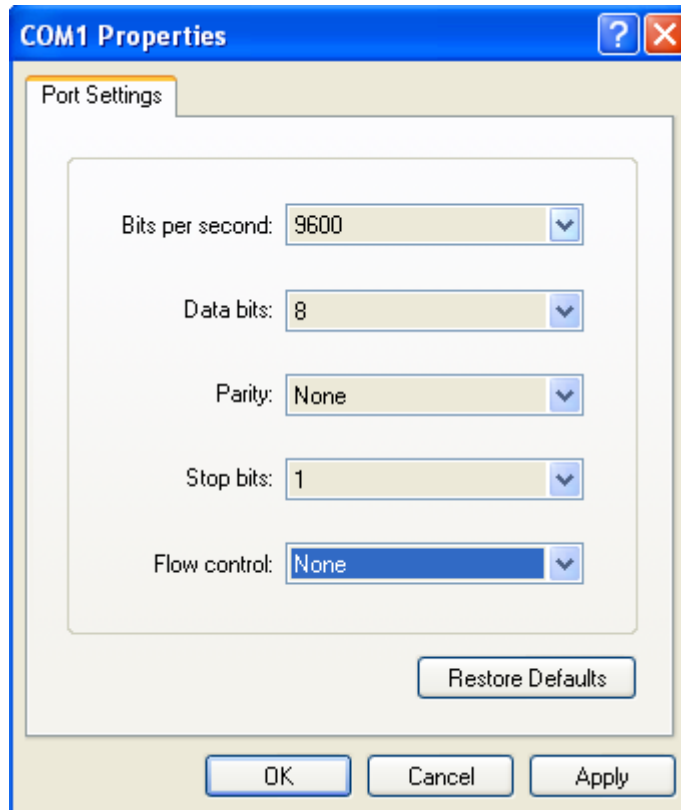


Figure 2-2 Configuring communication parameters in Hyper Terminal

2.1.3 Accessing through Telnet

Use a PC to log in to the SNR-S212i-8POE remotely through Telnet, log in to an SNR-S212i-8POE from the PC at first, and then Telnet other SNR-S212i-8POE devices on the network. You do not need to connect a PC to each SNR-S212i-8POE.

Telnet services provided by the SNR-S212i-8POE are as below.

- Telnet Server: run the Telnet client program on a PC to log in to the SNR-S212i-8POE, and conduct configuration and management. As shown in Figure 2-3, the SNR-S212i-8POE is providing Telnet Server service at this time.

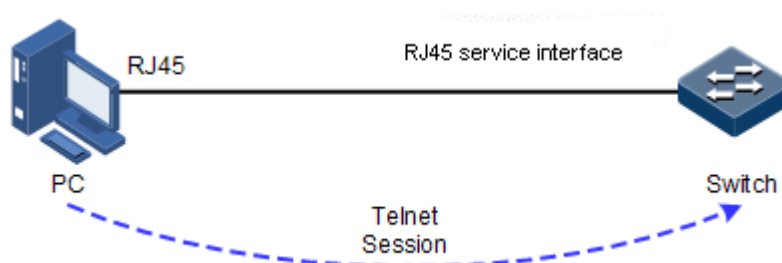


Figure 2-3 Networking with device as Telnet server

Before accessing the SNR-S212i-8POE through Telnet, you need to log in to the SNR-S212i-8POE through the Console interface and start the Telnet service. Configure the SNR-S212i-8POE that needs to start Telnet service.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# I nterface <i>ip i f-number</i>	Enter Layer 3 interface configuration mode
3	NAG(confi g-i p)# I p address <i>ip-address [ip-mask]</i> [sub] [<i>vlan-id</i>] NAG(confi g-i p)# qui t	Configure the IP address of the SNR-S212i-8POE, and bind the VLAN of specified ID. The interface on which the Telnet service is started belongs to this VLAN.
4	NAG(confi g)# tel net-server enable	Start the Telnet server.
5	NAG(confi g)# tel net-server accept port-l i st <i>port-list</i>	(Optional) configure the interface to support the Telnet function.
6	NAG(confi g)# tel net-server cl ose termi nal -tel net <i>sessi on-number</i>	(Optional) release the specified Telnet session.
7	NAG(confi g)# tel net-server max-sessi on <i>sessi on-number</i>	(Optional) configure the maximum number of Telnet sessions supported by the SNR-S212i-8POE. By default, the maximum number of Telnet sessions is 5.

- **Telnet Client:** after you connect a PC to the SNR-S212i-8POE through the terminal emulation program or Telnet client program, telnet another device through the SNR-S212i-8POE, and configure/manage it. As shown in Figure 2-4, Switch A not only acts as the Telnet server but also provides Telnet Client service.

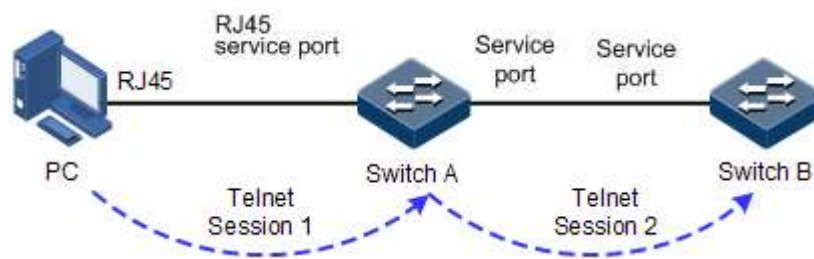


Figure 2-4 Networking with device as Telnet client

Configure the Telnet client as below.

Step	Command	Description
1	NAG# tel net <i>ip-address [port port-id]</i>	Log in to another device through Telnet.

2.1.4 Accessing through SSH

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

The way that traditional Telnet and FTP transmit password and data in plain text becomes difficult for users to accept. SSH is a network security protocol, which can effectively prevent the disclosure of information in remote management through data encryption, and provides higher security for remote login and other network services on a network.

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


Before accessing the SNR-S212i-8POE through SSH, you must log in to the SNR-S212i-8POE through the Console interface and start SSH service.

Default configurations of accessing through SSH 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
Allowable failure times for SSH authentication	20
SSH snooping port number	22
SSH session status	Enable
SSH protocol version	v1 and v2

Configure SSH service for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#generate ssh-key [length]	Generate local SSH key pair and designate its length.
3	NAG(confi g)#ssh server rekey-i nterval i nterval	(Optional) configure SSH key renegotiation period.
4	NAG(confi g)#ssh server authenti cati on { password rsa-key }	(Optional) configure SSH authentication mode.

Step	Command	Description
5	NAG(config)#ssh server authentication pubkey-name public- key [public-key]	(Optional) type the public key of clients to the SNR-S212i-8POE in rsa-key authentication mode.
6	NAG(config)#ssh server authentication- timeout period	(Optional) configure SSH authentication timeout. The SNR-S212i-8POE refuses to authenticate and then closes the connection when the client authentication time exceeds the upper limit.
7	NAG(config)#ssh server authentication- retries times	(Optional) configure the allowable failure times for SSH authentication. The SNR-S212i-8POE refuses to authenticate and then closes the connection when the times for the client to be authenticated exceed the upper limit.
8	NAG(config)#ssh server port port-id	(Optional) configure SSH snooping port number.  Note When you configure SSH Snooping port number, the input parameter cannot take effect until SSH is restarted.
9	NAG(config)#ssh server version { both v1 v2 }	(Optional) configure SSH protocol version.
10	NAG(config)#ssh server	Start the SSH server.
11	NAG(config)#ssh server session session-list enable	(Optional) enable SSH session on the SNR-S212i-8POE.

2.1.5 Checking configurations

Use the following commands to check the configuration results.

No.	Command	Description
1	NAG#show telnet-server	Show configurations of the Telnet server.
2	NAG#show ssh public-key [authentication]	Show the public key for SSH authentication used on the device and client.
3	NAG#show ssh { server session }	Show information about the SSH server or session.

2.2 CLI

2.2.1 Introduction

The CLI is a medium for you communicating with the SNR-S212i-8POE. You can configure, monitor, and manage the SNR-S212i-8POE through the CLI.

You can log in to the SNR-S212i-8POE through a terminal or a PC that runs terminal emulation program. Enter commands at the system prompt.

The CLI supports following features:

- Configure the SNR-S212i-8POE locally through the Console interface.
- Configure the SNR-S212i-8POE locally or remotely through Telnet/Secure Shell (SSH).
- Commands are classified into different levels. You can execute the commands that correspond to your level only.
- The commands available to you depend on which mode you are currently in.
- Keystrokes can be used to execute commands.
- Check or execute a historical command by checking command history. The last 20 historical commands can be saved on the SNR-S212i-8POE.
- Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.
- The SNR-S212i-8POE supports multiple intelligent analysis methods, such as fuzzy match and context association.

2.2.2 Levels

The SNR-S212i-8POE uses hierarchical protection methods to divide command line privileges into 16 levels from low to high.

- 0–4: visitor. Users can execute the **ping**, **clear**, and **history** commands, etc. in this level.
- 5–10: monitor. Users can execute the **show** command, etc.
- 11–14: operator. Users can execute commands for different services like Virtual Local Area Network (VLAN), Internet Protocol (IP), etc.
- 15: administrator. Users can execute basic command for operating the system.

2.2.3 Modes

The command mode is an environment where a command is executed. A command can be executed in one or multiple certain modes. The commands available to you depend on which mode you are currently in.

After connecting the SNR-S212i-8POE, if the device is configured with default value, you enter the user EXEC mode, where the following command is displayed:

```
NAG>
```

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

```
NAG>enabl e
Password:
NAG#
```



Note

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

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

```
NAG#confi g termi nal
NAG(confi g)#
```



Note

- The CLI prompt NAG is a default host name. You can modify it by executing the **hostname** *string* command in privileged EXEC mode.
- Commands executed in global configuration mode can also be executed in other modes. The functions vary with command modes.
- You can enter the **exit** or **quit** command to return to upper command mode. However, in privileged EXEC mode, you need to execute the **disable** command to return to user EXEC mode.
- You can execute the **end** command to return to privileged EXEC mode from any mode but user EXEC mode and privileged EXEC mode.

The SNR-S212i-8POE supports the following command line modes.

Mode	Enter method	Description
User EXEC	Log in to the SNR-S212i-8POE, use correct username and password	NAG>
Privileged EXEC	In user EXEC mode, use the enable command and correct password.	NAG#
Global configuration	In privileged EXEC mode, use the config [terminal] command.	NAG(confi g)#
Physical layer interface configuration	In global configuration mode, use the interface port <i>port-id</i> command.	NAG(confi g-port)#
Physical layer interface batch configuration	In global configuration mode, use the interface port-list <i>port-list</i> command.	NAG(confi g-range)#

Mode	Enter method	Description
Layer 3 interface configuration	In global configuration mode, use the interface ip <i>if-number</i> command.	NAG(confi g-i p)#
VLAN configuration	In global configuration mode, use the vlan <i>vlan-id</i> command.	NAG(confi g-vl an)#
Traffic classification configuration	In global configuration mode, use the class-map <i>class-map-name</i> command.	NAG(confi g-cmap)#
Traffic policy configuration	In global configuration mode, use the policy-map <i>policy-map-name</i> command.	NAG(confi g-pmap)#
Traffic policy configuration mode binding with traffic classification	In floe policy configuration mode, use the class-map <i>class-map-name</i> command.	NAG(confi g-pmap-c)#
Access control list configuration	In global configuration mode, use the access-list-map <i>acl-number</i> { deny permit } command.	NAG(confi g-acl map)#
Aggregation group configuration	In global configuration mode, use the interface port-channel <i>port-channel-number</i> command.	NAG(confi g-aggregator)#
MST region configuration	In global configuration mode, use the spanning-tree region-configuration command.	NAG(confi g-regi on)#
Cluster configuration	In global configuration mode, use the cluster command.	NAG(confi g-cl uster)#

2.2.4 Shortcut keys

The SNR-S212i-8POE supports the following shortcut keys:

Shortcut key	Description
Up cursor key (↑)	The previous command is displayed. If the current command is already the first command, nothing changes on the screen.
Down cursor key (↓)	The next command is displayed. If the current command is already the last command, nothing changes on the screen.
Left cursor key (←)	Move the cursor back one character. If the cursor is already at the beginning of a command line, nothing changes on the screen.

Shortcut key	Description
Right cursor key (→)	Move the cursor forward one character. If the cursor is already at the end of a command line, nothing changes on the screen.
Backspace	Erase the character to the left of the cursor. If the cursor is already at the beginning of a command line, nothing changes on the screen.
Tab	<p>When you press it after entering a complete keyword, the cursor moves forward a space. When you press it again, the keywords matching the complete keyword are displayed.</p> <p>When you press it after entering an incomplete keyword, the system automatically executes some commands:</p> <ul style="list-style-type: none"> • If the incomplete keyword matches a unique complete keyword, the unique complete keyword replaces the incomplete keyword, with the cursor forward a space from the unique complete keyword. • If the incomplete keyword matches no or more complete keywords, the prefix is displayed. You can press the Tab key to alternate the matched complete keywords, with the cursor at the end of the matched complete keyword. Then, press the Space bar to enter the next keyword. • If the incomplete keyword is wrong, you can press the Tab key to wrap, and then error information is displayed. However, the input incomplete keyword remains.
Ctrl+A	Move the cursor to the beginning of the command line.
Ctrl+B	Act as the left arrow (←).
Ctrl+C	The ongoing command will be interrupted, such as ping , and tracert .
Ctrl+D or Delete	Delete the character at the cursor.
Ctrl+E	Move the cursor to the end of the command line.
Ctrl+F	Act as the right arrow (→).
Ctrl+K	Delete all characters from the cursor to the end of the command line.
Ctrl+L	Clear information displayed at the screen.
Ctrl+S	Act as the down arrow (↓).
Ctrl+W	Act as the up arrow (↑).
Ctrl+X	Delete all characters from the cursor to the beginning of the command line.
Ctrl+Y	Show historical commands.
Ctrl+Z	Return to privileged EXEC mode from the current mode (excluding user EXEC mode).
Space or Y	Scroll down one screen.

Shortcut key	Description
Enter	Scroll down one line.

2.2.5 Acquiring help

Complete help

You can acquire complete help under following three conditions:

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

```
NAG>?
```

The command output is displayed as below.

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

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

```
NAG(config)#ntp ?
```

The command output is displayed 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** and enter a question mark (?), the value range and descriptions are displayed if the question mark (?) matches a parameter.

```
NAG(config)#interface Ip ?
```

The command output is displayed as below.

```
<0-14> IP interface 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.

```
NAG(config)#c?
```

The command output is displayed as below.

```
cache          Cache information
class-map      Set class map
clear          Reset functions
cluster        cluster configuration
cluster-autoactive Cluster autoactive function
command-log    Log the command to the file
cpu            Configure cpu parameters
create         Create static VLAN
```

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

```
NAG(config)#show ll?
```

The command output is displayed as below.

```
link-aggregation Link aggregation
link-state-tracking Link state 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 message

The SNR-S212i-8POE prints out the following error messages according to error types when you input incorrect commands.

Error message	Description
% Incomplete command.	The input command is incomplete.
Error input in the position marked by '^'.	It is illegal to enter commands at the position marked by '^'
Ambiguous input in the position marked by '^'	The keyword marked with '^' is unclear.



Note

Use the help information to resolve the above error messages if they are displayed.

2.2.6 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 2-1.

Table 2-1 Shortcut keys for display features

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

Filtering display information

The SNR-S212i-8POE provides a series of commands which begin with **show** to show configuration, running status, or diagnostic message of the device. You can add filtering rules to remove unwanted information.

The **show** command supports 3 filtering modes:

- | **begin string**: show all commands which start from matched specific character string.
- | **exclude string**: show all commands which do not match specific character string.
- | **include string**: show all commands which only match specific character string.

Page-break

Page-break is used to suspend displaying messages when they are displayed at more than one screen. After page-break is enabled, you can use shortcut keys listed in Table 2-1. 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 page-break for the SNR-S212i-8POE as below.

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

2.2.7 Command history

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

Configure command history for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG> terminal history <i>number</i>	(Optional) configure the number of system stored historical command.
2	NAG> terminal time-out <i>period</i>	(Optional) configure the Console terminal timeout period.
3	NAG> enable	Enter privileged EXEC mode.
4	NAG# history	Show historical input commands.
5	NAG# show terminal	Show terminal configurations.

2.2.8 Restoring default value of command line

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

To restore the default value of a commands, use the **no/enable | disable** form of the command.

- **no** form of a command: be provided in front of a command and used to restore the default value. It is used to 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 of a command: be provided behind a command or in the middle of a command. The **enable** parameter is used to enable some feature or function while the **disable** parameter is used to disable some feature or function.

For example:

- In physical layer configuration mode, the **description** *text* command is used to modify descriptions about an interface while the **no description** command is used to delete descriptions about the interface.
- Use the **shutdown** command in physical layer interface mode to disable an interface; use the **no shutdown** command to enable an interface.
- Use the **terminal page-break enable** command in global configuration mode to enable page-break; use the **terminal page-break disable** command to disable page-break.



Note

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

2.2.9 Logging command lines

Configure logging command lines for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# command-l og enabl e	Enable command line logging.
3	NAG(confi g)# show command-l og status	Show command line logging status.
4	NAG(confi g)# show command-l og	Show records on executing historical commands.

2.3 Managing users

2.3.1 Introduction

When you start the SNR-S212i-8POE for the first time, connect the PC through Console interface to the SNR-S212i-8POE, input the initial user name and password in HyperTerminal to log in and configure the SNR-S212i-8POE.

If there is not any privilege restriction, any remote user can log in to the SNR-S212i-8POE through Telnet or access network by building Point to Point Protocol (PPP) connection when service interfaces are configured with IP addresses. This is unsafe to the SNR-S212i-8POE and network. Creating user for the SNR-S212i-8POE and setting password and privilege helps manage the login users and ensures network and device security.

Authenticating user login

Users can log in to the SNR-S212i-8POE 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 levels can execute commands of the corresponding level. User privileges are also user priorities, which are classified into 15 levels corresponding to command levels, and four types:

- Levels 1–4: users can execute visitor commands.
- Levels 5–10: users can execute monitor or below commands.
- Levels 11–14: users can execute operator or below commands.
- Level 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 prohibiting them from executing some commands below their privileges.

2.3.2 Preparing for configurations

Scenario

To prevent malicious users from logging in to the SNR-S212i-8POE, and to eliminate risks on the SNR-S212i-8POE, you must effectively manage users in terms of basic information, login, and user commands.

Prerequisite

N/A

2.3.3 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: admin • Password: admin
New user privilege	15
New user activation status	Activate
New user service type	N/A
Enable password	admin
User login authentication mode	local-user
Enable login authentication mode	local-user

2.3.4 Creating user basic information

Create user basic information for the SNR-S212i-8POE as below.

Step	Configuration	Description
1	NAG#user name <i>user-name</i> password [cipher simple] <i>password</i>	Create information about a local user, or modify the login password of the specified user.
2	NAG#user <i>user-name</i> privilege <i>privilege</i>	(Optional) modify local user privilege.
3	NAG#user <i>user-name</i> service-type { lan-access ssh telnet web console all }	Configure user service type.
4	NAG#user <i>user-name</i> state { active inactive }	Configure user activation status.



Note

- Up to 10 local users can be created.
- The login password is 8–16 characters, mandatorily including digits, case-sensitive letters, and other special characters.

2.3.5 Managing user login

Manage user login for the SNR-S212i-8POE as below.

Step	Configuration	Description
1	NAG#enable password [cipher <i>password</i>]	(Optional) modify the password for entering privileged EXEC mode.
2	NAG#user login { local -radius local - user radius-local [server-no- response] radius-user local -tacacs tacacs-local [server-no-response] tacacs-user }	(Optional) configure authentication mode for user login.
3	NAG#enable login { local -radius local - user radius-local [server-no- response] radius-user local -tacacs tacacs-local [server-no-response] tacacs-user }	(Optional) modify the password authentication mode for entering privileged EXEC mode.



Note

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

2.3.6 Managing user commands

Manage user commands for the SNR-S212i-8POE as below.

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



Note

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

2.3.7 Checking configurations

Use the following commands to check the configuration results.

No.	Command	Description
1	<code>NAG#show user table [detail]</code>	Show login user information.
2	<code>NAG#show user online</code>	Show configurations of online users.

2.3.8 Example for configuring user management

Networking requirements

As shown in Figure 2-5, to prevent malicious users from logging in to the SNR-S212i-8POE, and to eliminate risks on the SNR-S212i-8POE, configure user management as below:

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

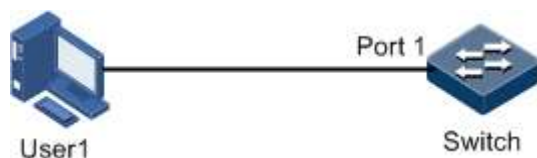


Figure 2-5 User management networking

Configuration steps

- Step 1 Configure user login authentication mode.

```
NAG#user login local -user
```

Step 2 Create a local user user1.

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

Step 3 Configure user privilege.

```
NAG#user user1 privilege 10
```

Step 4 Configure user service type.

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

Step 5 Configure user command management.

```
NAG#user user1 allow-exec mirror
```

Checking results

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

```
NAG#show user table detail
```

```
User Login : local -user
```

```
Enable Login: local -user
```

```
Username   : admin
```

```
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 SNR-S212i-8POE, and check whether user privilege is correctly configured.

```
Logi n: user1  
Password:  
NAG>enabl e  
NAG#confi g  
NAG(confi g)#mi rror enabl e  
Set successful l y.
```

As you can see above, user1 of privilege 10 can execute the command starting with **mirror** successfully after you configure user command management.

2.4 Web network management

2.4.1 Introduction

You can manage and configure the SNR-S212i-8POE through the Web configuration interface. With the Web browser, you can access the homepage related to the IP address of the management VLAN interface.

2.4.2 Preparing for configuraitons

Scenario

After Web network management is enabled, remote users can log in to the SNR-S212i-8POE through the Web browser and manage it. After Web network management is disabled, all established Hyper Text Transport Protocol/Hyper Text Transport Protocol Secure (HTTP/HTTPS) connections are disconnected and related user information is cleared.

Prerequisite

Configure the IP address of the management VLAN interface.

2.4.3 Default configurations of Web network management

Default configurations of Web network management are as below.

Function	Default value
HTTP	Enable
HTTPS	Disable
HTTP listening port ID	80
HTTPS listening port ID	443
Login authentication mode	local
Timeout for no operation after login	1200s

2.4.4 Configuring Web network management

Configure Web network management for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i p http server enable	Enable HTTP.
3	NAG(confi g)# i p https server enable	(Optional) enable HTTPS.
4	NAG(confi g)# i p { http https } port port-number	(Optional) configure the HTTP/HTTPS listening port ID.
5	NAG(confi g)# i p http timeout time	(Optional) configure the timeout for no operation after login.

2.4.5 Checking configurations

No.	Command	Description
1	NAG# show web server	Show configurations of the Web server.
2	NAG# show web clients	Show information about Web users.

2.5 Managing files

2.5.1 Managing BootROM files

The BootROM file is used to boot the SNR-S212i-8POE and finish device initialization. You can upgrade the BootROM file through File Transfer Protocol (FTP) FTP or Trivial File Transfer Protocol (TFTP). By default, the name of the BootROM file is bootrom or bootromfull.

After powering on the SNR-S212i-8POE, run the BootROM files at first, click **Ctrl+B** to enter BootROM menu when the prompt "Press Ctrl+B into Bootrom menu..." appears:

```
starting.....
Press <CTRL+B> key to enter boot menu: 0
```

In Boot mode, you can do the following operations.

Operation	Description
?	List all executable operations.
v	Show BootROM version information.
b	Quickly execute system bootrom software.
c	Modify parameters of the TFTP server.
m	Download the .bin file to the Random Access Memory (RAM).
T	Download and replace the system startup file through TFTP.
B	Update the Boot file through TFTP to the flash.
X	Update the Boot file through the XMODEM to the flash
R	Reboot the SNR-S212i-8POE.

Configure the SNR-S212i-8POE as below.

All the following steps are optional and no sequencing.

Step	Configuration	Description
1	<code>NAG#download bootstrap [master slave] { ftp ip-address user-name password file-name sftp ip-address user-name password file-name tftp ip-address file-name }</code>	(Optional) download the BootROM file through FTP, Secure File Transfer Protocol (SFTP), or TFTP.
2	<code>NAG#upload bootstrap [master slave] { ftp ip-address user-name password file-name sftp ip-address user-name password file-name tftp ip-address file-name }</code>	(Optional) upload the BootROM file through FTP, SFTP, or TFTP.
3	<code>NAG#erase [file-name]</code>	(Optional) delete files saved in the flash.

2.5.2 Managing system files

System files are the files needed for system operation (like system startup software and configuration file). These files are usually saved in the memory. The SNR-S212i-8POE

manages them by a file system to facilitate user managing the memory. The file system can create, delete, and modify the file and directory.

In addition, the SNR-S212i-8POE supports dual-system. There are 2 sets of system software saved at the memory. These 2 sets of system software are independent. When the SNR-S212i-8POE fails to work due to upgrade failure, you can use another set to boot the SNR-S212i-8POE.

Manage system files for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# download system [<i>master</i> <i>slave</i>] { ftp <i>ip-address user-name password file-name</i> sftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }	(Optional) download the system boot file through FTP, SFTP, or TFTP.
2	NAG# upload system [<i>master</i> <i>slave</i>] { ftp <i>ip-address user-name password file-name</i> sftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }	(Optional) upload the system boot file through FTP, SFTP, or TFTP.
3	NAG# erase [<i>file-name</i>]	(Optional) delete files saved in the Flash.

2.5.3 Managing configuration files

Configuration files are loaded after starting the system; different files are used in different scenarios to achieve different service functions. After starting the system, you can configure the SNR-S212i-8POE and save the configuration files. New configurations will take effect in next boot.

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

- Be saved as 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 SNR-S212i-8POE 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 SNR-S212i-8POE uses the default parameters for initialization.

The configuration that is currently used by the SNR-S212i-8POE is called the running configuration.

You can modify the running configuration of SNR-S212i-8POE through CLI. The running configuration can be used as initial configuration upon next power-on. You must use the **write** command to save running configurations in the memory and form a configuration file.

Manage configuration files for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# download startup-config { ftp <i>ip-address user-name password file-name</i> sftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }	Download the startup configuration file through FTP, SFTP, or TFTP.
2	NAG# erase [<i>file-name</i>]	Delete files saved in the Flash.
3	NAG# upload startup-config { ftp <i>ip-address user-name password file-name</i> sftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }	Upload the startup configuration file through FTP, SFTP, or TFTP.
4	NAG# upload logging-file [master slave] { ftp <i>ip-address user-name password file-name</i> sftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }	Upload the system log file through FTP, SFTP, or TFTP.
5	NAG# upload command-log { ftp <i>ip-address user-name password file-name</i> sftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }	Upload the command line logging file and system logs through FTP, SFTP, or TFTP.
6	NAG# wri te	Save the running configuration file into the Flash.

2.5.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG# show startup-config	Show configurations loaded upon device startup.
2	NAG# show running-config [interface [port-list <i>port-list</i>]]	Show the running configurations.

2.6 System upgrade

The SNR-S212i-8POE needs to be upgraded if you wish to add new features, optimize functions, or fix bugs in the current software version.

The SNR-S212i-8POE supports the following two upgrade modes:

- Upgrade through BootROM
- Upgrade through CLI

2.6.1 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.

Before upgrading system software through BootROM, you should build a TFTP environment, and use the PC as the TFTP server and the SNR-S212i-8POE as the client. Basic requirements are as below.

- Configure the TFTP server. Ensure that the FTP server is available.
- Configure the IP address of the TFTP server; keep it in the same network segment with IP address of the SNR-S212i-8POE.

Upgrade system software through BootROM for the SNR-S212i-8POE as below.

Step	Operation
1	<p>Log in to the SNR-S212i-8POE through serial interface as the administrator, enter Privileged EXEC mode, and reboot the SNR-S212i-8POE with the reboot command.</p> <pre>NAG#reboot Please input 'yes' to confirm: yes Rebooting ... 1970-01-01, 08: 03: 26 SYSTEM-4-SYSTEM_REBOOT: system reboot starting.... Press <CTRL+B> key to enter boot menu: 0</pre>
2	<p>When the system displays "Press Ctrl+B to enter big boot menu", press Ctrl+B to enter the Boot# interface, which displays the following command lines:</p> <pre>***** * SNR-S212i -8POE BOOT Menu * ***** v - Show uboot versi on i nformati on b - Boot system from flash c - Set TFTP parameters m - Download Image to RAM and Run (TFTP) T - Update ROS App to flash (TFTP) B - Update boot to flash (TFTP) X - Update boot to flash (XModem) R - Reboot system Boot#</pre> <p> Caution Input letters are case sensitive.</p>

Step	Operation
3	<p>Input "T" to download and replace the system bootstrap file as below:</p> <pre> Boot# T dev name: SNR-S212i -8POE file name: system_boot.Z s212i_8POE_1. 1. 1. 20120705 local ip: 192.168.4.33 192.168.18.250 server ip: 192.168.4.13 192.168.18.16 Loading... Done Saving file to flash... </pre> <p> Caution The file name input here must be correct and cannot exceed 80 characters. Ensure that the SNR-S212i-8POE is powered on during saving the system file to the Flash.</p>
4	Input "b" to quick execute the BootRom file. The SNR-S212i-8POE will restart and load the downloaded the system bootstrap file.

2.6.2 Upgrading system software through CLI

Before upgrading system software through CLI, you should build a FTP environment, and use a PC as the FTP server and the SNR-S212i-8POE as the client. Basic requirements are as below.

- The SNR-S212i-8POE connects to the FTP/SFTP/TFTP server.
- Configure the FTP/SFTP/TFTP server, and ensure that the server is available.
- Configure the IP address of the FTP/SFTP/TFTP server to ensure that SNR-S212i-8POE can access the server.

Upgrade system software through CLI for the SNR-S212i-8POE as below.

Step	Command	Description
1	<pre> NAG#download system [master slave] { ftp ip-address user- name password file-name sftp ip-address user-name password file-name tftp ip-address file-name } </pre>	Download the system bootstrap file through FTP/SFTP/TFTP.
2	<pre> NAG#reboot [now] </pre>	Reboot the SNR-S212i-8POE, and it will automatically load the downloaded system bootstrap file.

2.6.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG# show version	Show system version.

2.7 Configuring time management

2.7.1 Configuring time and time zone

To make the SNR-S212i-8POE to work coordinately with other devices, you must configure system time and belonged time zone accurately.

The SNR-S212i-8POE 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
System time zone	+08:00
Time zone offset	+08:00
DST status	Disable
System clock display mode	Default


Configure time and time zone for the SNR-S212i-8POE as below.

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

2.7.2 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 SNR-S212i-8POE as below.

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



Note

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

2.7.3 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 SNR-S212i-8POE adopts multiple NTP working modes for time synchronization:

- Server/Client 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 peer mode

In this mode, the symmetric active peer sends a clock synchronization message to the symmetric passive peer. The symmetric passive peer works in passive mode automatically

after receiving the message and sends the answering message back. By exchanging messages, the two peers build up the symmetric peer mode. The symmetric active peer and symmetric passive peer in this mode can synchronize each other.

Default configurations of NTP are as below.

Function	Default value
Whether the SNR-S212i-8POE is NTP master clock	No
Global NTP server	Inexistent
Global NTP symmetric peer	Inexistent
Reference clock source	0.0.0.0

Configure NTP for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#ntp server <i>ip-address</i> [<i>version</i> [<i>v1</i> <i>v2</i> <i>v3</i>]]	(Optional) configure NTP server address for the client working in server/client mode.
3	NAG(confi g)#ntp peer <i>ip-address</i> [<i>version</i> [<i>v1</i> <i>v2</i> <i>v3</i>]]	(Optional) configure NTP peer address for the SNR-S212i-8POE working in symmetric peer mode.
4	NAG(confi g)#ntp refcl ock-master [<i>ip-address</i>] [<i>stratum</i>]	Configure clock of the SNR-S212i-8POE as NTP reference clock source for the SNR-S212i-8POE.



Note

If the SNR-S212i-8POE is configured as the NTP reference clock source, it cannot be configured as the NTP server or NTP symmetric peer; vice versa.

2.7.4 Configuring SNTP

Simple Network Time Protocol (SNTP) is used to synchronize the system time of the SNR-S212i-8POE with the time of the SNTP device on the network. The time synchronized by SNTP protocol is Greenwich Mean Time (GMT), which can be translated into the local time according to system settings of time zone.

Default configurations of SNTP are as below.

Function	Default value
IP address of the SNTP server	Inexistent
Broadcast status of the SNTP client	Disable

Function	Default value
Multicast status of the SNTP client	Disable
SNTP status of the IP interface	Disable

Configuring unicast feature of SNTP client

Configure unicast feature of SNTP client for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#sntp server <i>ip-address</i>	Configure the IP address of the SNTP unicast server. After the SNTP server is configured with an IP address, the SNR-S212i-8POE tries to get the clock information from the SNTP server every 10s. In addition, the maximum timeout is 60s.

Configuring broadcast feature of SNTP client

Configure broadcast feature of the SNTP client for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#sntp broadcast client	(Optional) configure the broadcast feature of the SNTP client. The IP address of the SNTP server is unavailable. The SNR-S212i-8POE listens to the multicast address (255.255.255.255) at any time and obtains the clock information from the SNTP broadcast server. In addition, the maximum timeout is 60s.
3	NAG(confi g)#i nterface ip <i>if-number</i>	Enter Layer 3 interface configuration mode.
4	NAG(confi g-i p)#sntp enabl e	Enable SNTP.

Configuring multicast feature of SNTP client

Configure multicast feature of SNTP client for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.

Step	Command	Description
2	<code>NAG(config)#sntp multicast client</code>	(Optional) configure the multicast feature of the SNTP client. The IP address of the SNTP server is unavailable. The SNR-S212i-8POE listens to the multicast address (224.0.1.1) at any time and obtains the clock information from the SNTP multicast server. In addition, the maximum timeout is 60s.
3	<code>NAG(config)#interface ip <i>if-number</i></code>	Enter Layer 3 interface configuration mode.
4	<code>NAG(config-ip)#sntp enable</code>	Enable SNTP.

2.7.5 Checking configurations

Use the following commands to check configuration results.

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

2.8 Configuring interface management

2.8.1 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 SNR-S212i-8POE supports both Ethernet electrical and optical interfaces.

Auto-negotiation

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

Cable connection

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

The Ethernet cable of the SNR-S212i-8POE supports MDI/MDI-X auto-negotiation.

2.8.2 Default configurations of interface management

Default configurations of interface management are as below.

Function	Default value
Maximum forwarding frame length of interface	9712 Bytes
Duplex mode of interface	Auto-negotiation
Interface rate	Auto-negotiation
Time interval of interface dynamic statistics	2s
MDI wiring of the electrical interface	Auto
Interface flow control status	Disable
Interface status	Enable
L2protocol peer stp status	Disable

2.8.3 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 then you have to adjust the interface attributes to make the devices at both ends match each other.

The Ethernet physical layer works in three modes as below:

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

Configure the basic attributes of interface for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.

Step	Command	Description
2	NAG(config)# system mtu size	Configure the MTU for all interfaces. MTU is the maximum number of Bytes allowed to pass on the interface (without fragment). When the length of the message to be forwarded exceeds the maximum value, the SNR-S212i-8POE will discard this message automatically.
3	NAG(config)# interface port port-id	Enter physical layer interface configuration mode.
4	NAG(config-port)# duplex { auto full half }	Configure the duplex mode of the interface.
5	NAG(config-port)# speed { auto 10 100 }	Configure the interface rate. The rate of an optical interface depends on specifications of the selected optical module.
6	NAG(config-port)# mdi { auto normal xover }	Configure the MDI wiring of the electrical interface.

2.8.4 Configuring interface rate statistics

Enabling interface rate statistics

Enable interface rate statistics for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(config)# interface port port-id	Enter physical layer interface configuration mode.
3	NAG(config-port)# rate-statistics enable	Enable interface rate statistics.

Configuring dynamic interface statistics

Configure dynamic interface statistics for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(config)# dynamic statistics time period	(Optional) configure the interval for dynamically taking interface statistics.
3	NAG(config)# clear interface port-list port-list statistics	Clear interface statistics saved on the SNR-S212i-8POE.

Configuring interval for interface rate statistics

Configure the interval for interface rate statistics for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# rate-moni tor i nterval <i>second</i>	(Optional) configure the interval for interface rate statistics.

Configuring interface rate threshold

Configure the interface rate threshold for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i nterface port <i>port-i d</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)# rate- threshol d { egress i ngress } <i>threshol d</i>	Configure the interface rate threshold.

2.8.5 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 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 SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i nterface port <i>port-i d</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)# fl owcontrol { off on }	Enable/Disable interface flow control over 802.3x packets.

2.8.6 Enabling/Disabling interfaces

Enable/Disable an interface for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.

Step	Command	Description
2	NAG(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(config-port)# shutdown	Disable the current interface. Use the no shutdown command to re-enable the disabled interface.

2.8.7 Configuring L2Protocol Peer STP

To interconnect with the device that sends STP packets with the destination MAC address of 0180.C200.0008, you need to configure L2Protocol Peer STP on the SNR-S212i-8POE. If this function is enabled, the destination MAC address of BPDU, sent through STP, is 0180.C200.0008; otherwise, it is 0180.C200.0000.

Configure L2Protocol Peer STP for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(config-port)# l 2protocol peer stp	Enable L2Protocol Peer STP.



2.8.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG# show interface [port-list <i>port-list</i>]	Show interface status.
2	NAG# show interface port-list <i>port-list</i> statistics [dynamic] [detail] NAG# show interface port statistics	Show interface statistics.
3	NAG# show interface port-list <i>port-list</i> flowcontrol NAG# show interface port flowcontrol	Show flow control on the interface.
4	NAG# show system mtu	Show the system MTU.
5	NAG# show l2protocol peer stp [port- list <i>port-list</i>]	Show status of L2protocol Peer STP on the interface.
6	NAG# show interface port mdi	Show the MDI wiring of the interface.
7	NAG# show rate-monitor [port-list <i>port-</i> <i>list</i>]	Show configurations of monitoring interface rate.

2.9 Configuring basic information

Configure basic information for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#hostname <i>name</i>	(Optional) configure the device name. By default, the device name is NAG. The system supports changing device name to make users distinguish different devices on the network. Once the device name changes, it can be seen in terminal prompt.
2	NAG#language { chinese english }	(Optional) configure language mode. By default, the language is English.
3	NAG#write	Save configurations. Save configurations to the SNR-S212i-8POE after configurations, and the new configurations will overwrite the original configurations. Without saving, the new configurations will be lost after rebooting, and the SNR-S212i-8POE will continue working with the original configurations.  Caution After saving the configuration file, you can use the dir command to show it. Use the erase file-name command to delete the configuration file. This operation cannot be rolled back, so use this command with care.
4	NAG#reboot [now]	(Optional) configure reboot options. When the SNR-S212i-8POE fails, reboot it to try to solve the problem according to actual condition.  Caution <ul style="list-style-type: none"> • Rebooting the SNR-S212i-8POE interrupts services, so use the command with care. • Save configurations before rebooting to avoid loss of configurations.

2.10 Task scheduling

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

The SNR-S212i-8POE supports realizing task scheduling by combining the program list to command lines. You just need to specify the start time of the task, period, and end time in the

program list, and then bind the program list to command lines to realize the periodic execution of command lines.

Configure task scheduling for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)# schedul e-l i s t <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 time-</i> <i>interval</i> [stop <i>mm-dd-yyyy hh:mm:ss</i>] } NAG(confi g)# schedul e-l i s t <i>list-number</i> start date-time <i>mm-dd-yyyy hh:mm:ss</i> every weekday-l i s t { <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>worki ng-day</i> <i>weekday-l i s t</i> } NAG(confi g)# schedul e-l i s t <i>list-number</i> start up-time <i>days-after-startup hh:mm:ss</i> [every <i>days-interval time-interval</i> [stop <i>days-after-startup hh:mm:ss</i>]]	Create a schedule list, and configure it.
3	NAG(confi g)# command-string schedul e-l i s t <i>list-number</i>	Bind the command line which needs periodical execution and supports the schedule list to the schedule list.
4	NAG# show schedul e-l i s t [<i>list-number</i>]	Show configurations of the scheduling list.

2.11 Watchdog

2.11.1 Introduction

External electromagnetic field interferes with the working of single chip microcomputer, and causes program fleet and dead circulation so that the system cannot work normally. Considering the real-time monitoring of the running state of single chip microcomputer, a program is specially used to monitor the running status of switch hardware, which is commonly known as the Watchdog.

The SNR-S212i-8POE will be rebooted when it fails due to task suspension or dead circulation, and without feeding the dog within a feeding dog cycle.

The Watchdog function can prevent the system program from dead circulation due to uncertain fault, thus improving stability of the system.

2.11.2 Preparing for configurations

Scenario

By configuring Watchdog, you can prevent the system program from dead circulation due to uncertain fault and thus improve the stability of system.

Prerequisite

N/A

2.11.3 Default configurations of watchdog

Default configurations of Watchdog are as below.

Function	Default value
Watchdog status	Enable Watchdog.

2.11.4 Configuring Watchdog

Configure Watchdog for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# watchdog enable	Enable Watchdog. Use the watchdog disable command to disable this function.
2	NAG# show watchdog	Show Watchdog status.

3 Ethernet

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

- MAC address table
- VLAN
- QinQ
- VLAN mapping
- STP/RTSTP
- MSTP
- GARP
- Loopback detection
- Line detection
- Interface protection
- Port mirroring
- Layer 2 protocol transparent transmission

3.1 MAC address table

3.1.1 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 fast forwarding of packets, and reduces broadcast traffic. The MAC address table is saved in the memory of the SNR-S212i-8POE, of which the capacity determines the number of MAC addresses it can save.

The MAC address table contains the following information:

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

The SNR-S212i-8POE supports showing MAC address information by device, interface, or VLAN.

MAC address forwarding modes

When forwarding packets, based on the information about MAC addresses, the SNR-S212i-8POE adopts 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 SNR-S212i-8POE will directly forward the packet to the receiving port through the egress interface of the MAC address entry. If the entry is not listed, the SNR-S212i-8POE broadcasts the packet to all interfaces except the receiving interface.
- **Multicast:** when the SNR-S212i-8POE receives a packet of which the destination MAC address is a multicast address, it sends the packet in broadcast mode. It sends the packet to the specified Report interface if multicast is enabled. If this MAC address is listed in the MAC address table, the SNR-S212i-8POE transmits the packet from the egress interface. If the MAC address is not listed, the SNR-S212i-8POE broadcasts the packet to all interfaces except the receiving interface.
- **Broadcast:** when the SNR-S212i-8POE receives an all-F packet, or this MAC address is not listed in the MAC address table, the SNR-S212i-8POE forwards the packet to all interfaces except the receiving interface.

Classification of MAC addresses

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

- **Static MAC address entry:** also called "permanent address", added and removed by the user manually, not aged with time. For a network with small changes of devices, adding static address entry manually can reduce the network broadcast flow, improve the security of the interface, and prevent entries from being lost after the system is rebooted.
- **Dynamic MAC address entry:** the SNR-S212i-8POE can add dynamic MAC address entries through MAC address learning. The entries are aged according to the configured aging time, and will be empty after the system is rebooted.

The SNR-S212i-8POE supports the maximum 16K dynamic MAC addresses, and 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 SNR-S212i-8POE. To maximize the use of the MAC address table, the SNR-S212i-8POE uses the aging mechanism to update the MAC address table. For example, when the SNR-S212i-8POE creates a dynamic entry, it starts the aging timer. If it does not receive packets from the MAC address in the entry during the aging time, the SNR-S212i-8POE will delete the entry.

MAC address limit

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

MAC address limit improves the speed of forwarding packets.

3.1.2 Preparing for configurations

Scenario

Configure the static MAC address table in the following situations:

- The static MAC address can be configured for a fixed server, special persons (manager, financial staff, etc.), fixed and important hosts to ensure that all data flow forwarding to these MAC addresses are forwarded from static MAC address related interface in priority.
- For the interface with fixed static MAC address, you can disable MAC address learning to avoid other hosts visiting LAN data from the interface.

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

Prerequisite

N/A

3.1.3 Default configurations of MAC address table

Default configurations of the MAC address table are as below.

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

3.1.4 Configuring static MAC address

Configure static MAC address as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# mac-address-table static unicast <i>mac-address</i> vl an <i>vlan-id</i> port <i>port-id</i>	Configure static unicast MAC addresses.
	NAG(confi g)# mac-address-table static multi cast <i>mac-address</i> vl an <i>vlan-id</i> port-list <i>port-list</i>	Configure static multicast MAC addresses.



Note

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

3.1.5 Configuring blackhole MAC address

Configure blackhole MAC addresses as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#mac-address-table bl ackhol e <i>mac-address</i> vl an <i>vl an- id</i>	Configure blackhole MAC addresses.

3.1.6 Filtering unknown multicast packets

Filter unknown multicast packets for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#mac-address-table mul ti cast fi lter { all vl an <i>vl an-list</i> }	(Optional) configure filtering unknown multicast packets.

3.1.7 Configuring MAC address learning

Configure MAC address learning for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#mac-address-table l earni ng enabl e port-l i st <i>port-list</i>	Enable MAC address learning.

3.1.8 Configuring MAC address limit

Configure the MAC address limit for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#i nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)#mac-address- tabl e threshol d <i>threshol d-val ue</i>	Configure the MAC address limit on the interface.

3.1.9 Configuring aging time of MAC addresses

Configure the aging time of MAC addresses for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#mac-address-table agi ng-ti me { 0 <i>period</i> }	Configure the aging time of MAC addresses.

3.1.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show mac-address-table stati c [<i>port port-id</i> <i>vlan vlan-id</i>]	Show static unicast MAC addresses.
2	NAG#show mac-address-table mul ti cast [<i>vlan vlan-id</i>] [<i>count</i>]	Show all Layer 2 multicast addresses and the current multicast MAC address limit.
3	NAG#show mac-address-table bl ackhol e	Show blackhole MAC addresses.
4	NAG#show mac-address-table l2- address [<i>count</i>] [<i>vlan vlan-id</i> <i>port port-id</i>]	Show all Layer 2 unicast MAC addresses and the current unicast MAC address limit.
5	NAG#show mac-address-table threshol d [<i>port-list port-list</i>]	Show dynamic MAC address limit.
6	NAG#show mac agi ng-ti me	Show the aging time of dynamic MAC addresses.
7	NAG#show mac-address-table l earni ng <i>port-list port-list</i>	Show MAC address learning status.

3.1.11 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	NAG(confi g)#cl ear mac-address-table { <i>all</i> <i>blackhole</i> <i>dynamic</i> <i>static</i> }	Clear MAC addresses.
2	NAG(confi g)#search mac-address <i>mac-</i> <i>address</i> { <i>all</i> <i>dynamic</i> <i>static</i> } [<i>port port-id</i>] [<i>vlan vlan-id</i>]	Search for an MAC address.

3.1.12 Example for configuring MAC address table

Networking requirements

As shown in Figure 3-1, configure Switch A as below:

- Configure a static unicast MAC address 0001.0203.0405 on Port 2 and set its VLAN to VLAN 10.
- Set the aging time to 500s.

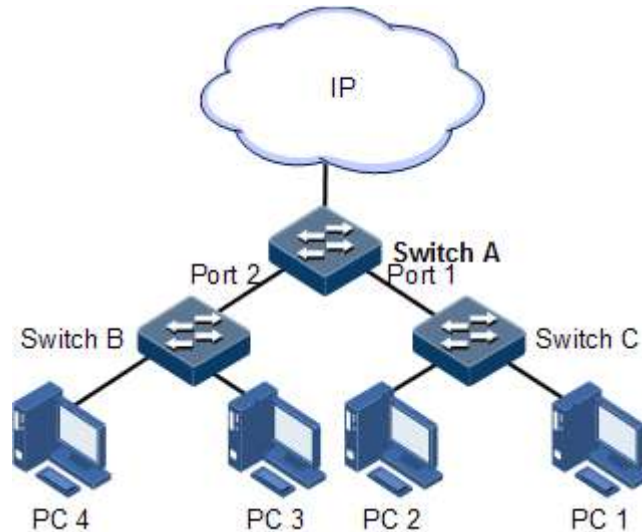


Figure 3-1 MAC networking

Configuration steps

Step 1 Create VLAN 10 and active it, and add Port 2 into VLAN 10.

```
NAG#confi g
NAG(confi g)#create vl an 10 acti ve
NAG(confi g)#i nterface port 2
NAG(confi g-port)#swi tchport mode access
NAG(confi g-port)#swi tchport access vl an 10
NAG(confi g-port)#exi t
```

Step 2 Configure a static unicast MAC address 0001.0203.0405 on Port 2, which belongs to VLAN 10.

```
NAG(confi g)#mac-address-table stati c uni cast 0001.0203.0405 vl an 10 port 2
```

Step 3 Set the aging time to 500s.

```
NAG(confi g)#mac-address-table agi ng-ti me 500
```

Checking results

Use the **show mac-address-table l2-address port** *port-id* to show configurations of MAC addresses.

```
NAG#show mac-address-table l2-address port 2
Aging time: 500 seconds
Mac Address      Port      Vl an    Fl ags
-----
0001.0203.0405  port2    10      stati c
```

3.2 VLAN

3.2.1 Introduction

Overview

Virtual Local Area Network (VLAN) is a protocol to solve Ethernet broadcast and security problem. It is a Layer 2 isolation technique that partitions a LAN into different broadcast domains logically rather than physically, and then the different broadcast domains can work as virtual groups without any influence from one another. In terms of functions, VLAN has the same features as LAN, but members in one VLAN can access one another without restriction by physical location, as shown in Figure 3-2.

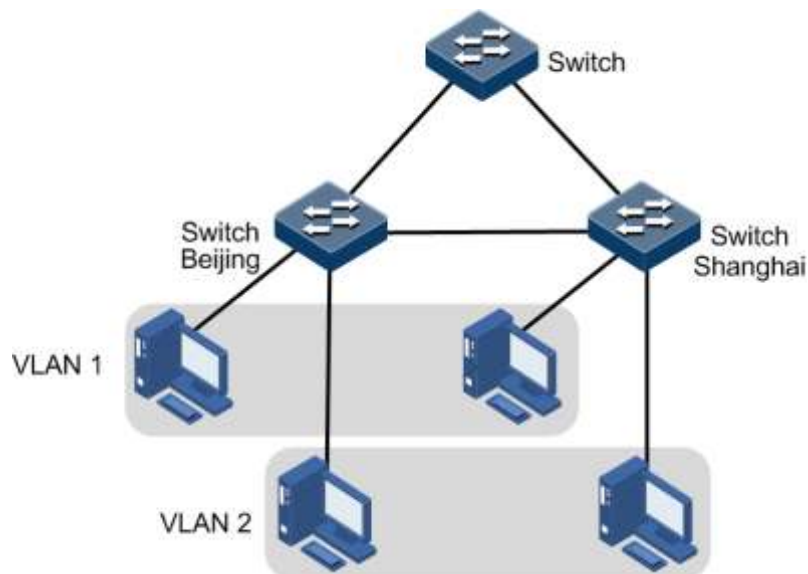


Figure 3-2 Partitioning VLANs

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

The SNR-S212i-8POE complies with IEEE 802.1Q standard VLAN and supports 4094 concurrent VLANs.

Interface forwarding mode

The SNR-S212i-8POE supports VLAN partitioning by interface. The SNR-S212i-8POE has two interface modes: Access mode and Trunk mode. The method of dealing with packet for the two modes shows as below.

Table 3-1 Interface mode and packet processing

Interface type	Processing ingress packets		Processing egress packets
	Untag packets	Tag packets	
Access	Add Access VLAN Tag to the packet.	<ul style="list-style-type: none"> • If VLAN ID = Access VLAN ID, receive the packet. • If VLAN ID ≠ Access VLAN ID, discard the packet. 	<ul style="list-style-type: none"> • If VLAN ID = Access VLAN ID, remove Tag and transmit the packet. • The VLAN ID list allowed to pass by the interface does not include the VLAN ID of the packet, discard the packet.
Trunk	Add Native VLAN Tag to the packet.	<ul style="list-style-type: none"> • If the packet VLAN ID is included in the VLAN ID list allowed to pass by the interface, receive the packet. • If the packet VLAN ID is not included in the VLAN ID list allowed to pass by the interface, discard the packet. 	<ul style="list-style-type: none"> • If VLAN ID = Native VLAN ID, remove Tag and transmit the packet. • If VLAN ID ≠ Native VLAN ID, and the interface allows the packet to pass, transmit the packet with Tag.

3.2.2 Preparing for configurations

Scenario

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

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

want to communicate among different VLAN. The cascaded interfaces among devices are set in Trunk mode.

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

Prerequisite

N/A

3.2.3 Default configurations of VLAN

Default configurations of VLAN are as below.

Function	Default value
Create VLAN	VLAN 1 and VLAN 4093
Active status of static VLAN	Suspend
Interface mode	Access
Access VLAN	VLAN 1
Native VLAN of Trunk interface	VLAN 1
Allowable VLAN in Trunk mode	All VLANs
Allowable Untag VLAN in Trunk mode	VLAN 1

3.2.4 Configuring VLAN attributes

Configure VLAN attributes for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# create vl an <i>vlan-list</i> { acti ve suspend }	Create a VLAN. The command can also be used to create VLANs in batches.
3	NAG(confi g)# vl an <i>vlan-id</i>	Enter VLAN configuration mode.
4	NAG(confi g-vl an)# name <i>vlan-name</i>	(Optional) configure the VLAN name.
5	NAG(confi g-vl an)# state { acti ve suspend }	Configure VLAN in active or suspend status.



Note

- The VLAN created by the **vlan** *vlan-id* command is in suspend status, you need to use the **state active** command to activate the VLAN to make it take effect in the system.
- By default, there are two VLANs in system, the default VLAN (VLAN 1) and cluster VLAN (VLAN 4093). All interfaces in Access mode belong to default VLAN. Both VLAN 1 and VLAN 4093 cannot be created and deleted.
- By default, the default VLAN (VLAN 1) is called Default. Other VLAN is named as "VLAN + 4-digit VLAN ID". For example, VLAN 10 is named VLAN0010 by default, and VLAN 4094 is named as VLAN4094 by default.
- All configurations of VLAN do not take until the VLAN is activated. When VLAN status is Suspend, you cannot configure the VLAN, such as deleting/adding interface, setting VLAN name. The system will save the configurations. Once the VLAN is activated, the configurations will take effect in the system.

3.2.5 Configuring interface mode

Configure interface mode for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)# swi tchport mode { access trunk }	Configure the interface to Access or Trunk mode.

3.2.6 Configuring VLAN on Access interface

Configure VLAN on the Access interface for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)# swi tchport mode access NAG(confi g-port)# swi tchport access vl an <i>vlan-id</i>	Configure interface in Access mode, and add the Access interface into the VLAN.
4	NAG(confi g-port)# swi tchport access egress-al lowed vl an { { all <i>vlan-list</i> } [confi rm] { 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, and the forwarded packets do not carry VLAN Tag.
- When setting 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 or suspend the Access VLAN manually, the system will automatically set the interface Access VLAN as default VLAN.
- If the configured Access VLAN is not 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.
- The allowed VLAN list of the Access interface is only effective to static VLANs, and ineffective to cluster VLAN, GVRP dynamic VLAN, etc.

3.2.7 Configuring VLAN on Trunk interface

Configure VLAN on the Trunk interface for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#i nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)#swi tchport mode trunk	Configure the interface in Trunk mode.
4	NAG(confi g-port)#swi tchport trunk native vl an <i>vl an-id</i>	Configure the Native VLAN of the interface.
5	NAG(confi g-port)#swi tchport trunk allowed vl an { { all <i>vl an-list</i> } [confi rm] { add remove } <i>vl an-list</i> }	(Optional) configure VLANs allowed to pass by the Trunk interface.
6	NAG(confi g-port)#swi tchport trunk untagged vl an { { all <i>vl an-list</i> } [confi rm] { add remove } <i>vl an-list</i> }	(Optional) configure VLANs from which the Trunk interface can remove Tag.



Note

- The interface allows Native VLAN packets to pass regardless of configuration in the VLAN list and Untagged VLAN list allowed by the Trunk interface, and the forwarded packets do not carry VLAN Tag.
- The system will create and activate the VLAN if no VLAN is created and activated in advance when setting the Native VLAN.
- The system set the interface Trunk Native VLAN as default VLAN if you have deleted or blocked Native VLAN manually.
- The interface allows incoming and outgoing VLAN packet allowed by the Trunk interface. If the VLAN is Trunk Untagged VLAN, the VLAN Tag is removed from the packets at the egress interface; otherwise the packets are not modified.

- If the configured Native VLAN is not default VLAN, and there is no default VLAN in Trunk interface allowed VLAN list, the interface will not allow default VLAN packets to pass.
- When setting Trunk Untagged VLAN list, the system automatically adds all Untagged VLAN into the VLAN allowed by the Trunk interface.
- The VLAN list and Untagged VLAN list allowed by the Trunk interface are only effective to static VLAN, and ineffective for cluster VLAN, GVRP dynamic VLAN, etc.

3.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show vl an [vl an-l i s t s t a t i c d y n a m i c] [d e t a i l]	Show VLAN configurations.
2	NAG#show i n t e r f a c e <i>port port-id</i> s w i t c h p o r t	Show configurations of the interface VLAN.

3.3 QinQ

3.3.1 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 takes double VLAN Tag to transmit through backbone network (public network) of the carrier. On the public network, packets are transmitted in accordance with outer VLAN Tag (namely the public network VLAN Tag), the user private network VLAN Tag is transmitted as data in packets.

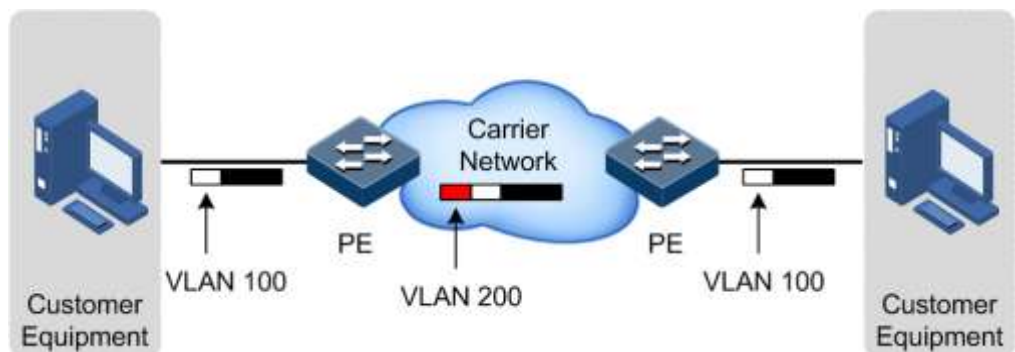


Figure 3-3 Principle of basic QinQ

Typical networking of basic QinQ is shown as Figure 3-3, the SNR-S212i-8POE is the PE.

The packet transmitted to the switch from user device, and the VLAN ID of packet tag is 100. The packet will be printed outer tag with VLAN 200 when passing the user side interface on the PE device and then enter the PE network.

The VLAN 200 packet is transmitted to the PE on the other end of the carrier, and then the other Switch will remove the outer tag VLAN 200 and send it to the user device. So the packet returns to the status that it carries VLAN 100 Tag only.

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

Selective QinQ

Selective QinQ is an enhancement to basic QinQ, which classifies flow according to user data features, then encapsulates different types flow into different outer VLAN Tags. This technique is realized by 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 Tag 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.

The SNR-S212i-8POE supports up to 1000 selective QinQ.

3.3.2 Preparing for configurations

Scenario

Basic QinQ configuration and selective QinQ configuration for the SNR-S212i-8POE are based on different service requirements.

- Basic QinQ

With application of basic QinQ, you can add outer VLAN Tag to layout Private VLAN ID freely to make the user device data at both ends of carrier network take transparent transmission without conflicting with VLAN ID in service provider network.

- Selective QinQ

Different from basic QinQ, outer VLAN Tag of selective QinQ can be selectable according to different services. There are multiple services and different private VLAN ID in the user network which are divided by adding different outer VLAN Tag for voice, video, and data services etc. Then packets are forwarded to different services through different flows, and inner and outer VLAN mapping is implemented.

Prerequisite

- Connect interfaces and configure interface physical parameters to make the physical status Up.
- Create VLANs.

3.3.3 Default configurations of QinQ

Default configurations of QinQ are as below.

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

3.3.4 Configuring basic QinQ

Configure basic QinQ on the ingress interface for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#ml s doubl e-taggi ng tpi d tpi d</code>	(Optional) configure TPID.
3	<code>NAG(confi g)#I nterface port port-id</code>	Enter physical layer interface configuration mode.
4	<code>NAG(confi g-port)#swi tchport qi nq dot1q-tunnel</code>	Enable basic QinQ on ingress the interface.



Caution

When you configure basic QinQ, use the **mls qos cos-remark enable** command to enable CoS Remark will change inner and outer layer priorities of the packet. Thus, we do not recommend concurrently configuring basic QinQ and CoS Remark.

3.3.5 Configuring selective QinQ

Configure selective QinQ on the ingress interface for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#ml s doubl e-taggi ng tpi d tpi d</code>	(Optional) configure TPID.
3	<code>NAG(confi g)#I nterface port port-id</code>	Enter physical layer interface configuration mode.
4	<code>NAG(confi g-port)#swi tchport vl an-mappi ng cvl an vlan-list add-outer vlan-id</code>	Configure selective QinQ rules on the interface.



Caution

In selective QinQ, when the global TPID is 8100, you have to use the **mls qos cos-remark enable** command to enable CoS Remark if you do not wish to change priority of packets.

3.3.6 Configuring egress interface toTrunk mode

Configure the egress interface toTrunk mode for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)# swi tchport mode trunk	Configure interface trunk mode, permit double Tag packet to pass.
4	NAG(confi g-port)# swi tchport trunk al lowed vl an { { all <i>vlan-list</i> } [confi rm] { add remove } <i>vlan-list</i> }	(Optional) configure VLANs allowed to pass by the Trunk interface.

3.3.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG# show swi tchport qi nq	Show configurations of basic QinQ.
2	NAG# show i nterface port <i>port-id</i> vl an-mappi ng add-outer	Show configurations of selective QinQ.

3.3.8 Example for configuring basic QinQ

Networking requirements

As shown in Figure 3-4, Switch A and Switch B are connected to VLAN 100 and VLAN 200 respectively. Department C and department E need to communicate through the carrier network. Department D and Department F need to communicate, too. Thus, you need to set the outer Tag to VLAN 1000. Set Port 2 and Port 3 to dot1q-tunnel mode on Switch A and Switch B, and connect these two interfaces two different VLANs. Port 1 is the uplink interface connected to the ISP, and it is set to the Trunk mode to allow double Tag packets to pass. The carrier TPID is 9100.

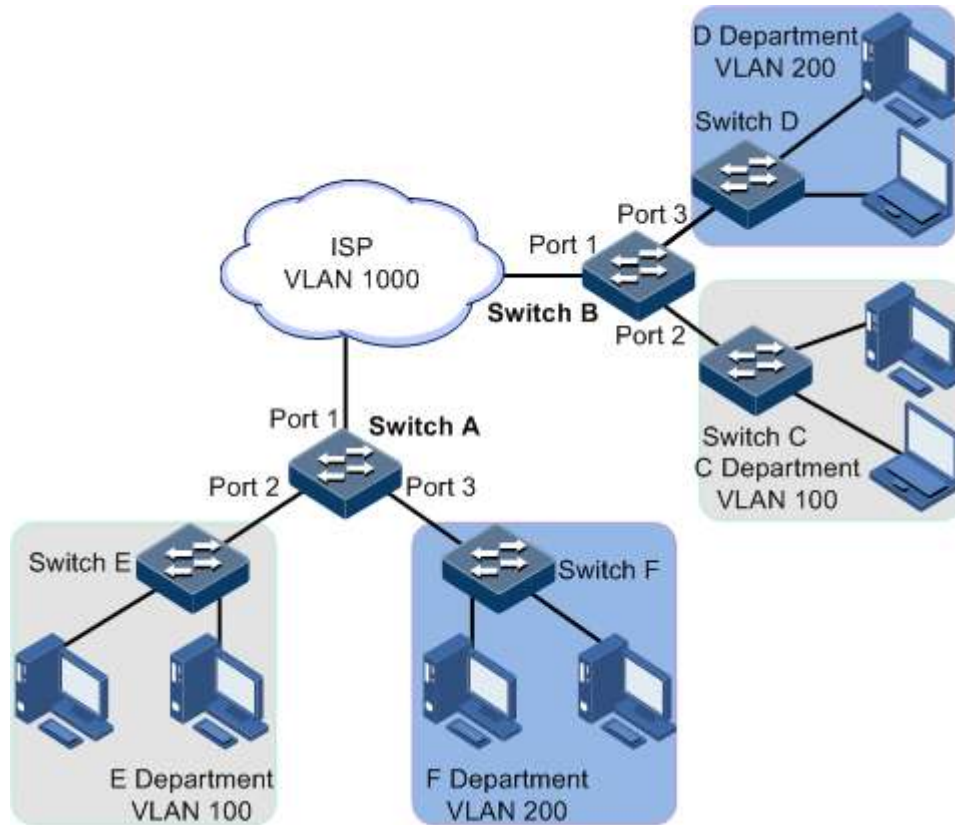


Figure 3-4 Basic QinQ networking

Configuration steps

Step 1 Create VLAN 100, VLAN 200, and VLAN 1000, and activate them. TPID is 9100.

Configure Switch A.

```
NAG#hostname SwitchA
SwitchA#config
SwitchA(config)#mls double-tagging tpid 9100
SwitchA(config)#create vlan 100,200,1000 active
```

Configure Switch B.

```
NAG#hostname SwitchB
SwitchB#config
SwitchB(config)#mls double-tagging tpid 9100
SwitchB(config)#create vlan 100,200,1000 active
```

Step 2 Set Port 2 and Port 3 to dot1q mode.

Configure Switch A.

```
Swi tchA(confi g)#I nterface port 2
Swi tchA(confi g-port)#swi tchport mode trunk
Swi tchA(confi g-port)#swi tchport trunk nati ve vl an 1000
Swi tchA(confi g-port)#swi tchport qi nq dot1q-tunnel
Swi tchA(confi g-port)#exi t
Swi tchA(confi g)#I nterface port 3
Swi tchA(confi g-port)#swi tchport mode trunk
Swi tchA(confi g-port)#swi tchport trunk nati ve vl an 1000
Swi tchA(confi g-port)#swi tchport qi nq dot1q-tunnel
Swi tchA(confi g-port)#exi t
```

Configure Switch B.

```
Swi tchB(confi g)#I nterface port 2
Swi tchB(confi g-port)#swi tchport mode trunk
Swi tchB(confi g-port)#swi tchport trunk nati ve vl an 1000
Swi tchB(confi g-port)#swi tchport qi nq dot1q-tunnel
Swi tchB(confi g-port)#exi t
Swi tchB(confi g)#I nterface port 3
Swi tchB(confi g-port)#swi tchport mode trunk
Swi tchB(confi g-port)#swi tchport trunk nati ve vl an 1000
Swi tchB(confi g-port)#swi tchport qi nq dot1q-tunnel
Swi tchB(confi g-port)#exi t
```

Step 3 **Set Port 1 to allow double Tag packets to pass.**

Configure Switch A.

```
Swi tchA(confi g)#I nterface port 1
Swi tchA(confi g-port)#swi tchport mode trunk
Swi tchA(confi g-port)#swi tchport trunk al l owed vl an 1000 confi rm
```

Configure Switch B.

```
Swi tchB(confi g)#I nterface port 1
Swi tchB(confi g-port)#swi tchport mode trunk
Swi tchB(confi g-port)#swi tchport trunk al l owed vl an 1000 confi rm
```

Checking results

Use the **show switchport qinq** command to show QinQ configurations.

Take Switch A for example.

```
Swi tchA#show swi tchport qi nq
```

```

Outer TPID: 0x9100
Interface      QinQ Status
-----
port1         --
port2         Dot1q-tunnel
port3         Dot1q-tunnel
port4         --
.....

```

3.3.9 Example for configuring selective QinQ

Networking requirements

As shown in Figure 3-5, the carrier network contains common PC Internet access service and IP phone service. PC Internet access service is assigned to VLAN 1000, and IP phone service is assigned to VLAN 2000.

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

- Add outer Tag VLAN 1000 to VLANs 100–150 assigned to PC Internet access service.
- Add outer Tag 2000 to VLANs 300–400 for IP phone service.
- The carrier TPID is 9100.

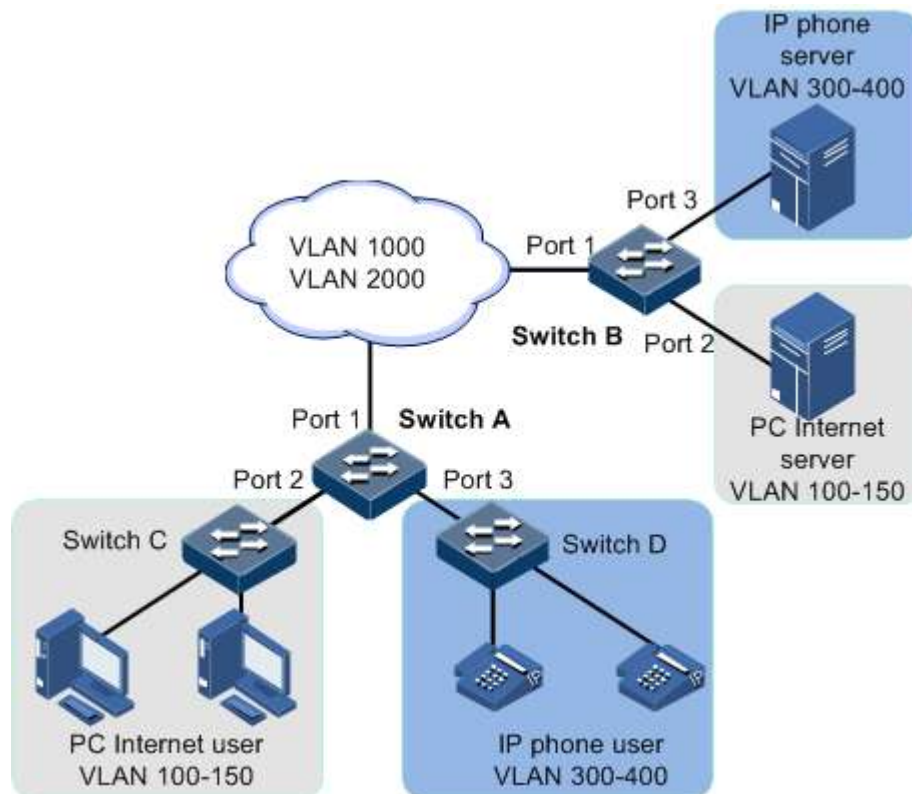


Figure 3-5 Selective QinQ networking

Configuration steps

Step 1 **Create and activate VLAN 100, VLAN 200, and VLAN 1000. The TPID is 9100.**

Configure Switch A.

```
NAG#hostname SwitcA
SwitcA#confi g
SwitcA(confi g)#ml s doubl e-taggi ng tpi d 9100
SwitcA(confi g)#create vl an 100-150, 300-400, 1000, 2000 acti ve
```

Configure Switch B.

```
NAG#hostname SwitcB
SwitcB#confi g
SwitcB(confi g)#ml s doubl e-taggi ng tpi d 9100
SwitcB(confi g)#create vl an 100-150, 300-400, 1000, 2000 acti ve
```

Step 2 **Set parameters of Port 2 and Port 3, and configure selective QinQ.**

Configure Switch A.

```
SwitcA(confi g)#i nterface port 2
SwitcA(confi g-port)#swi tchport mode trunk
SwitcA(confi g-port)#swi tchport vl an-mappi ng cvl an 100-150 add-outer 1000
SwitcA(confi g-port)#swi tchport trunk untagged vl an 1000, 2000 confi rm
SwitcA(confi g-port)#exi t
SwitcA(confi g)#i nterface port 3
SwitcA(confi g-port)#swi tchport mode trunk
SwitcA(confi g-port)#swi tchport vl an-mappi ng cvl an 300-400 add-outer 2000
SwitcA(confi g-port)#swi tchport trunk untagged vl an 1000, 2000 confi rm
SwitcA(confi g-port)#exi t
```

Configure Switch B.

```
SwitcB(confi g)#i nterface port 2
SwitcB(confi g-port)#swi tchport mode trunk
SwitcB(confi g-port)#swi tchport vl an-mappi ng cvl an 100-150 add-outer 1000
SwitcB(confi g-port)#swi tchport trunk untagged vl an 1000, 2000 confi rm
SwitcB(confi g-port)#exi t
SwitcB(confi g)#i nterface port 3
SwitcB(confi g-port)#swi tchport mode trunk
SwitcB(confi g-port)#swi tchport vl an-mappi ng cvl an 300-400 add-outer 2000
SwitcB(confi g-port)#swi tchport trunk untagged vl an 1000, 2000 confi rm
SwitcB(confi g-port)#exi t
```

Step 3 Enable Double-tagging on Port 1.

Configure Switch A.

```

SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 1000,2000 config

```

Configure Switch B.

```

SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk allowed vlan 1000,2000 config

```

Checking results

Use the **show interface port *port-id* vlan-mapping add-outer** command to show QinQ configurations.

Take Switch A for example.

```

SwitchA#show interface port-list 2 vlan-mapping add-outer
Based inner VLAN QinQ mapping rule:
Interface Original Inner VLAN List      Add-outer VLAN Hw Status Hw-ID
-----
port2          100-150                1000           Enable   1
SwitchA#show interface port-list 3 vlan-mapping add-outer
Based inner VLAN QinQ mapping rule:
Interface Original Inner VLAN List      Add-outer VLAN Hw Status Hw-ID
-----
port3          300-400                2000           Enable   2

```

3.4 VLAN mapping

3.4.1 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 3-6 shows the principle of VLAN mapping.

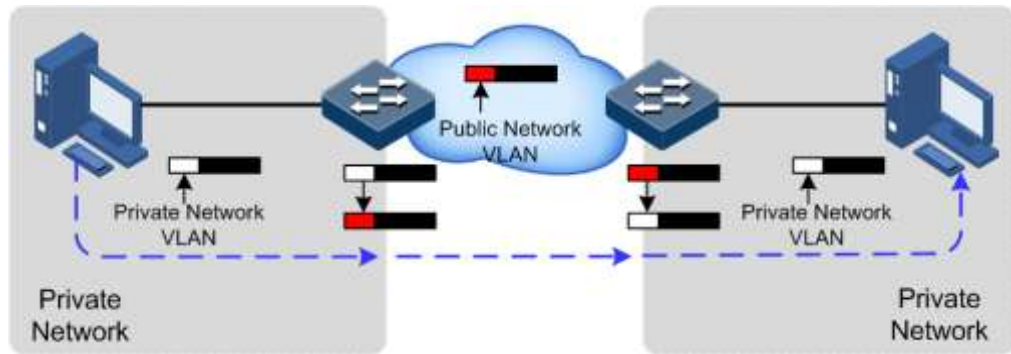


Figure 3-6 Principle of VLAN mapping

After receiving a VLAN Tag contained in a user private network packet, the SNR-S212i-8POE 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 SNR-S212i-8POE replaces the VLAN Tag carried by a packet from a specified VLAN to the new VLAN Tag.

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

The SNR-S212i-8POE supports up to 680 ingress VLAN mapping rules.

3.4.2 Preparing for configurations

Scenario

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

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

Prerequisite

- Connect the interface and configure its physical parameters to make it Up at the physical layer.
- Create VLANs.

3.4.3 Default configurations of VLAN mapping

Default configurations of VLAN mapping are as below.

Function	Default value
VLAN mapping status	Disable

3.4.4 Configuring 1:1 VLAN mapping

Configure 1:1 VLAN mapping for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#I nterface port port-i d</code>	Enter physical layer interface configuration mode.
3	<code>NAG(confi g-port)#swi tchport vl an-mappi ng i ngress cvlan- list transl ate vlan-i d</code>	Configure interface-based 1:1 VLAN mapping rules in the ingress direction.



Caution

In selective QinQ, when the global TPID is 9100, you have to use the **mls qos cos-remark enable** command to enable CoS Remark if you do not wish to change priority of packets.

3.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>NAG#show i nterface port-l ist port-l ist vl an- mappi ng i ngress transl ate</code>	Show configurations of 1:1 VLAN mapping.

3.5 STP/RTSTP

3.5.1 Introduction

STP

With the increasing complexity of network structure and growing number of switches on the network, the Ethernet network loops become the most prominent problem. Because of the packet broadcast mechanism, a loop causes the network to generate storms, exhaust network resources, and have serious impact to forwarding normal data. The network storm caused by the loop is shown in Figure 3-7.

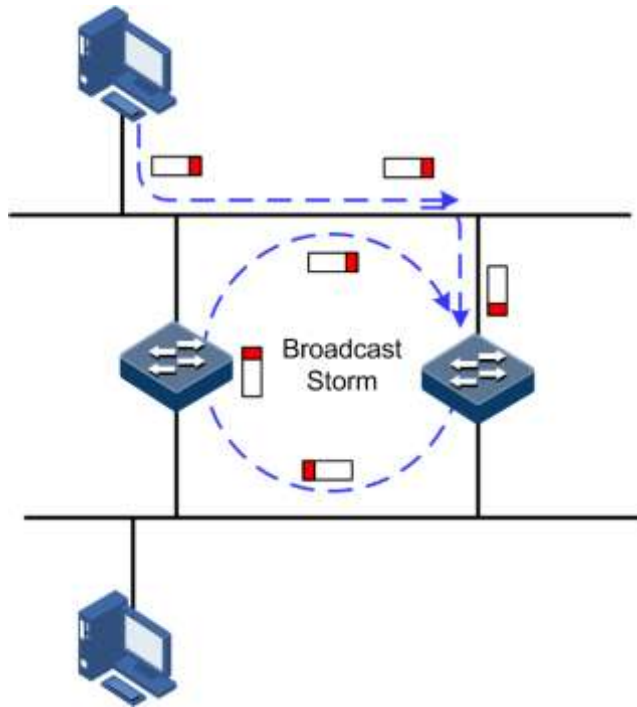


Figure 3-7 Network storm due to loopback

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

The SNR-S212i-8POE running STP can process Bridge Protocol Data Unit (BPDU) packet with each other for the election of root switch and selection of root port and designated port. It also can block loop interface on the SNR-S212i-8POE logically according to the selection results, and finally trims the loop network structure to tree network structure without loop which takes a SNR-S212i-8POE as root. This prevents the continuous proliferation and limitless circulation of packet on the loop network from causing broadcast storms and avoids declining packet processing capacity caused by receiving the same packets repeatedly.

Figure 3-8 shows loop networking running STP.

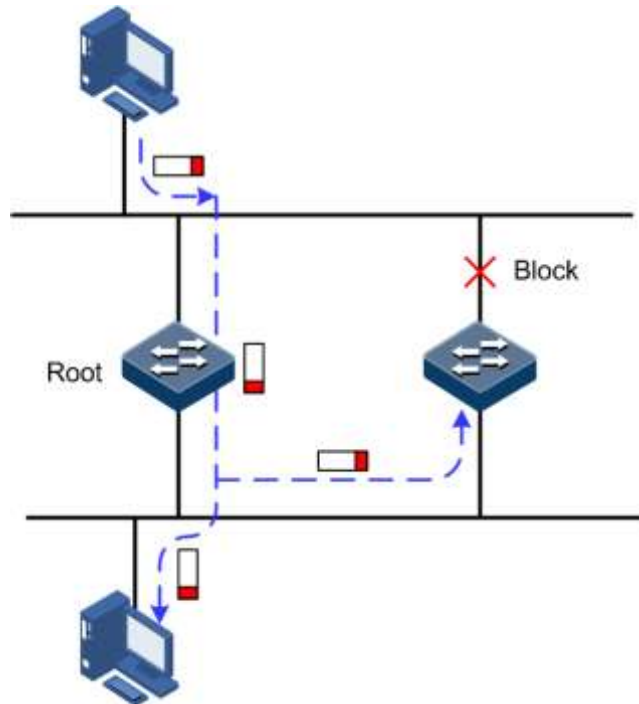


Figure 3-8 Loop networking with STP

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

The major disadvantage of STP is the slow convergence speed.

RSTP

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

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

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

- The whole switching network has only one spanning tree, which will lead to longer convergence time on a larger network.
- Waste of bandwidth since a link does not carry any flow after it is blocked.
- Packet of partial VLAN cannot be forwarded when network structure is unsymmetrical. As shown in Figure 3-9, Switch B is the root switch; RSTP blocks the link between Switch A and Switch C logically and makes that the VLAN 100 packet cannot be transmitted and Switch A and Switch C cannot communicate.

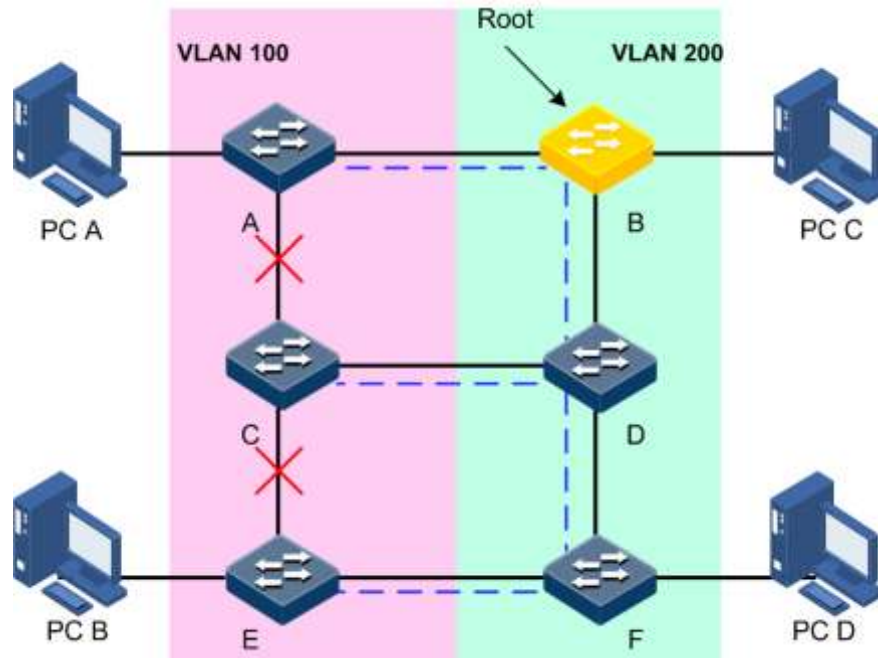


Figure 3-9 VLAN packet forward failure due to RSTP

3.5.2 Preparing for configurations

Scenario

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

Prerequisite

N/A

3.5.3 Default configurations of STP

Default configurations of STP are as below.

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

Function	Default value
Hello Time timer	2s
Forward Delay timer	15s

3.5.4 Enabling STP

Configure STP for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# spanni ng-tree enabl e	Enable STP.
3	NAG(confi g)# spanni ng-tree mode { stp rstp }	Configure spanning tree mode.
4	NAG(confi g)# i nterface <i>port port-id</i>	Enter physical layer interface configuration mode.
5	NAG(confi g-port)# spanni ng-tree enabl e	Enable interface STP.

3.5.5 Configuring STP parameters

Configure STP parameters for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# spanni ng-tree pri ori ty <i>pri ori ty-val ue</i>	(Optional) configure device priorities.
3	NAG(confi g)# spanni ng-tree root { pri mary secondary }	(Optional) configure the SNR-S212i-8POE as the root or backup device.
4	NAG(confi g)# i nterface <i>port port-id</i> NAG(confi g-port)# spanni ng-tree pri ori ty <i>pri ori ty-val ue</i>	(Optional) configure interface priorities on the SNR-S212i-8POE.
5	NAG(confi g-port)# spanni ng-tree i nter-path-cost <i>cost-val ue</i> NAG(confi g-port)# exl t	(Optional) configure path cost of interfaces on the SNR-S212i-8POE.
6	NAG(confi g)# spanni ng-tree hel lo-ti me <i>val ue</i>	(Optional) configure the value of Hello Time.
7	NAG(confi g)# spanni ng-tree transi t-l i mi t <i>val ue</i>	(Optional) configure the maximum transmission rate on the interface.
8	NAG(confi g)# spanni ng-tree forward-del ay <i>val ue</i>	(Optional) configure forward delay.

Step	Command	Description
9	NAG(config)#spanning-tree max-age <i>value</i>	(Optional) configure the maximum age.

3.5.6 Checking configurations

Use the following commands to check configuration results.

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

3.5.7 Example for configuring STP

Networking requirements

As shown in Figure 3-10, Switch A, Switch B, and Switch C forms a ring network, so the loopback must be eliminated in the situation of a physical ring. Enable STP on them, set the priority of Switch A to 0, and path cost from Switch B to Switch A to 10.

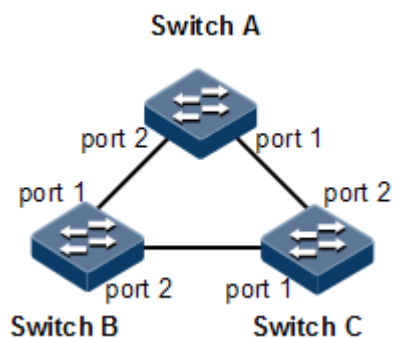


Figure 3-10 STP networking

Configuration steps

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

Configure Switch A.

```

NAG#hostname Swit chA
Swit chA#confi g
Swit chA(config)#spanni ng-tree enabl e
Swit chA(config)#spanni ng-tree mode stp
  
```

Configure Switch B.

```
NAG#hostname Swi tchB
Swi tchB#confi g
Swi tchB(confi g)#spanni ng-tree enabl e
Swi tchB(confi g)#spanni ng-tree mode stp
```

Configure Switch C.

```
NAG#hostname Swi tchC
Swi tchC#confi g
Swi tchC(confi g)#spanni ng-tree enabl e
Swi tchC(confi g)#spanni ng-tree mode stp
```

Step 2 Configure interface modes on three switches.**Configure Switch A.**

```
Swi tchA(confi g)#I nterface port 1
Swi tchA(confi g-port)#swi tchport mode trunk
Swi tchA(confi g-port)#exi t
Swi tchA(confi g)#I nterface port 2
Swi tchA(confi g-port)#swi tchport mode trunk
Swi tchA(confi g-port)#exi t
```

Configure Switch B.

```
Swi tchB(confi g)#I nterface port 1
Swi tchB(confi g-port)#swi tchport mode trunk
Swi tchB(confi g-port)#exi t
Swi tchB(confi g)#I nterface port 2
Swi tchB(confi g-port)#swi tchport mode trunk
Swi tchB(confi g-port)#exi t
```

Configure Switch C.

```
Swi tchC(confi g)#I nterface port 1
Swi tchC(confi g-port)#swi tchport mode trunk
Swi tchC(confi g-port)#exi t
Swi tchC(confi g)#I nterface port 2
Swi tchC(confi g-port)#swi tchport mode trunk
Swi tchC(confi g-port)#exi t
```

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

Configure Switch A.

```
Swi tchA(confi g)#spanni ng-tree pri ori ty 0
Swi tchA(confi g)#I nterface port 2
Swi tchA(confi g-port)#spanni ng-tree extern-path-cost 10
```

Configure Switch B.

```
Swi tchB(confi g)#I nterface port 1
Swi tchB(confi g-port)#spanni ng-tree extern-path-cost 10
```

Checking results

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

Take Switch A for example.

```
Swi tchA#show spanni ng-tree
Spanni ng-tree admi n state: enable
Spanni ng-tree protocol mode: STP
Bridgel d: Mac 000E.5E00.1234 Pri ori ty 0
Root: Mac 000E.5E00.1234 Pri ori ty 0 RootCost 0
Operati onal: Hel loTi me 2 ForwardDel ay 15 MaxAge 20
Confi gured: Hel loTi me 2 ForwardDel ay 15 MaxAge 20 Transmi tLi mi t 3
MaxHops 20 Di ameter 7
```

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

Take Switch A for example.

```
Swi tchA#show spanni ng-tree port-l i st 1, 2
port1
PortEnabl e: admi n: enable oper: enable
Rootguard: di sabl e
Loopguard: di sabl e
ExternPathCost: 200000
Partner STP Mode: stp
Bpdus send: 184 (TCN<0> Confi g<184> RST<0> MST<0>)
Bpdus recei ved: 6 (TCN<2> Confi g<1> RST<0> MST<3>)
State: forwardi ng Rol e: desi gnated Pri ori ty: 128 Cost: 200000
Root: Mac 000E.5E00.1234 Pri ori ty 0 RootCost 0
Desi gnatedBri dge: Mac 000E.5E00.1234 Pri ori ty 0 Desi gnatedPort 32769

port2
```

```
PortEnable: admin: enable oper: enable
Rootguard: disable
Loopguard: disable
ExternPathCost: 200000
Partner STP Mode: stp
Bpdus send: 184 (TCN<0> Config<184> RST<0> MST<0>)
Bpdus received: 8 (TCN<3> Config<1> RST<0> MST<4>)
State: forwarding Role: designated Priority: 128 Cost: 10
Root: Mac 000E. 5E00. 1234 Priority 0 RootCost 0
DesignatedBridge: Mac 000E. 5E00. 1234 Priority 0 DesignatedPort 32770
```

3.6 MSTP

3.6.1 Introduction

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

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

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

Compared with STP and RSTP, MSTP also introduces total root (CIST Root) and domain 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 domain root is a local concept, which is relative to an instance in a domain. As shown in Figure 3-11, all connected devices only have one total root, and the number of domain root contained in each domain is associated with the number of instances.

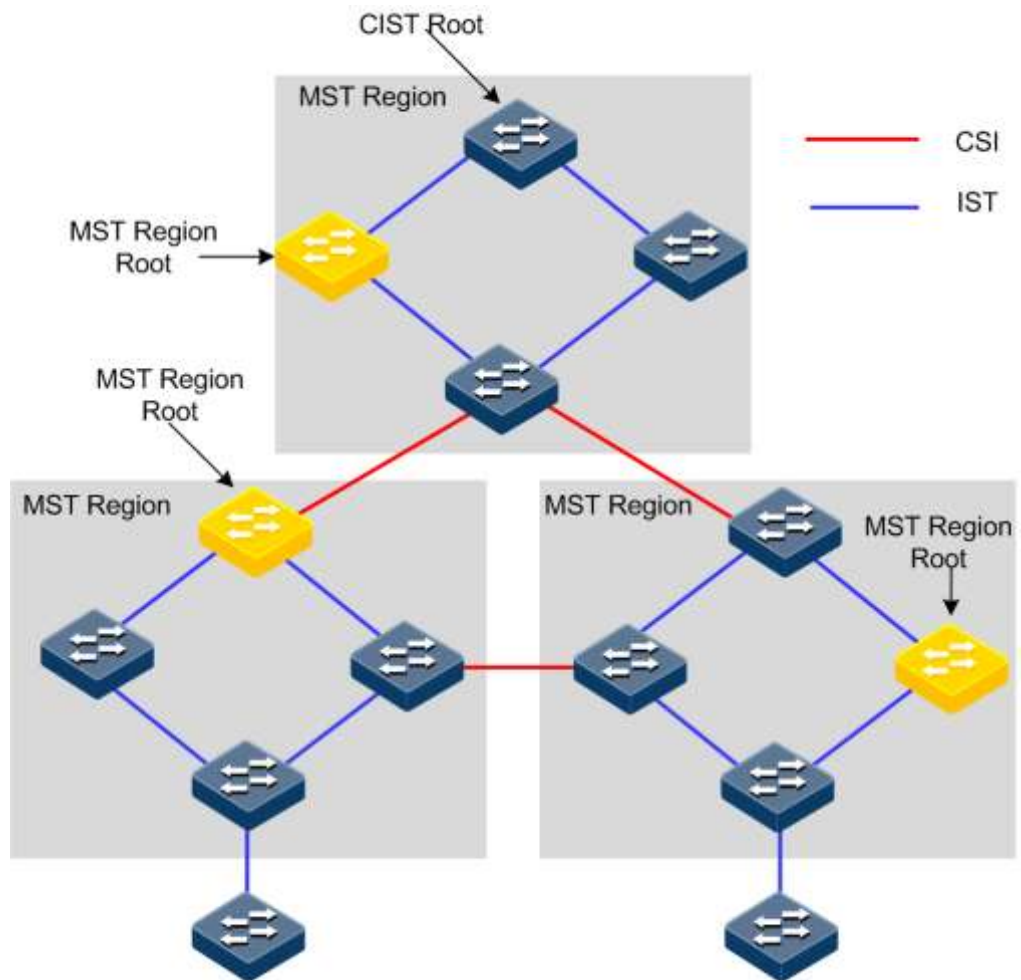


Figure 3-11 Basic concepts of MSTI network

There can be different MST instance in each MST domain, which associates VLAN and MSTI by setting VLAN mapping table (relationship table of VLAN and MSTI). The concept sketch map of MSTI is shown in Figure 3-12.

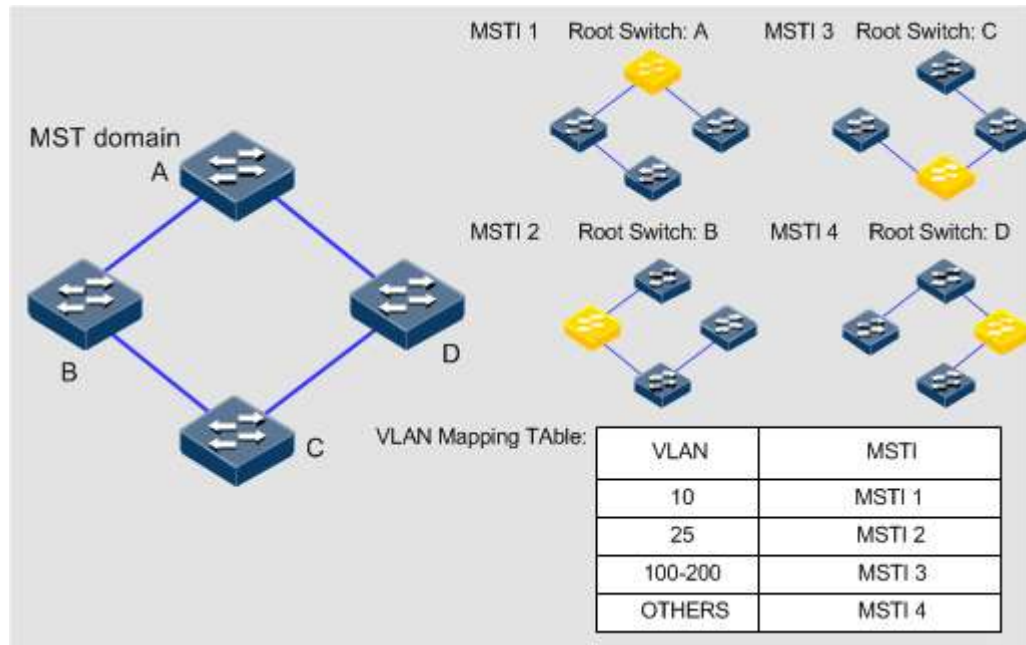


Figure 3-12 MSTI concepts



Note

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

Compared with STP and RSTP mentioned previously, MSTP has obvious advantages, including cognitive ability of VLAN, load sharing, similar RSTP interface status switching as well as 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.

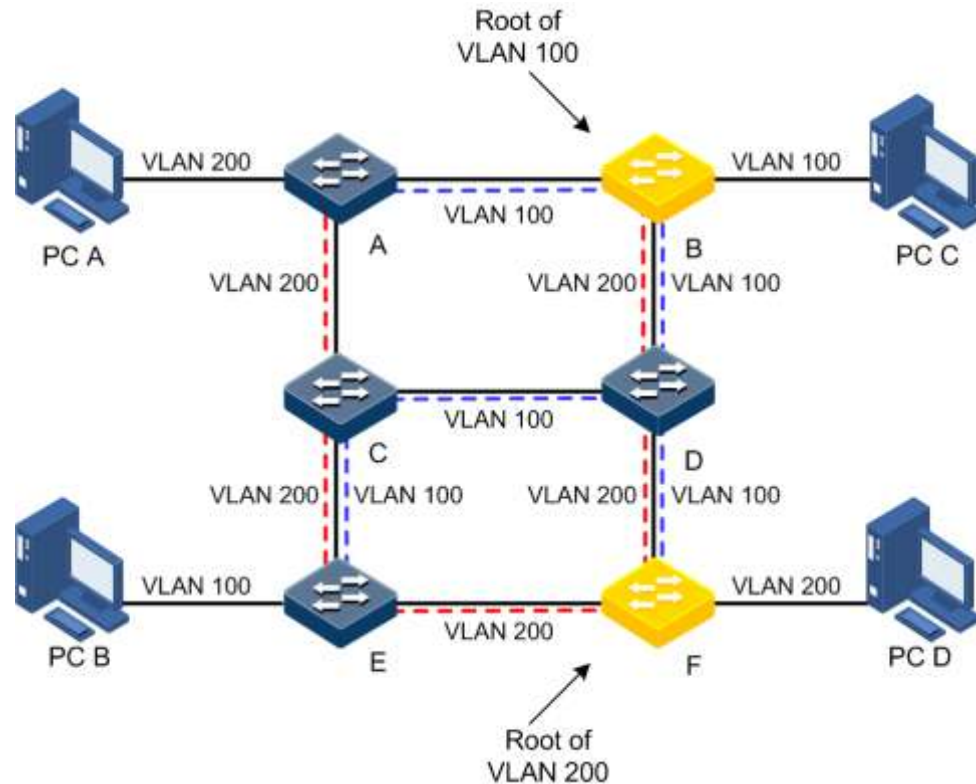


Figure 3-13 Networking of multiple spanning trees instances in MST domain

Apply MSTP to the network as shown in Figure 3-13. After calculation, there are two spanning trees generated at last (two MST instances):

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

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

3.6.2 Preparing for configurations

Scenario

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

Prerequisite

Configure interface physical parameters to make it Up before configuring MSTP.

3.6.3 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 domain	20
MSTP priority of the device	32768
MSTP priority of the interface	128
Path cost of the interface	0
Maximum number of packets sent within each Hello time	3
Max Age timer	20s
Hello Time timer	2s
Forward Delay timer	15s
Revision level of MST domain	0

3.6.4 Enabling MSTP

Enable MSTP for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# spanni ng-tree enabl e	Enable STP.
3	NAG(confi g)# i nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
4	NAG(confi g-port)# spanni ng-tree enabl e	Enable interface STP.

3.6.5 Configuring MST domain and its maximum number of hops

You can set domain information for the SNR-S212i-8POE when it is running in MSTP mode. The device MST domain is decided by domain name, VLAN mapping table and configuration of MSTP revision level. You can set current device in a specific MST domain through following configuration.

MST domain scale is restricted by the maximum number of hops. Starting from the root bridge of spanning tree in the domain, the configuration message (BPDU) reduces 1 hop count once it is forwarded passing a device; the SNR-S212i-8POE discards the configuration message whose number of hops is 0. The device exceeding the maximum number of hops cannot join spanning tree calculation and then restrict MST domain scale.

Configure MSTP domain and its maximum number of hops for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#spanni ng-tree regi on-confi gurati on	Enter MST domain configuration mode.
3	NAG(confi g-regi on)#name <i>name</i>	Configure MST domain name.
4	NAG(confi g-regi on)#revi sl on- level <i>level -val ue</i>	Set revision level for MST domain.
5	NAG(confi g-regi on)#l nstance <i>instance-id</i> vl an <i>vlan-list</i> NAG(confi g-regi on)#exl t	Set mapping relationship from MST domain VLAN to instance.
6	NAG(confi g)#spanni ng-tree max- hops <i>hops-val ue</i>	Configure the maximum number of hops for MST domain.



Note

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

3.6.6 Configuring root bridge/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 of the root bridge of related instance. In this case, if a new root bridge is assigned, the backup bridge will not become the root bridge. If several backup bridges for a spanning tree are configured, once the root bridge stops working, MSTP will choose the backup root with the smallest MAC address as the new root bridge.



Note

We recommend not 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 root bridge or backup bridge for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#spanni ng-tree [i nstance <i>instance-id</i>] root { pri mary secon dary }	Set the SNR-S212i-8POE 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; namely, they cannot only be the root bridge or backup bridge of one instance, but also the root bridge or backup bridge of other spanning tree instances. However, in a spanning tree instance, a device cannot be used as the root bridge and backup bridge concurrently.
- You cannot assign two or more root bridges for one spanning tree instance, but can assign several backup bridges for one spanning tree. Generally, you had better assign one root bridge and several backup bridges for a spanning tree.

3.6.7 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 decides whether the SNR-S212i-8POE can be selected as the root of the spanning tree. Configuring smaller priority helps obtain smaller Bridge ID and designate the SNR-S212i-8POE as the root. If priorities of two SNR-S212i-8POE devices are identical, the SNR-S212i-8POE with smaller 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 interface priority and system priority for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)# spanni ng-tree [i nstance <i>instance-id</i>] p ri ori ty <i>p ri ori ty-val ue</i> NAG(confi g-port)# exi t	Set interface priority for a STP instance.
4	NAG(confi g)# spanni ng-tree [i nstance <i>instance-id</i>] p ri ori ty <i>p ri ori ty-val ue</i>	Set system priority for a STP instance.



Note

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

3.6.8 Configuring network diameter for switching 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 domain, it is considered as just one node. Actually, network diameter should be defined as the domain number in the path crossing the most domains. The network diameter is 1 if there is only one domain in the whole network.

The maximum number of hops of MST domain is used to measure the domain scale, while the 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 domain, only when the SNR-S212i-8POE is configured as the CIST root device can this configuration take effect. MSTP will automatically set 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	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#spanni ng-tree bri dge-di ameter <i>bri dge-di ameter-val ue</i>	Configure the network diameter for the switching network.

3.6.9 Configuring inner path cost for interface

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

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

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

Configure the inner path cost for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#i nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)#spanni ng-tree [i nstance <i>instance-id</i>] i nter-path-cost <i>cost-val ue</i>	Configure the inner path cost on the interface.

3.6.10 Configuring external path cost on interface

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

Configure the external path cost for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i nterface port <i>port-i d</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)# spanni ng-tree extern-path-cost <i>cost-val ue</i>	Configure the external path cost on interface.

3.6.11 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 maximum transmission rate on the interface for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# spanni ng-tree transi t-l i mi t <i>val ue</i>	Configure the maximum transmission rate on the interface.

3.6.12 Configuring MSTP timer

- **Hello Time:** the SNR-S212i-8POE sends the interval of bridge configuration information (BPDU) regularly to check whether there is failure in detection link of the SNR-S212i-8POE. The SNR-S212i-8POE sends hello packets to other devices around in 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 condition. 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; namely, 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 SNR-S212i-8POE 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 over greater age value will make STP not adapt to network topology change timely.

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

Configure the MSTP timer for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#spanni ng-tree hel lo- time <i>val ue</i>	Set Hello Time.
3	NAG(confi g)#spanni ng-tree forward-del ay <i>val ue</i>	Set Forward Delay.
4	NAG(confi g)#spanni ng-tree max- age <i>val ue</i>	Set Max Age.

3.6.13 Configuring edge interface

Configure the edge interface for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#I nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)#spanni ng-tree edged-port { auto force-true force-fal se }	Configure attributes of the RSTP edge interface.

3.6.14 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 SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#spanni ng-tree edged-port bpdu-fi lter enable port-l ist <i>port-list</i>	Enable BPDU filtering on the edge interface.

3.6.15 Configuring BPDU Guard

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

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

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

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

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#spanni ng-tree bpduguard enable	Enable BPDU Guard.
3	NAG(confi g)#i nterface port port-i d	Enter physical layer interface configuration mode.
4	NAG(confi g-port)#no spanni ng- tree bpduguard shutdown port	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 packet.

3.6.16 Configuring STP/RSTP/MSTP mode switching

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

- STP compatible mode: the SNR-S212i-8POE does not implement fast switching from the replacement interface to the root interface and fast 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 SNR-S212i-8POE implements fast switching from the replacement interface to the root interface and fast 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 SNR-S212i-8POE 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 domain.

Configure the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#spanni ng-tree mode { stp rstp mstp }	Configure spanning tree mode.

3.6.17 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 configure this item in auto status and the system will automatically detect whether the interface is connected to a point-to-point link.

Configure link type for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#I nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)#spanni ng-tree l i nk-type { auto poi nt-to-poi nt shared }	Configure link type for interface.

3.6.18 Configuring root interface protection

The network will select a bridge again when it receives a packet with higher priority, which influences network connectivity and also consumes CPU resource. For the MSTP network, if someone sends BPDU packets with higher priority, the network may become unstable for the continuous election. Generally, priority of each bridge has already been configured in network planning phase. The nearer a bridge is to the edge, the lower the bridge priority is. So the downlink interface cannot receive the packets higher than bridge priority unless under someone attacks. For these interfaces, you can enable rootguard to refuse to process packets with priority higher than bridge priority and block the interface for a period to prevent other attacks from attacking sources and damaging the upper layer link.

Configure root interface protection for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#I nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)#spanni ng-tree rootguard enabl e	Enable root interface protection.

3.6.19 Configuring interface loopguard

The spanning tree has two functions: loopguard and link backup. Loopguard requires carving up the network topology into tree structure. There must be redundant 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, and the link has failed if it has not received packet in a period. Then select a new link and enable backup interface. In actual networking, the cause to failure in receiving packets may not link fault. In this case, enabling the backup interface may lead to loop.

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



Note

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

Configure interface loop protection for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#I nterface port <i>port-id</i></code>	Enter physical layer interface configuration mode.
3	<code>NAG(confi g-port)#spanni ng-tree l oopguard enabl e</code>	Enablere interface loopguard.

3.6.20 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>NAG#show spanni ng-tree [i nstance <i>instance-id</i>] [detai l]</code>	Show basic configurations of STP.
2	<code>NAG#show spanni ng-tree [i nstance <i>instance-id</i>] port-l ist <i>port-list</i> [detai l]</code>	Show configurations of spanning tree on the interface.
3	<code>NAG#show spanni ng-tree regi on- operati on</code>	Show operation information about the MST domain.
4	<code>NAG(confi g-regi on)#show spanni ng- tree regi on-confi gurati on</code>	Show configurations of MST domain.

3.6.21 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	NAG(config-port)#spanning-tree clear statistics	Clear statistics of spanning tree on the interface.

3.6.22 Example for configuring MSTP

Networking requirements

As shown in Figure 3-14, three SNR-S212i-8POE devices are connected to form a ring network through MSTP, with the domain 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 related to VLAN 3. Instant 4 is related to 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 loopback and implements load sharing.

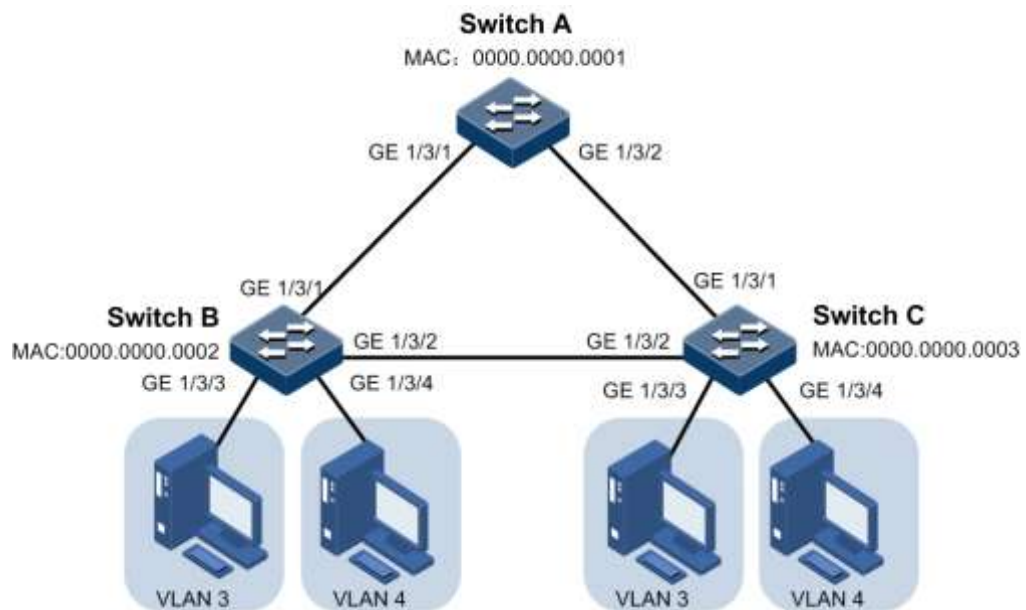


Figure 3-14 MSTP networking

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.

```
NAG#hostname Swi tchA
Swi tchA#confi g
Swi tchA(confi g)#create vl an 3-4 acti ve
```

Configure Switch B.

```
NAG#hostname Swi tchB
Swi tchB#confi g
Swi tchB(confi g)#create vl an 3-4 acti ve
```

Configure Switch C.

```
NAG#hostname Swi tchC
Swi tchC#confi g
Swi tchC(confi g)#create vl an 3-4 acti ve
```

- Step 2 Configure Port 1 and Port 2 on Switch A to allow all VLAN packets to pass in Trunk mode. Configure Port 1 and Port 2 on Switch B to allow all VLAN packets to pass in Trunk mode. Configure Port 1 and Port 2 on Switch C to allow all VLAN packets to pass in Trunk mode. Configure Port 3 and Ggaethernet 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.

```
Swi tchA(confi g)#i nterface port 1
Swi tchA(confi g-port)#swi tchport mode trunk
Swi tchA(confi g-port)#exi t
Swi tchA(confi g)#i nterface port 2
Swi tchA(confi g-port)#swi tchport mode trunk
Swi tchA(confi g-port)#exi t
```

Configure Switch B.

```
Swi tchB(confi g)#i nterface port 1
Swi tchB(confi g-port)#swi tchport mode trunk
Swi tchB(confi g-port)#exi t
Swi tchB(confi g)#i nterface port 2
Swi tchB(confi g-port)#swi tchport mode trunk
Swi tchB(confi g-port)#exi t
Swi tchB(confi g)#i nterface port 3
Swi tchB(confi g-port)#swi tchport access vl an 3
Swi tchB(confi g-port)#exi t
Swi tchB(confi g)#i nterface port 4
Swi tchB(confi g-port)#swi tchport access vl an 4
Swi tchB(confi g-port)#exi t
```

Configure Switch C.

```
Swi tchC(confi g)#i nterface port 1
```

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

- Step 3 Set spanning tree mode of Switch A, Switch B, and Switch C to MSTP, and enable STP. Enter MSTP configuration mode, and set the domain name to **aaa**, revised version to 0. Map instance 3 to VLAN 3, and instance 4 to VLAN 4. Exit from MST configuration mode.

Configure Switch A.

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

Configure Switch B.

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

Configure Switch C.

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

Step 4 Set the inner path cost of Port 1 of spanning tree instance 3 to 500000 on Switch B.

```
SwitchB(config)#interface port 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 domain.

Take Switch A for example.

```
SwitchA#show spanning-tree region-operation
Operational Information:
-----
Name: aaa
Revision Level: 0
Instances running: 3
Digest: 0X024E1CF7E14D5DBBD9F8E059D2C683AA
Instance  Vlan  Mapped
-----
0          1-2, 5-4094
3          3
4          4
Operational Information:
-----
Name:
Revision Level: 0
Instances running: 1
Digest: 0XAC36177F50283CD4B83821D8AB26DE62
Instance  Vlan  Mapped
-----
0          1-4094
```

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

- Switch A:

```
SwitchA#show spanning-tree instance 3
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 3
-----
BridgeId:      Mac 0000.0000.0001 Priority 32768
Regional Root: Mac 0000.0000.0001 Priority 32768 InternalRootCost 0
PortId PortState PortRole PathCost PortPriority LinkType
-----
port1   forwarding  root      200000 128      point-to-point
```

```
port2      forwarding designated 200000 128      poi nt-to-poi nt
```

- **Switch B:**

```
Swi tchB#show spanni ng-tree i nstance 3
```

```
Spanni ng-tree admi n state: enable
```

```
Spanni ng-tree protocol mode: MSTP
```

```
MST I D: 3
```

```
-----
Bridg eId:   Mac 0000.0000.0002 Pri ori ty 32768
```

```
Regi onal Root: Mac 0000.0000.0001 Pri ori ty 32768   Internal RootCost 0
```

```
PortId PortState PortRole PathCost PortPri ori ty Li nkType
```

```
-----
port1      forwarding designated 500000 128      poi nt-to-poi nt
```

```
port2      forwarding root      200000 128      poi nt-to-poi nt
```

- **Switch C:**

```
Swi tchC#show spanni ng-tree i nstance 3
```

```
Spanni ng-tree admi n state: enable
```

```
Spanni ng-tree protocol mode: MSTP
```

```
MST I D: 3
```

```
-----
Bridg eId:   Mac 0000.0000.0003 Pri ori ty 32768
```

```
Regi onal Root: Mac 0000.0000.0001 Pri ori ty 32768   Internal RootCost 200000
```

```
PortId PortState PortRole PathCost PortPri ori ty Li nkType
```

```
-----
port1      di scardi ng al ternate 200000 128      poi nt-to-poi nt
```

```
port2      forwardi ng root      200000 128      poi nt-to-poi nt
```

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

Take Switch A for example.

```
Swi tchA#show spanni ng-tree i nstance 4
```

```
Spanni ng-tree admi n state: enable
```

```
Spanni ng-tree protocol mode: MSTP
```

```
MST I D: 4
```

```
-----
Bridg eId:   Mac 000E.5E00.0000 Pri ori ty 32768
```

```
Regi onal Root: Mac 000E.5E00.0000 Pri ori ty 32768   Internal RootCost 0
```

```
Port   PortState PortRole PathCost PortPri ori ty Li nkType
```

```
-----
port1      forwardi ng root      200000 128      poi nt-to-poi nt
```

```
port2      forwardi ng desi gnated 200000 128      poi nt-to-poi nt
```


3.7 GARP

3.7.1 Introduction

Generic Attribute Registration Protocol (GARP) provides a mechanism to help GARP members in the same LAN to distribute, broadcast, and register information (such as VLAN and multicast information).

GARP is not an entity on a device. Those applications complying with GARP are called GARP applications. GARP VLAN Registration Protocol (GVRP) is a GARP application. When a GARP application entity is connected to an interface of a device, the interface is mapped into the GARP application entity.

Packets of the GARP application entity use a specific multicast MAC address as its destination MAC address. When receiving packets of the GARP application entity, a device distinguishes them by destination MAC address and transmits them to different GARP applications (such as GAVP) for processing.

GARP messages

GARP members exchange information by transmitting messages, including the following three types of messages:

- Join message: a GARP application entity sends out a Join message when:
 - It needs another device to register its attributes (such as VLAN information).
 - It receives a Join message from other entities; or it has been statically configured with some parameters, and needs another GARP application entity to register.
- Leave message: a GARP application entity sends out a Leave message when:
 - It needs another device to register its attributes.
 - It receives a Join message from other entities to deregister its attributes or it statically deregisters its attributes.
- LeaveAll message: when the GARP application entity is started, the LeaveAll timer starts. It sends a LeaveAll message when this timer expires. The LeaveAll message is used to deregister all attributes so that other GARP application entities can register all attributes of the GARP application entity. When the GARP application entity receives a LeaveAll message from the peer, its LeaveAll time is restored and then starts.
- The Leave message or LeaveAll message cooperates with the Join message to deregister or reregister attributes. Through message exchange, all attributes to be registered can be transmitted to all GARP entities in the same LAN.

GARP timer

The interval for sending the GARP message is configured by timers. GARP defines three timers to control the interval.

- Join timer: if no message is replied to the first Join message sent by the GARP application entity, this entity will send another Join message to ensure secure transmission. The interval between sending these two messages is controlled by the Join timer. If the entity has received reply from other GARP application entities, it will not send the Join message.
- Leave timer: when a GARP application entity needs to deregister an attribute, it sends a Leave message to another GARP application entity which will later start a Leave timer.

It deregisters the attribute if failing to receive the Join message to deregister the attribute before the Leave timer expires.

- LeaveAll timer: when a GARP application entity starts, its LeaveAll timer starts as well. When the LeaveAll timer expires, the GARP application entity sends a LeaveAll message so that other GARP application entities can register all attributes of the GARP application entity. Then, the LeaveAll time is restored and starts again for new timing.

GVRP

GARP VLAN Registration Protocol (GVRP) is a GARP application. Based on GARP working mechanism, it maintains VLAN dynamic registration information of the switch, and sends the information to other switches.

All GVRP-supportive switches can receive VLAN registration information from other switches, and dynamically update local VLAN registration information. In addition, all GVRP-supportive switches can send local VLAN registration information to other switches so that they have consistent VLAN registration information in the same VLAN. VLAN registration information sent by GVRP includes local manually configured static registration information and dynamic registration information from other switches.

GVRP has three registration modes:

- Normal: in this mode, GVRP allows dynamic registration and deregistration of VLANs, and sends dynamic and static VLAN information.
- Fixed: in this mode, GVRP forbids dynamic registration and deregistration of VLANs, and sends static rather than dynamic VLAN information.
- Forbidden: in this mode, GVRP forbids dynamic registration and deregistration of VLANs, forbids creating static VLANs on the interface, deletes all VLANs except VLAN 1, allows packets of the default VLAN (VLAN 1) to pass, and transmits packets of the default VLAN to other GARP members.

As shown in Figure 3-15, to configure VLAN on multiple devices on a network and allow packets of the specified VLAN to pass are complex. By using GVRP to dynamically register and transmit the specified VLAN, the network administrator can improve working efficiency and accuracy.

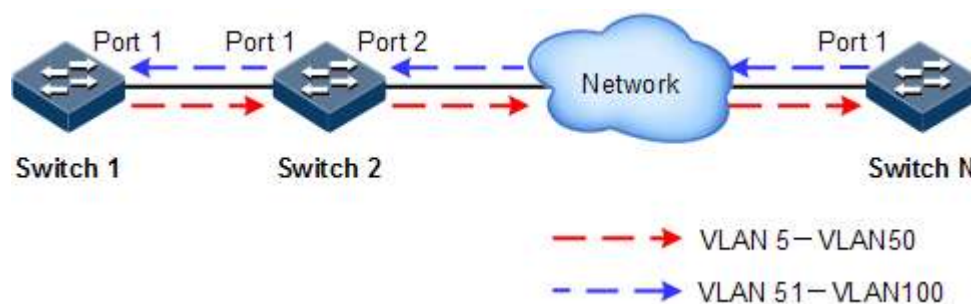


Figure 3-15 GVRP working principle

As shown in Figure 3-15, Port 1 on Switch 1, Port 1 and Port 2 on Switch 2, and Port 1 on Switch N are Trunk interfaces. Create VLANs 5-50 on Switch 1, and then these VLANs will be dynamically registered on the Rx interface along the red direction until Switch N is registered. Create VLANs 51-100 on Switch N, and then these VLANs will be dynamically registered on the Rx interface along the blue direction so that each switch can completely process packets of VLANs 5-100.

GMRP

GARP Multicast Registration Protocol (GMRP) is used to maintain dynamic multicast registration information on the switch. All GMRP-supportive switches can receive multicast registration information from other switches, and dynamically update local multicast registration information. In addition, all GVRP-supportive switches can send local multicast registration information to other switches so that they have consistent multicast registration information in the same VLAN.

When a host needs to join a multicast group, it sends a GMRP Join message. The switch adds the interface that receives the GMRP Join message to the multicast group and sends the GMRP Join message to the multicast VLAN so that multicast sources in the VLAN can sense existence of multicast members. When a multicast source sends multicast packets to the multicast group, the switch forwards these multicast packets to the interface connected to the multicast group members. Multicast registration information sent by GMRP includes local manually configured static multicast registration information and dynamic multicast registration information from other switches.

GMRP has three registration modes:

- **Normal:** in this mode, GMRP allows dynamic registration and deregistration of VLANs, and sends dynamic and static multicast information.
- **Fixed:** in this mode, GMRP forbids dynamic registration and deregistration of multicasts, and sends static rather than dynamic multicast information, allows packets of static multicasts, and transmits packets of static multicasts to other GARP members.
- **Forbidden:** in this mode, GMRP forbids dynamic registration and deregistration of VLANs, and does not transmit dynamic or static multicast information.

3.7.2 Preparing for configurations

Scenario

GARP enables configurations of a GARP member to fast spread to all GARP-enabled devices in the LAN.

The values of the Join timer, Leaver timer, and LeaveAll timer configured through GARP will be applied to all GARP applications in the LAN, including GVRP and GMRP features.

Prerequisite

N/A

3.7.3 Default configurations of GARP

Default configurations of GARP are as below.

Function	Default value
GARP Join timer	20 (in unit of 10ms)
GARP Leave timer	60 (in unit of 10ms)
GARP LeaveAll timer	1000 (in unit of 10ms)
Global GVRP status	Enable

Function	Default value
Interface GVRP status	Disable
GVRP registration mode	Normal
Global GMRP status	Disable
Interface GMRP status	Disable
GMRP registration mode	Normal

3.7.4 Configuring basic functions of GARP

Configure basic functions of GARP for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#i nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)#garp timer { j o i n l e a v e l e a v e a l l } <i>time-value</i>	Configure the GARP timer.

Caution

- The value of the Join timer must be smaller than half of that of the Leave timer.
- The value of the Leave timer must be greater than twice of that of the Join timer, and smaller than that of the LeaveAll timer.
- The value of the LeaveAll timer must be greater than that of the Leave timer.
- In actual networking, we recommend you set the Join timer, Leave timer, LeaveAll timer to 3000, 15000, and 20000.

3.7.5 Configuring GVRP

Configure GVRP for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#gvrp enabl e	Enable global GVRP.
3	NAG(confi g)#i nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
4	NAG(confi g-port)#swi tchport mode trunk	Set the interface to Trunk mode.
5	NAG(confi g-port)#gvrp regi strati on { fi xed forbi dden normal }	(Optional) configure GVRP registration mode.

Step	Command	Description
6	NAG(config g-port)#gvrp enable	Enabling interface GVRP.



Caution

- Interface GVRP can be enabled only after the interface is set to Trunk mode.
- We do not recommend enabling GVRP on a LAG member interface.

3.7.6 Configuring GMRP



Caution

GMRP and IGMP Snooping are mutually exclusive, so you cannot configure them concurrently.

Configure GMRP for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(config g)#gmrp enable	Enable global GMRP.
3	NAG(config g)#i nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
4	NAG(config g-port)#swi tchport mode trunk	Set the interface to Trunk mode.
5	NAG(config g-port)#gmrp regi stration { fixed forbi dden normal }	(Optional) configure GMRP registration mode.
6	NAG(config g-port)#gmrp enable	Enable interface GMRP.

3.7.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show garp [port-list <i>port-list</i>]	Show configurations of the GARP timer.
2	NAG#show garp port-list <i>port-list</i> stati stics	Show GARP statistics.
3	NAG#show gvrp [port-list <i>port-list</i>]	Show GVRP configurations.
4	NAG#show gvrp port-list <i>port-list</i> stati stics	Show GVRP statistics.
5	NAG#show gmrp [port-list <i>port-list</i>]	Show GMRP configurations.

No.	Command	Description
6	NAG# show gmrp port-list <i>port-list</i> statistics	Show GMRP statistics.

3.7.8 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	NAG(config)# clear garp port-list <i>port-list</i> statistics	Clear GARP statistics on the interface.
2	NAG(config)# clear gvrp port-list <i>port-list</i> statistics	Clear GVRP statistics on the interface.
3	NAG(config)# clear gmrp port-list <i>port-list</i> statistics	Clear GMRP statistics on the interface.

3.7.9 Example for configuring GVRP

Networking requirements

As shown in Figure 3-16, to dynamically register, deregister, and update VLAN information between switches, configure GVRP on these switches. Detailed requirements are as below:

- Configure static VLANs 5–10 on Switch A and Switch C.
- Configure static VLANs 15–20 on Switch D.
- Configure static VLANs 25–30 on Switch E.
- Set the interfaces that are connected to other switches to Trunk mode, and enable GVRP on these interfaces.
- Set the Join timer, Leave timer, and LeaveAll timer of GARP on each interface to 3000, 15000, and 20000, in unit of 10ms.

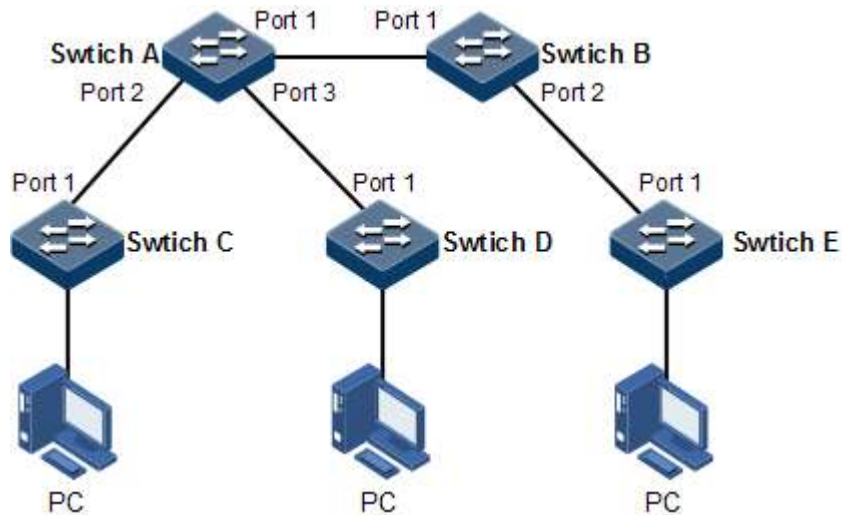


Figure 3-16 GVRP networking

Configuration steps

Step 1 Create VLANs and enable global GVRP.

Configure Switch A.

```
NAG#hostname Swi tchA
Swi tchA#confi g
Swi tchA(confi g)#create vl an 5-10 acti ve
Swi tchA(confi g)#gvrp enabl e
```

Configure Switch B.

```
NAG#hostname Swi tchB
Swi tchB#confi g
Swi tchB(confi g)#gvrp enabl e
```

Configure Switch C.

```
NAG#hostname Swi tchC
Swi tchC#confi g
Swi tchC(confi g)#create vl an 5-10 acti ve
Swi tchC(confi g)#gvrp enabl e
```

Configure Switch D.

```
NAG#hostname Swi tchD
```

```
Swi tchD#confi g
Swi tchD(confi g)#create vlan 15-20 active
Swi tchD(confi g)#gvrp enable
```

Configure Switch E.

```
NAG#hostname Swi tchE
Swi tchE#confi g
Swi tchE(confi g)#create vlan 25-30 active
Swi tchE(confi g)#gvrp enable
```

Step 2 Set interfaces to Trunk mode and enable GVRP on them.

Configure Switch A.

```
Swi tchA(confi g)#interface port-list 1-3
Swi tchA(confi g-range)#swi tchport mode trunk
Swi tchA(confi g-range)#gvrp enable
Swi tchA(confi g-port)#exi t
```

Configure Switch B.

```
Swi tchB(confi g)#interface port-list 1-2
Swi tchB(confi g-range)#swi tchport mode trunk
Swi tchB(confi g-range)#gvrp enable
Swi tchB(confi g-range)#exi t
```

Configure Switch C.

```
Swi tchC(confi g)#interface port-list 1
Swi tchC(confi g-port)#swi tchport mode trunk
Swi tchC(confi g-port)#gvrp enable
Swi tchC(confi g-port)#exi t
```

Configure Switch D.

```
Swi tchD(confi g)#interface port 1
Swi tchD(confi g-port)#swi tchport mode trunk
Swi tchD(confi g-port)#gvrp enable
Swi tchD(confi g-port)#exi t
```


Configure Switch E.

```
Swi tchE(confi g)#i nterface port 1
Swi tchE(confi g-port)#swi tchport mode trunk
Swi tchE(confi g-port)#gvrp enable
Swi tchE(confi g-port)#exi t
```

Step 3 Configure the GARP timers on each interface.**Configure Switch A.**

```
Swi tchA(confi g)#i nterface port-l i st 1-3
Swi tchA(confi g-range)#garp ti mer leaveal l 20000
Swi tchA(confi g-range)#garp ti mer leave 15000
Swi tchA(confi g-range)#garp ti mer joi n 3000
```

Configure Switch B.

```
Swi tchB(confi g)#i nterface port-l i st 1-2
Swi tchB(confi g-range)#garp ti mer leaveal l 20000
Swi tchB(confi g-range)#garp ti mer leave 15000
Swi tchB(confi g-range)#garp ti mer joi n 3000
```

Configure Switch C.

```
Swi tchC(confi g)#i nterface port 1
Swi tchC(confi g-port)#garp ti mer leaveal l 20000
Swi tchC(confi g-port)#garp ti mer leave 15000
Swi tchC(confi g-port)#garp ti mer joi n 3000
```

Configure Switch D.

```
Swi tchD(confi g)#i nterface port 1
Swi tchD(confi g-port)#garp ti mer leaveal l 20000
Swi tchD(confi g-port)#garp ti mer leave 15000
Swi tchD(confi g-port)#garp ti mer joi n 3000
```

Configure Switch E.

```
Swi tchE(confi g)#i nterface port 1
Swi tchE(confi g-port)#garp ti mer leaveal l 20000
```

```

SwitchE(config-port)#garp timer leave 15000
SwitchE(config-port)#garp timer join 3000

```

Checking results

Use the **show gvrp port-list** *port-list* command to show GVRP configurations on the interface.

Take Switch A for example.

```

SwitchA#show gvrp port-list 1-3

```

Port	PortStatus	RegMode	LastPduOrigin	FailedTimes	PortRunStatus
port1	Enable	Normal	0000.0000.0000	0	Enable
port2	Enable	Normal	0000.0000.0000	0	Enable
port3	Enable	Normal	0000.0000.0000	0	Enable

3.7.10 Example for configuring GMRP

Networking requirements

As shown in Figure 3-17, to dynamically register and update multicast information between switches, configure GMRP on each switch. Detailed requirements are as below:

- Configure static VLANs 3–10 on Switch A and Switch B.
- Enable GMRP on the interface connected to the peer switch.
- Configure different static multicast MAC addresses on Switch A and Switch B.
- Set the Join timer, Leave timer, and LeaveAll timer of GARP on each interface to 3000, 15000, and 20000, in unit of 10ms.

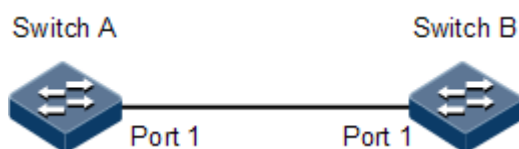


Figure 3-17 GMRP networking

Configuration steps

Step 1 Create VLANs and enable global GMRP.

Configure Switch A.

```

NAG#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 3-10 active
SwitchA(config)#gmrp enable

```

Configure Switch B.

```
NAG#hostname Swi tchB
Swi tchB#confi g
Swi tchB(confi g)#create v l an 3-10 acti ve
Swi tchB(confi g)#gmrp enabl e
```

Step 2 **Set interfaces to Trunk mode and enable GMRP on them.**

Configure Switch A.

```
Swi tchA(confi g)#I nterface port 1
Swi tchA(confi g-port)#gmrp enabl e
Swi tchA(confi g-port)#swi tchport mode trunk
Swi tchA(confi g-port)#exi t
```

Configure Switch B.

```
Swi tchB(confi g)#I nterface port 1
Swi tchB(confi g-port)#gmrp enabl e
Swi tchB(confi g-port)#swi tchport mode trunk
Swi tchB(confi g-port)#exi t
```

Step 3 **Configure static multicast MAC addresses.**

Configure Switch A.

```
Swi tchA(confi g)#mac-address-tabl e stati c mul ti cast 0100.5e05.0600 v l an 3
port-l i st 1
Swi tchA(confi g)#mac-address-tabl e stati c mul ti cast 0100.5e05.0600 v l an 4
port-l i st 1
Swi tchA(confi g)#mac-address-tabl e stati c mul ti cast 0100.5e05.0600 v l an 5
port-l i st 1
```

Configure Switch B.

```
Swi tchB(confi g)#mac-address-tabl e stati c mul ti cast 0100.5e05.0607 v l an 6
port-l i st 1
```

Step 4 **Configure the GARP timers on each interface.**

Configure Switch A.

```

SwitchA(config)#interface port 1
SwitchA(config-port)#garp timer leaveall 20000
SwitchA(config-port)#garp timer leave 15000
SwitchA(config-port)#garp timer join 3000

```

Configure Switch B.

```

SwitchA(config)#interface port 1
SwitchA(config-port)#garp timer leaveall 20000
SwitchA(config-port)#garp timer leave 15000
SwitchA(config-port)#garp timer join 3000

```

Checking results

Use the **show gmrp port-list** *port-list* command to show GMRP configurations on a specified interface.

Take Switch B for example.

```

SwitchB#show gmrp port-list 1
Port  PortStatus  RegMode  LastPduOrigin  FailedTimes  PortRunStatus
-----
port1  Enable       Normal   0000.0000.0000  0             Enable

```

Use the **show mac-address-table multicast** command to show multicast information on the SNR-S212i-8POE.

Take Switch B for example.

```

SwitchB#show mac-address-table multicast
Filter mode for unknown multicast: flood all
Vlan      Multicast address      Ports[Static]
-----
3         0100.5E05.0600         port 1 [port 1]
4         0100.5E05.0600         port 1 [port 1]
5         0100.5E05.0600         port 1 [port 1]
6         0100.5E05.0607         port 1 [port 1]

```

3.8 Loopback detection

3.8.1 Introduction

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

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

As shown in Figure 3-18, Switch B and Switch C connect the user network.

- Self-loop: user loop on the same Ethernet interface of the same device. User network B has a loop, which forms self-loop.
- Internal loop: the loop forming on different Ethernet interfaces of the same device. Port 1 and Port 3 on Switch C forms an internal loop with the user network A.
- External loop: the loop forming on the Ethernet interface of different devices. Switch A, Switch B, and Switch C form external loop with user network C.

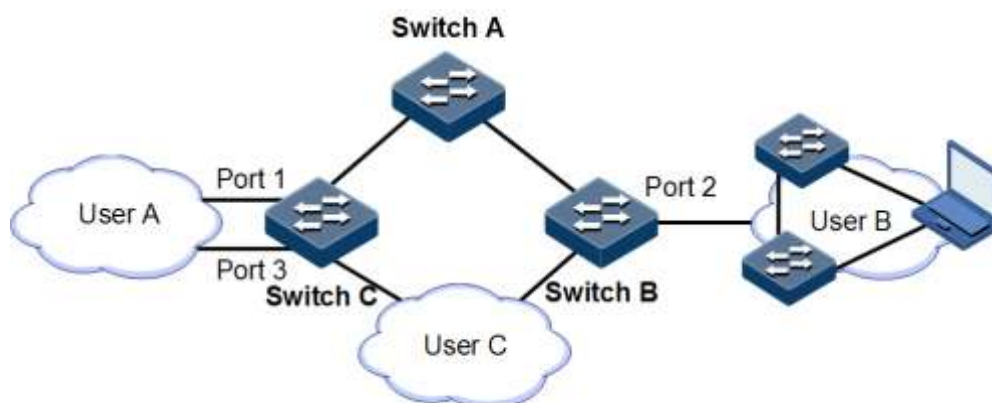


Figure 3-18 Loopback detection networking

Principle for processing loops

The SNR-S212i-8POE processes loops as below:

- If the device sending the loopback detection packet is not the one receiving the packet, process the device with the larger MAC address to eliminate the loop (external loop).
- If the device sending the loopback 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 (internal 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 3-18, assume that both Switch B and Switch connect user network interfaces enabled with loop detection. The system processes loops for the three loop types as below:

- Self-loop: the interface sending the packet and the interface receiving the packet on Switch B are the same, the configured loopback detection action will be taken to eliminate the loop on Port 2.
- Internal loop: Switch C will receive the loop detection packets sent by it and the interface sending the packet and the interface receiving the packet are the same, the configured loopback detection action will be taken to eliminate the loop on the interface with a bigger interface number, namely, Port 3.
- External loop: Switch B and Switch C will receive the loop detection packets from each other, and the configured loopback detection action will be taken to eliminate the loop on the switch with a bigger MAC address.

Action for processing loops

The action for procee loops is the mothod for the SNR-S212i-8POE to use upon loopback detection. You can define different actions on the specified interface according to actual situations, including:

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

Loopback detection modes

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

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

If the loopback detection processing mode is Trap-only in the previous two modes, the SNR-S212i-8POE sends Trap only.

Loop restoration

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

- If an interface is configured as automatical restoration after a specified period, the system will start loopback 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 automatical restoaration, namely, the automatical restoration time is infinite, it will not be automatically restored. However, you can use

the **no loopback-detection discarding** command to manually restore the interface blocked or shut down upon loopback detection.

3.8.2 Preparing for configurations

Scenario

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

Prerequisite

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

3.8.3 Default configurations of loopback detection

Default configurations of loopback detection are as below.

Function	Default value
Interface loopback detection status	Disable
Automatic recovery time for the blocked interface	No automatic recovery
The loop process mode of loopback detection	Trap-only
Loopback detection period	4s
Loopback detection mode	VLAN mode
Time for recovering the block interface due to loopback detection	Infinite

3.8.4 Configuring loopback detection

Loopback detection support physical interfaces and Link Aggregation Group (LAG) interfaces.


Configure loopback detection for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#l oopback-detecti on enabl e { port-l i st port-l i st port- channel port-channel -l i st }</code>	Enable loopback detection on the interface.
3	<code>NAG(confi g)#l oopback-detecti on hel l o-ti me peri od</code>	Configure the period for sending loopback detection packets.

Step	Command	Description
4	NAG(config)#loopback-detection mode { port-based vlan-based }	(Optional) configure loopback detection mode.
5	NAG(config)#loopback-detection loop { discard trap-only shutdown } { port-list port-list port-channel port-channel-list }	(Optional) configure processing mode when the interface receives loopback detection packets from other devices.
6	NAG(config)#loopback-detection down-time { time-value infinite }	(Optional) configure the time for automatically recover the blocked interface due to loopback detection.
7	NAG(config)#no loopback-detection discard { port-list port-list port-channel port-channel-list }	Enable the interface blocked due to loopback detection.

3.8.5 Configuring uplink interface for loopback detection

Configure uplink interface for loopback detection for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#config	Enter global configuration mode.
2	NAG(config)#loopback-detection loop upstream { port-list port-list port-channel port-channel-list } [delete-vlan]	Configure the uplink interface for loopback detection and processing mode for the uplink interface upon loopback detection.  Caution The delete-vlan parameter takes effects on VLAN mode only in loopback detection.

3.8.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show loopback-detection [port-list port-list port-channel port-channel-list]	Show configurations of loopback detection on the interface.
2	NAG#show loopback-detection blocked-vlan [port-list port-list port-channel port-channel-list]	Show information about the VLAN blocked due to loopback detection.
3	NAG#show loopback-detection statistics [port-list port-list port-channel port-channel-list]	Show statistics of loopback detection on the interface
4	NAG#show loopback-detection vlan-list vlan-list	Show loopback detection status of a specified VLAN.

3.8.7 Maintenance

Maintain the SNR-S212i-8POE by below commands.

No.	Command	Description
1	NAG(config-port)#clear loopback-detection statistic	Clear loopback detection statistics.
2	NAG(config-aggregator)#clear loopback-detection statistic	

3.8.8 Example for configuring internal loopback detection

Networking requirements

As shown in Figure 3-19, Port 2 and Port 3 on Switch A are connected to the user network. To avoid loops on the user network, enable loopback detection on Switch A to detect loops on user network, and then take actions accordingly. Detailed requirements are as below:

- Enable loopback detection on Port 2 and Port 3.
- Configure the interval for sending loopback detection packets to 3s.
- Configure loopback detection mode to VLAN mode.
- Configure the loopback detection processing mode to discarding, namely, blocking the interface.

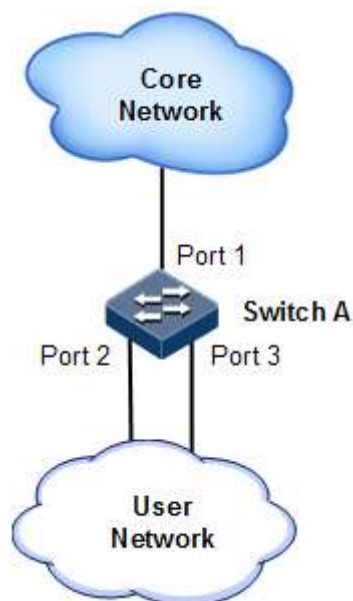


Figure 3-19 Loopback detection networking

Configuration steps

- Step 1 Create VLAN 3, and add ports into VLAN 3.

```

NAG#confi g
NAG(confi g)#create vl an 3 acti ve
NAG(confi g)#I nterface port 2
NAG(confi g-port)#swl tchport access vl an 3
NAG(confi g-port)#exl t
NAG(confi g)#I nterface port 3
NAG(confi g-port)#swl tchport access vl an 3
NAG(confi g-port)#exl t

```

Step 2 Enable loopback detection on the specified ports.

```

NAG(confi g)#l oopback-detecti on enabl e port 2-3

```

Step 3 Configure loopback detection modes.

```

NAG(confi g)#l oopback-detecti on mode vl an-based

```

Step 4 Configure loopback detection processing modes.

```

NAG(confi g)#l oopback-detecti on l oop di scardi ng port-l i st 2

```

Step 5 Configure the interval for sending loopback detection packets.

```

NAG(confi g)#l oopback-detecti on hel l o-ti me 3

```

Checking results

Use the **show loopback-detection** command to show loopback detection status.

```

NAG#show l oopback-detecti on port-l i st 2
Destinati on address: ffff. ffff. ffff
Mode: Vl an-based
Peri od of l oopback-detecti on: 3s
Restore ti me: i nfi ni te
Port      PortState      State      Status      l oop-act      vl an l i st
-----
Port2     Up              Ena        yes         di scardi ng   3

```

3.8.9 Example for configuring external loop for loopback detection

Networking requirements

As shown in Figure 3-20, Switch A, Switch B, and Switch C are connected to the user network (VLAN 3). To avoid loops on the user network, enable loopback detection on Switch A and Switch B to detect loops on user network, and then take actions accordingly. Detailed requirements are as below:

- Enable loopback detection on Port 1 on both Switch A and Switch B.
- Configure the interval for sending loopback detection packets to 3s.
- Configure loopback detection mode to Port mode.
- Configure the loopback detection processing mode to shutdown, namely, shutting down the interface.

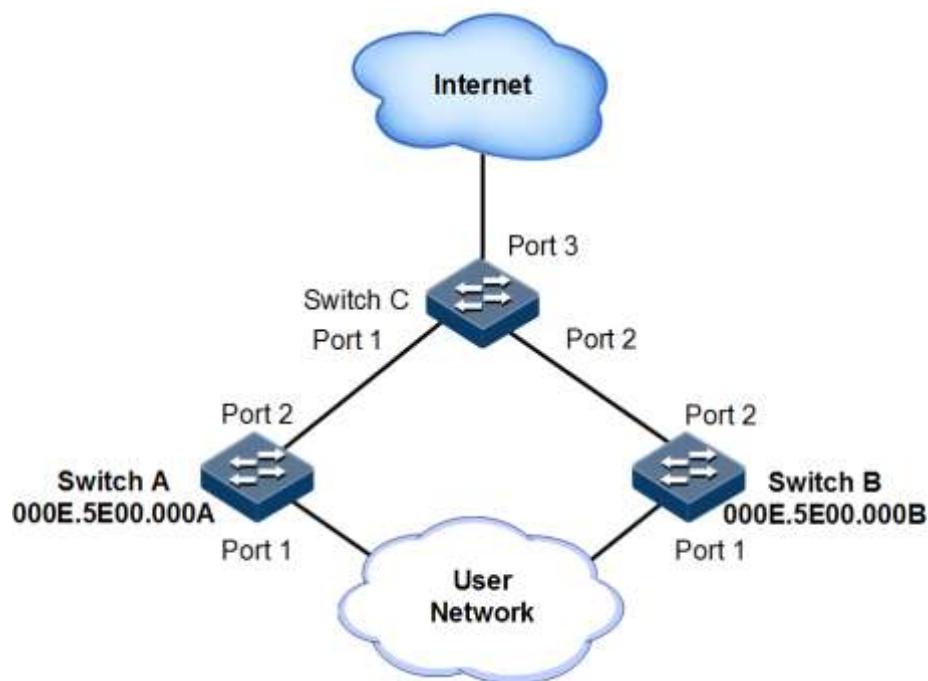


Figure 3-20 Networking with external loopback for loopback detection

Configuration steps

Step 1 Create VLAN 3, and add ports into VLAN 3.

Configure Switch A.

```

NAG#hostname Swi tchA
Swi tchA#confi g
Swi tchA(confi g)#create vl an 3 acti ve
Swi tchA(confi g)#i nterface port 1
Swi tchA(confi g-port)#swi tchport mode access
Swi tchA(confi g-port)#swi tchport access vl an 3
Swi tchA(confi g-port)#exi t

```

```
Swi tchA(confi g)#I nterface port 2
Swi tchA(confi g-port)#swi tchport mode trunk
Swi tchA(confi g-port)#exi t
```

Configure Switch B.

```
NAG#hostname Swi tchB
Swi tchB#confi g
Swi tchB(confi g)#create vl an 3 active
Swi tchB(confi g)#I nterface port 1
Swi tchB(confi g-port)#swi tchport mode access
Swi tchB(confi g-port)#swi tchport access vl an 3
Swi tchB(confi g-port)#exi t
Swi tchB(confi g)#I nterface port 2
Swi tchB(confi g-port)#swi tchport mode trunk
Swi tchB(confi g-port)#exi t
```

Configure Switch C.

```
NAG#hostname Swi tchC
Swi tchC#confi g
Swi tchC(confi g)#I nterface port-l ist 1-2
Swi tchC(confi g-range)#swi tchport mode trunk
```

Step 2 Enable loopback detection.

Configure Switch A.

```
Swi tchA(confi g)#l oopback-detecti on enable port-l ist 1
Swi tchA(confi g)#l oopback-detecti on mode port-based
Swi tchA(confi g)#l oopback-detecti on l oop shutdown port-l ist 1
Swi tchA(confi g)#l oopback-detecti on hel lo-ti me 3
```

Configure Switch B.

```
Swi tchB(confi g)#l oopback-detecti on enable port-l ist 1
Swi tchB(confi g)#l oopback-detecti on mode port-based
Swi tchB(confi g)#l oopback-detecti on l oop shutdown port-l ist 1
Swi tchB(confi g)#l oopback-detecti on hel lo-ti me 3
```

Checking results

Use the **show loopback-detection** command on Switch A and Switch B to show loopback detection status. Port 1 on Switch B will be shut down to eliminate the loop because the MAC address of Switch B is larger than that of Switch A.

```
SwitchA#show loopback-detection port-list 1
Destination address: FFFF.FFFF.FFFF
Mode: Port-based
Period of loopback-detection: 3s
Restore time: infinite
Port      PortState      State      Status      Loop-act      Vlan list
-----
Port1     Down           Ena       no          shutdown

```

```
SwitchB#show loopback-detection port-list 1
Destination address: FFFF.FFFF.FFFF
Mode: Port-based
Period of loopback-detection: 3s
Restore time: infinite
Port      PortState      State      Status      Loop-act      Vlan list
-----
Port1     Down           Ena       yes         shutdown

```

3.9 Line detection

3.9.1 Introduction

Line detection is a module to detect physical lines and provides you with status query function, so it can help you analyze fault source and maintain the network.

3.9.2 Preparing for configurations

Scenario

With this function, you can query status of physical lines between devices, analyze faults, and thus maintain the network.

Prerequisite

N/A

3.9.3 Configuring line detection

Configure line detection for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#test cable-diagnostics port-list port-list</code>	Detect physical link status.

3.9.4 Checking configurations

Use the following command to check configuration result.

No.	Command	Description
1	<code>NAG#show cable-diagnostics [port- list port-list]</code>	Show information about line detection.

3.9.5 Example for configuring line detection

Networking requirements

As shown in Figure 3-21, to help you analyze fault source, conduct line detection on the Switch.

No line detection is done before.

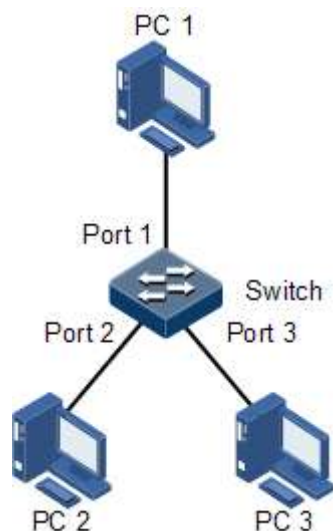


Figure 3-21 Line detection networking

Configuration steps

Conduct line detection on Ports 1–3 on the switch.

```
NAG#test cable-diagnostics port-list 1-3
```

Checking results

Use **show cable-diagnostics [port-list port-list]** command to show configurations of line detection on the interface.

```
NAG#show cable-diagnostics port-list 1-2
Port  Attribute      Time          RX Stat  RX Len(m)  TX Stat  TX Len(m)
-----
port1  Issued          01/09/2011 08:13:03  Normal   0          Normal   0
port2  Issued          01/09/2011 08:13:03  Normal   0          Normal   0
```

Remove the line that connects PC 1 and the switch from the PC 1, and conduct line detection again. Use the **show cable-diagnostics [port-list port-list]** command again to show configurations of line detection on the interface.

```
NAG#show cable-diagnostics port-list 1-2
Port  Attribute      Time          RX Stat  RX Len(m)  TX Stat  TX Len(m)
-----
port1  Issued          01/09/2011 08:18:09  Open     3          Open     3
port2  Issued          01/09/2011 08:18:09  Normal   0          Normal   0
```

3.10 Interface protection

3.10.1 Introduction

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

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

3.10.2 Preparing for configurations

Scenario

The interface protection function can realize mutual isolation of interfaces in the same VLAN, enhance network security and provide flexible networking solutions for you.

Prerequisite

N/A

3.10.3 Default configurations of interface protection

Default configurations of interface protection are as below.

Function	Default value
Interface protection status	Disable

3.10.4 Configuring interface protection



Caution

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

Configure interface protection for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i nterface port port-i d	Enter physical layer interface configuration mode.
3	NAG(confi g-port)# swi tchport protect	Enable interface protection.

3.10.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG# show swi tchport protect	Show interface protection configuration.

3.10.6 Example for configuring interface protection

Networking requirements

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

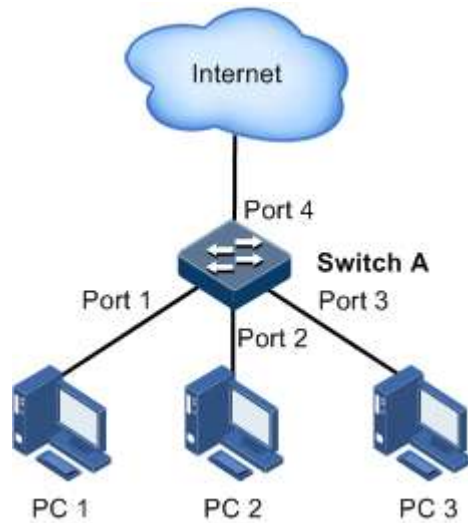


Figure 3-22 Interface protection networking

Configuration steps

Step 1 Enable interface protection on the Port 1.

```
NAG#confi g
NAG(confi g)#i nterface port 1
NAG(confi g-port)#swi tchport protect
NAG(confi g-port)#exi t
```

Step 2 Enable interface protection on the Port 2.

```
NAG(confi g)#i nterface port 2
NAG(confi g-port)#swi tchport protect
```

Checking results

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

```
NAG#show swi tchport protect
Port      Protected State
-----
port1     enabl e
port2     enabl e
port3     di sabl e
port4     di sabl e
port5     di sabl e
.....
```

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.

3.11 Port mirroring

3.11.1 Introduction

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

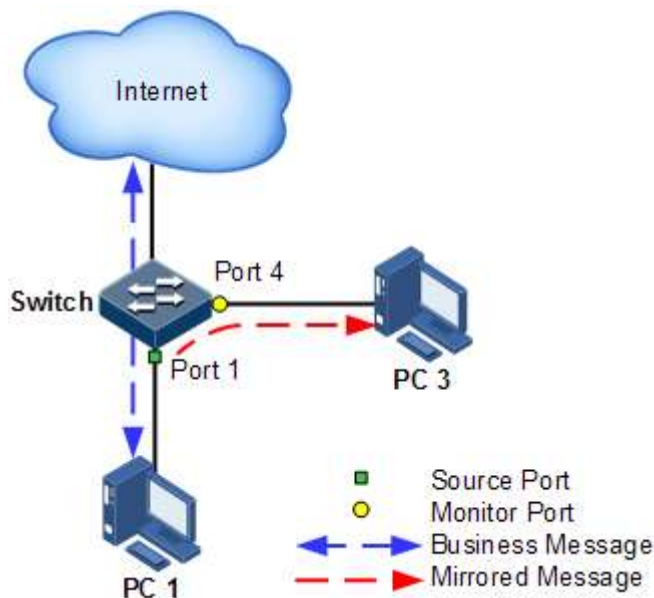


Figure 3-23 Port mirroring principle

The basic principle of port mirroring is shown in Figure 3-23. PC 1 connects to the external network through the Port 1; PC 3 is the monitor PC, connecting the external network through Port 4.

When monitoring packets from the PC 1, you need to assign Port 1 to connect to PC 1 as the mirroring source port, enable port mirroring on the ingress port and assign Port 4 as the monitor port to mirror packets to the destination port.

When service packets from PC 1 enter the switch, the switch will forward and copy them to monitor port (Port 4). The monitor device connected to mirror the monitor port can receive and analyze these mirrored packets.

The SNR-S212i-8POE supports data stream mirroring on the ingress port and egress port. The packets on ingress/egress mirroring port will be copied to the monitor port after the switch is enabled with port mirroring. The monitor port and mirroring port cannot be the same one.

3.11.2 Preparing for configurations

Scenario

Port mirroring is used to monitor network data type and flow regularly for 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

3.11.3 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
Monitor port	Port 1

3.11.4 Configuring port mirroring on local port



Caution

- There can be multiple source mirroring ports but only one monitor port.
- The ingress/egress mirroring port packet will be copied to the monitor port after port mirroring takes effect. The monitor port cannot be set to the mirroring port again.

Configure local port mirroring for the SNR-S212i-8POE as below.

Step	Configure	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#mi rror { moni tor-cpu moni tor-port port <i>port-id</i> }</code>	Configure mirroring packets to CPU or specified monitor port.
3	<code>NAG(confi g)#mi rror source-port-list { both port-list <i>port-list</i> egress port-list <i>port-list</i> ingress port-list <i>port-list</i> [egress port-list <i>port-list</i>] }</code>	Configure the mirror source port of port mirroring, and designate the mirroring rule for port mirroring.

Step	Configure	Description
4	NAG(confi g)#mi rror enable	Enable port mirroring.

3.11.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show mi rror	Show configurations of port mirroring.

3.11.6 Example for configuring port mirroring

Networking requirements

As shown in Figure 3-24, the network administrator wishes to monitor user network 1 through the monitor device, then to catch the fault or abnormal data flow for analyzing and discovering problem and then solve it.

The SNR-S212i-8POE is disabled with storm control and automatic packets sending. User network 1 accesses the SNR-S212i-8POE through Port 1, user network 2 accesses the SNR-S212i-8POE through Port 2, and the data monitor device is connected to Port 3.

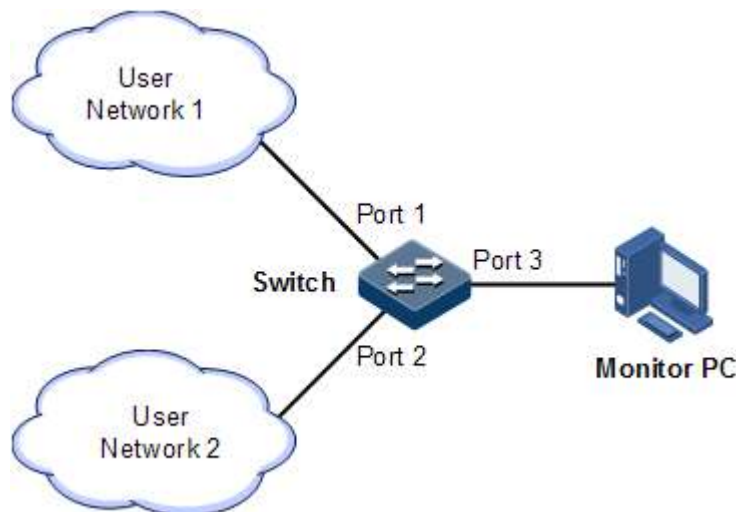


Figure 3-24 Port mirroring networking

Configuration steps

Enable port mirroring on the Switch.

```
NAG#confi g
NAG(confi g)#mi rror moni tor-port port 3
```

```
NAG(confi g)#mi rror source-port-l ist i ngress port-l ist 1
NAG(confi g)#mi rror enabl e
```

Checking results

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

```
NAG#show mi rror
Mi rror: Enabl e
Moni tor port: port3
-----the i ngress mi rror rul e-----
Mi rrored ports: port-l ist 1
-----the egress mi rror rul e-----
Mi rrored ports: --
```

3.12 Layer 2 protocol transparent transmission

3.12.1 Introduction

Transparent transmission is one of the main Ethernet device functions, and usually the edge network devices of carrier conduct Layer 2 protocol packet transparent transmission. Transparent transmission is enabled on the interface that connects edge network devices of carrier and user network. The interface is in Access mode, connecting to Trunk interface on user device. The layer 2 protocol packet of the user network is send from transparent transmission interface, encapsulated by the edge network device (ingress end of packets), and then send to the carrier network. The packet is transmitted through the carrier network to reach the edge device (egress end of packet) at the other end or carrier network. The edged device decapsulates outer layer 2 protocol packet and transparent transmits it to the user network.

The transparent transmission function includes packet encapsulation and decapsulation function, the basic implementing principle as below.

- Packet encapsulation: at the packet ingress end, the SNR-S212i-8POE modifies the destination MAC address from user network layer 2 protocol packets to special multicast MAC address (010E.5E00.0003 by default). On the carrier network, the modified packet is forwarded as data in user VLAN.
- Packet decapsulation: at the packet egress end, the SNR-S212i-8POE senses packet with special multicast MAC address (010E.5E00.0003 by default), reverts the destination MAC address to DMAC of Layer 2 protocol packets, then sends the packet to assigned user network.

Layer 2 protocol transparent transmission can be enabled at the same time with QinQ or enabled independently. In actual networking, after modifying the MAC address of protocol packets, you need to add outer Tag for packets to send them through the carrier network.

The SNR-S212i-8POE supports transparent transmission of BPDU packet, DOT1X packet, LACP packet, CDP packet, PVST packet, PAGP packet, UDLD packet, and VTP packet.

3.12.2 Preparing for configurations

Scenario

This function enables layer 2 protocol packets of one user network to traverse the carrier network to make a user network in different regions uniformly run the same Layer 2 protocol. You can configure rate limiting on transparent transmission packets to prevent packet loss.

Prerequisite

N/A

3.12.3 Default configurations of Layer 2 protocol transparent transmission

Default configurations of Layer 2 protocol transparent transmission are as below.

Function	Default value
Layer 2 protocol transparent transmission status	Disable
Egress interface and belonged VLAN of Layer 2 protocol packets	N/A
TAG CoS value of transparent transmission packets	0, displayed as "--"
Destination MAC address of transparent transmission packets	010E.5E00.0003
Packet loss threshold and disabling threshold for transparent transmission packets	N/A

3.12.4 Configuring transparent transmission parameters

Configure transparent transmission parameter for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#rel ay desti nati on- address mac-address</code>	(Optional) configure destination MAC for transparent transmission packets.
3	<code>NAG(confi g)#rel ay cos cos-val ue</code>	(Optional) configure CoS value for transparent transmission packets.
4	<code>NAG(confi g)#i nterface i nterface-type i nterface-number</code>	Enter physical layer interface configuration mode or LAG configuration mode.
5	<code>NAG(confi g-port)#rel ay { port port-id port-channel port- channel -number }</code> <code>NAG(confi g-aggregator)#rel ay { port port-id port-channel port-channel -number }</code>	Configure specified egress interface for transparent transmission packets.

Step	Command	Description
6	NAG(config-port)#rel ay vl an <i>vl an-id</i>	Configure specified VLAN for transparent transmission packets.
	NAG(config-aggregator)#rel ay vl an <i>vl an-id</i>	This configuration enables packets to be forwarded according to the specified VLAN instead of the ingress interface.
7	NAG(config-port)#rel ay { all cdp dot1x lacp pvst stp vtp }	Configure the type of transparent transmission packets on the interface and disable related protocol.
	NAG(config-aggregator)#rel ay { all cdp dot1x lacp pvst stp vtp }	

3.12.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show rel ay [port-list <i>port-list</i> port-channel -list <i>port-channel-</i> <i>list</i>]	Show configuration and status of transparent transmission.
2	NAG#show rel ay stati stics [port-list <i>port-list</i> port-channel -list <i>port-</i> <i>channel-list</i>]	Show statistics of transparent transmission packets.

3.12.6 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Commands	Description
1	NAG(config)#clear rel ay stati stics [port- list <i>port-list</i> port-channel -list <i>port-</i> <i>channel-list</i>]	Clear statistics of transparent transmission packets.

3.12.7 Example for configuring Layer 2 protocol transparent transmission

Networking requirements

As shown in Figure 3-25, Switch A and Switch B connect to two user networks VLAN 100 and VLAN 200 respectively. You need to configure Layer 2 protocol transparent transmission function on Switch A and Switch B to make the same user network in different regions run STP entirely.

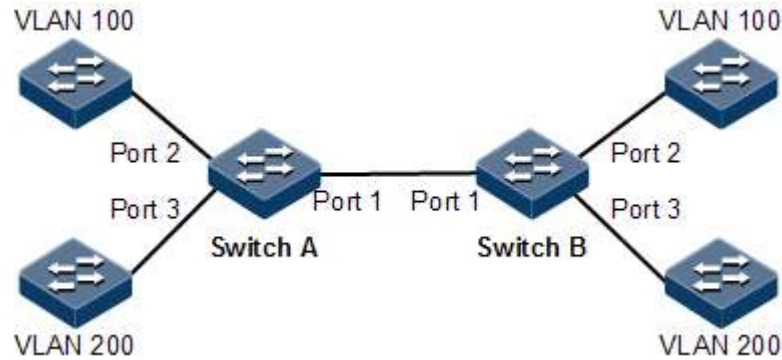


Figure 3-25 Layer 2 protocol transparent transmission networking

Configuration steps

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

Configure Switch A.

```
NAG#hostname Swi tchA
Swi tchA#confi g
Swi tchA(confi g)#create vl an 100, 200 acti ve
```

Configure Switch B.

```
NAG#hostname Swi tchB
Swi tchA#confi g
Swi tchA(confi g)#create vl an 100, 200 acti ve
```

Step 2 Set the switching mode of Port 2 to Access mode, set the Access VLAN to 100, and enable STP transparent transmission.

Configure Switch A.

```
Swi tchA(confi g)#i nterface port 2
Swi tchA(confi g-port)#swi tchport mode access
Swi tchA(confi g-port)#swi tchport access vl an 100
Swi tchA(confi g-port)#rel ay stp
Swi tchA(confi g-port)#rel ay port 1
Swi tchA(confi g-port)#exi t
```

Configure Switch B.

```
Swi tchB(confi g)#i nterface port 2
Swi tchB(confi g-port)#swi tchport mode access
```



```
Swi tchB(confi g-port)#swi tchport access vl an 100
Swi tchB(confi g-port)#rel ay stp
Swi tchB(confi g-port)#rel ay port 1
Swi tchB(confi g-port)#exi t
```

- Step 3 Set the switching mode of Port 3 to Access mode, set the Access VLAN to 200, and enable STP transparent transmission.

Configure Switch A.

```
Swi tchA(confi g)#i nterface port 3
Swi tchA(confi g-port)#swi tchport mode access
Swi tchA(confi g-port)#swi tchport access vl an 200
Swi tchA(confi g-port)#rel ay stp
Swi tchA(confi g-port)#rel ay port 1
Swi tchA(confi g-port)#exi t
```

Configure Switch B.

```
Swi tchB(confi g)#i nterface port 3
Swi tchB(confi g-port)#swi tchport mode access
Swi tchB(confi g-port)#swi tchport access vl an 200
Swi tchB(confi g-port)#rel ay stp
Swi tchB(confi g-port)#rel ay port 1
Swi tchB(confi g-port)#exi t
```

- Step 4 Set Port 1 to Trunk mode.

Configure Switch A.

```
Swi tchA(confi g)#i nterface port 1
Swi tchA(confi g-port)#swi tchport mode trunk
```

Configure Switch B.

```
Swi tchB(confi g)#i nterface port 1
Swi tchB(confi g-port)#swi tchport mode trunk
```

Checking results

Use the **show relay** command to show configurations of Layer 2 protocol transparent transmission.

Take Switch A for example.

```
SwitchA#show relay port-list 1-3
COS for Encapsulated Packets: --
Destination MAC Address for Encapsulated Packets: 010E.5E00.0003
Port      vlan  Egress-Port  Protocol
-----
port1(up)  --    --          stp
              dot1x
              lacp
              cdp
              vtp
              pvst
port2(up)  --    port1      stp(enable)
              dot1x
              lacp
              cdp
              vtp
              pvst
port3(up)  --    port1      stp(enable)
              dot1x
              lacp
              cdp
              vtp
              pvst
```

4 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

4.1 Introduction

4.1.1 PoE principle

Power over Ethernet (PoE) refers 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).

4.1.2 PoE modules

The PoE system is composed of the following modules:

- PSE: composed 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/IEEE 802.3at, such as IP phone and web camera.
- PI: the PoE-supportive Ethernet interface

4.1.3 PoE advantages

PoE has the following advantages:

- Safety and reliability: a centralized PSE supplies power with convenient backup, uniform management of power modules, and high security.
- Convenient power supply: the network terminal does not need an external power; instead, it needs only an 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.

4.1.4 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. When the PoE mode is auto, power on the PI connected PD with critical priority first, then the PD with high priority, and finally the PD with low priority.

There are two power supply management modes: auto and manual.

- In auto mode, when the SNR-S212i-8POE supplies power to external devices in full load, it first supplies power to the PD connected to the PI with the critical priority, then the PD connected to the PI with the high priority, and finally the PD connected to the PI with the low priority; it firstly supplies power to the PD connected to the PI with the smaller interface ID if two PIs
- In manual mode, when the SNR-S212i-8POE supplies power to external devices in full load, it supplies power in order that external devices are connected to it.

- Forcible power supply

When a device connected to the SNR-S212i-8POE fails to work properly in normal power supply mode, use this function to forcibly supply power to the device.

- 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 ratio exceeds the threshold, or the status of PoE changes, the SNR-S212i-8POE sends Trap to the NMS.

- PSE power utilization ratio threshold

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

4.2 Configuring PoE

4.2.1 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. The network terminal does not need an external power; instead, it needs only an Ethernet cable connected to the PoE interface.

Prerequisite

N/A

4.2.2 Default configurations of PoE

Default configurations of PoE are as below.

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

4.2.3 Enabling interface PoE

Enable interface PoE for the SNR-S212i-8POE as below:

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#i nterface port port-i d</code>	Enter physical layer interface configuration mode.
3	<code>NAG(confi g-port)#poe enabl e</code>	Enable interface PoE.

4.2.4 Configuring power supply modes

Configure power supply modes for the SNR-S212i-8POE as below:

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#power-management { auto manual }</code>	Configure power supply modes.

4.2.5 Configuring maximum output power of PoE

Configure the maximum output power of PoE for the SNR-S212i-8POE as below:

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#I nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)#poe max-power <i>max-power-value</i>	Configure the maximum output power of PoE.

4.2.6 Configuring priority of PoE

Configure priority of PoE for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#I nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)#poe pri ori ty { cri ti cal hi gh low }	Configure priority of PoE.

4.2.7 Configuring identifying non-standard PDs

Identify non-standard PDs for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#poe l egacy { enabl e di sabl e }	Enable/Disable PSE device to identify non-standard PDs.

4.2.8 Configuring PSE power utilization ratio threshold

Configure the PSE power utilization ratio threshold for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#poe pse power-thredshol d <i>percent</i>	Configure the PSE power utilization ratio threshold.

4.2.9 Enabling non-standard PD identification



Note

To use a non-standard PD, 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 over high power.

Enable non-standard PD identification for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# poe l egacy enabl e	Enable non-standard PD identification.

4.2.10 Enabling forcible power supply on interface



Caution

- When a device connected to the SNR-S212i-8POE fails to work properly in normal power supply mode, use this function to forclicly supply power to the device.
- Forcible power supply is recommended only when the power supply fails after using the **poe legacy enable** command and the user ensures to supply power to the PD.

Enable forcible power supply on interfaces for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# I nterface port port- id	Enter physical layer interface configuration mode.
3	NAG(confi g-port)# poe force-power	Enable forcible PoE power supply on the interface.

4.2.11 Enabling overtemperature protection

Enable overtemperature protection for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.

Step	Command	Description
2	NAG(confi g)# po e temperature-protecti on enable	Enable overtemperature protection.

4.2.12 Enabling global Trap

Enable global Trap for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# po e pse trap enable	Enable global Trap function.

4.2.13 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG# show po e port-l ist <i>port-l ist [detail]</i>	Show power supply status on specified interfaces.
2	NAG# show po e pse [detail]	Show PSE configurations and realtime operating information.

4.3 Example for configuring PoE power supply

Networking requirements

As shown in Figure 4-1, PoE-supportive Switch A is used to supply power to an IP phone and a monitor camera. It is required to supply power to the monitor camera in precedence when it runs in full load. Detailed requirements are as below:

- Set the maximum output power of Port 1 and Port 2 to 30000 mW.
- Enable overtemperature protection on the switch.
- Enable Trap function for power supply on the switch.
- Set the power supply management mode to auto.
- Set the priorities of Port 2 and Port 1 to high and low respectively.

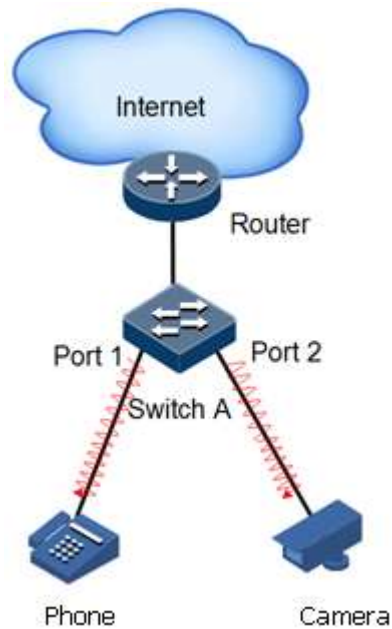


Figure 4-1 PoE switch power supply networking

Configuration steps

Step 1 Enable PoE on Port 1 and Port 2.

```
NAG#confi g
NAG(confi g)#i nterface port 1
NAG(confi g-port)#poe enabl e
NAG(confi g-port)#exi t
NAG(confi g)#i nterface port 2
NAG(confi g-port)#poe enabl e
NAG(confi g-port)#exi t
```

Step 2 Set the maximum output power of Port 1 and Port 2 to 30000 mW.

```
NAG(confi g)#i nterface port 1
NAG(confi g-port)#poe max-power 30000
NAG(confi g-port)#exi t
NAG(confi g)#i nterface port 2
NAG(confi g-port)#poe max-power 30000
NAG(confi g-port)#exi t
```

Step 3 Enable overtemperature protection.

```
NAG(confi g)#poe temperature-protecti on enabl e
```

Step 4 Enable global Trap.

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

Step 5 Set priorities of Port 2 and Port 1 to high and low respectively.

```
NAG(config)#interface port 2
NAG(config-port)#poe priority high
NAG(config-port)#exit
NAG(config)#interface port 1
NAG(config-port)#poe priority low
```

Checking results

Use the **show poe port-list 1,2 detail** command to show PoE configurations on Port 1 and Port 2.

```
NAG#show poe port-list 1,2 detail
```

```
Port: 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)
```

```
Port: 2
```

```
-----
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)
```

5 Ring network protection

This chapter describes ring network protection, and provides related configuration examples, including the following sections:

- G.8032
- RRPS

5.1 G.8032

5.1.1 Introduction

G.8032 (Ethernet Ring Protection Switching, ERPS) is an APS protocol over ITU-T G.8032 recommendation. It is specially used in Ethernet ring link protocol. Generally, G.8032 can avoid broadcast storm caused by data loopback. When Ethernet has loop or device malfunction, G.8032 can switch the link to backup link and ensure service restore quickly.

G.8032 takes the control VLAN in ring network to transmit ring network control information and meanwhile, combining with the topology feature of ring network to discover network fault quickly and enable backup link to restore service fast.

5.1.2 Preparing for configurations

Scenario

With the development from Ethernet to the telecom-grade network, voice and video multicast services bring forth higher requirements on Ethernet redundant protection and fault-restore time. The fault-restore convergent time of current STP system is in second level that is far away to meet requirement. G.8032 can switch the service link to the backup link if the ring link or node fails, thus eliminating loops, conducting fault Automatic Protection Switching (APS) and automatic fault restoration. In addition, the APS time is shorter than 50ms. It supports the single ring, intersecting ring, and tangent rings networking modes.

Prerequisite

- Connect interface and configure physical parameters for it, the interface is Up at physical layer.
- Create VLANs.

- Add interfaces into VLANs.

5.1.3 Default configurations of G.8032

Default configurations of G.8032 are as below.

Function	Default value
Protocol VLAN	1
Protection ring	Revertive mode
Protocol version	2
Ring WTR timer	5min
Guard timer	500ms
Ring HOLDOFF timer	0
G.8032 fault information reported to network management system	Disable
Sub-ring virtual path mode in intersecting node	with
Ring Propagate switch in intersecting node	Disable

5.1.4 Creating G.8032 ring


Create a G.8032 ring for the SNR-S212i-8POE as below.




Caution

- Only one Ring Protection Link (RPL) can be configured in a ring; namely, only one device can be configured as the RPL Owner in a ring. One device works as the RPL Neighbour, and other devices can only be configured as ring forwarding nodes.
- A tangent ring can be taken as two independent rings in fact, and its configurations are identical to common single rings. The intersecting ring has a master ring and a sub-ring; for its configurations, see section 5.1.5 (Optional) creating G.8032 sub-ring.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.

Step	Command	Description
2	NAG(config)# ethernet ring-protecti on <i>ring-id</i> east { port <i>port-id</i> port-channel <i>port-channel-number</i> } west { port <i>port-id</i> port-channel <i>port-channel-number</i> } [node-type rpl -owner rpl { east west }] [not-reverti ve] [protocol -vl an <i>vlan-id</i>] [block-vl an l i st <i>vlan-list</i>]	<p>Create a ring and configure the node as the RPL Owner.</p> <p>By default, protocol VLAN is 1, blocked VLAN range is 1-4094.</p> <p>A protection ring changes to non-revertive mode if configured with the not-revertive parameter. Traffic will be switched back to the current link from protection link after the fault of the current link is cleared; however, traffic is not switched in non-revertive mode.</p> <p> Note The east-bound and western-bound interface cannot be identical.</p>
	NAG(config)# ethernet ring-protecti on <i>ring-id</i> east { port <i>port-id</i> port-channel <i>port-channel-number</i> } west { port <i>port-id</i> port-channel <i>port-channel-number</i> } node-type rpl -neighbour rpl { east west } [not-reverti ve] [protocol -vl an <i>vlan-id</i>] [block-vl an l i st <i>vlan-list</i>]	Create a ring and configure node as RPL Neighbour.
	NAG(config)# ethernet ring-protecti on <i>ring-id</i> east { port <i>port-id</i> port-channel <i>port-channel-number</i> } west { port <i>port-id</i> port-channel <i>port-channel-number</i> } [not-reverti ve] [protocol -vl an <i>vlan-id</i>] [block-vl an l i st <i>vlan-list</i>]	Create a ring and configure node as ring forwarding node.
3	NAG(config)# ethernet ring-protecti on <i>ring-id</i> name <i>string</i>	(Optional) configure the ring name. The length of name cannot exceed 32 characters.
4	NAG(config)# ethernet ring-protecti on <i>ring-id</i> versi on { 1 2 }	(Optional) configure protocol version. All nodes in one ring must be consistent. Version 1 differentiates rings through protocol VLAN, so different rings need to be configured with different protocol VLANs. So does version 2.

Step	Command	Description
5	NAG(config)# ethernet ring-protecti on ring-id guard-ti me guard-ti me	(Optional) after configured with the Guard timer, the faulty node does not process APS protocol packets during restoration time. In some big ring network, restoring node fault immediately may receive fault notice from neighbor nodes and cause link Down. Configuring the Guard timer of the ring can solve this problem.
6	NAG(config)# ethernet ring-protecti on ring-id wtr-ti me wtr-ti me	(Optional) configure the WTR timer of the ring. In revertive mode, wait the WTR timer to expire to switch back current link when the current link restores from a fault.
7	NAG(config)# ethernet ring-protecti on ring-id hol doff-ti me hol doff-ti me	(Optional) the system delays reporting the fault when the current link becomes faults after configuring the HOLDOFF timer of the ring; namely, traffic will switch to the protection link after a delayed time. This can avoid current link switching frequently.  Note If the HOLDOFF timer is set over greater, the performance of 50ms switching will be affected. Thus it is set to 0 by default.
8	NAG(config)# ethernet ring-protecti on trap enable	(Optional) enable G.8032 fault information to be reported to NMS.


5.1.5 (Optional) creating G.8032 sub-ring

Caution

- Only the intersecting ring network contains the master ring and sub-ring.
- Configurations of a master ring are identical to configurations of a single ring or tangent ring. For details, see section 5.1.4 Creating G.8032 ring.
- Configure the master ring before configuring the sub-ring; otherwise, the sub-ring cannot find the interface of the master ring and the virtual path of the sub-ring cannot be established.
- The ID of the sub-ring must be greater than that of the master ring.

Create a G.8032 sub-ring for SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.

Step	Command	Description
2	<pre>NAG(config)#ethernet ring-protecti on ring-id { east west } { port port-id port-channel port-channel -number } node-type rpl -owner [not-reverti ve] [protocol -vl an vlan-id] [block-vl an l i st vlan- list]</pre>	<p>Create sub-ring and configure node as RPL Owner on intersecting node.</p> <p> Note</p> <p>The link between two intersecting nodes in intersecting rings belongs to the master ring, so either east-bound or wester-bound interface can be configured for sub-ring.</p>
	<pre>NAG(config)#ethernet ring-protecti on ring-id { east west } { port port-id port-channel port-channel -number } node-type rpl -nei ghbour [not-reverti ve] [protocol -vl an vlan-id] [block-vl an l i st vlan- list]</pre>	<p>Create a sub-ring, and configure the node as the RPL Neighbour on intersecting nodes.</p>
	<pre>NAG(config)#ethernet ring-protecti on ring-id { east west } { port port-id port-channel port-channel -number } [not-reverti ve] [protocol -vl an vlan-id] [block-vl an l i st vlan- list]</pre>	<p>Create a sub-ring, and configure the node as ring forwarding node on intersecting nodes.</p>
3	<pre>NAG(config)#ethernet ring-protecti on ring-id raps-vc { wl th wl thout }</pre>	<p>(Optional) configure sub-ring virtual path mode on the intersecting node. Protocol packets transmitted in the sub-ring are different from that transmitted on the master ring, including with mode and without mode:</p> <ul style="list-style-type: none"> • with: the primary ring provides access for sub-ring APS packet; the intersecting node in the sub-ring will transmit sub-ring APS packets to the primary ring to use primary ring to complete the communications among sub-ring intersecting nodes. • without: the sub-ring APS packets on cross nodes need to be ended and cannot be transmitted to the primary ring. <p>By default, sub-ring virtual path is configured with the with parameter. Configuration mode of two intersecting nodes must be consistent.</p>

Step	Command	Description
4	NAG(confi g)# ethernet ring-protecti on ring-id propagate enable	<p>Enable the ring Propagate switch on intersecting nodes.</p> <p>Sub-ring data needs to be forwarded by the master ring, so the sub-ring MAC address table also exists on the master ring device. When the sub-ring has fault, the Propagate switch notifies the master ring of refreshing the MAC address table in time and thus avoids flow loss.</p> <p>By default, the Propagate switch is disabled. Use the ethernet ring-protection ring-id propagate disable command to disable this function.</p>

5.1.6 (Optional) configuring G.8032 switching control

Configure G.8032 switching control for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# ethernet ring-protecti on ring-id force-swi tch { east west }	Configure Forced Switching (FS) of ring flow.
3	NAG(confi g)# ethernet ring-protecti on ring-id manual -swi tch { east west }	<p>Configure Manual Switching (MS) of traffic on the ring.</p> <p>MS has a lower priority than FS or APS upon fault of the current link.</p>
4	NAG(confi g)# clear ethernet ring-protecti on ring-id { command stati stics }	Clear switch control command, including force-switch and manual-switch , WTR timer, and WTB timer.



Note

By default, traffic will be switched to the protection link when the current link fails. Thus G.8032 is needed in some special conditions.

5.1.7 Enabling association between ERPS and RSTP

Configure G.8032 switching control for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# ethernet ring-protecti on ring-id bpd u-snoopi ng [time-interval time] enable	Enable association between ERPS and RSTP.

5.1.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show ethernet ring-protecti on	Show G.8032 ring configuration.
2	NAG#show ethernet ri ng-protecti on status	Show G.8032 ring status information.
3	NAG#show ethernet ri ng-protecti on statl stl cs	Show G.8032 ring statistics.

5.1.9 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	NAG(confi g)#cl ear ethernet ri ng- protecti on <i>ring-ld</i> statl stl cs	Clear protection ring statistics.

5.1.10 Example for configuring single ring G.8032

Networking requirements

As show in Figure 5-1, to improve Ethernet reliability, the four switches Switch A, Switch B, Switch C, and Switch D build up a G.8032 single ring.

Switch A is the RPL Owner; Switch B is the RPL Neighbour; the RPL link between Switch A and Switch B is blocked.

By default, VLAN is 1, and the range of blocked VLANs is 1–4094.

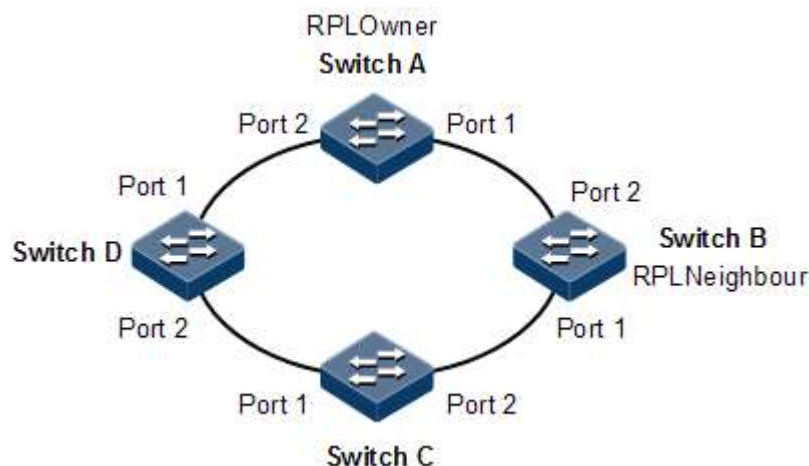


Figure 5-1 Single ring G.8032 networking

Configuration steps

Step 1 Add interfaces into VLANs 1–4094.

Configure Switch A.

```
NAG#hostname SwitchA
SwitchA#config
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
```

Configure Switch B.

```
NAG#hostname SwitchB
SwitchB#config
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
```

Configure Switch C.

```
NAG#hostname SwitchC
SwitchC#config
```

```
Swi tchC(confi g)#i nterface port 1
Swi tchC(confi g-port)#swi tchport mode trunk
Swi tchC(confi g-port)#exi t
Swi tchC(confi g)#i nterface port 2
Swi tchC(confi g-port)#swi tchport mode trunk
Swi tchC(confi g-port)#exi t
```

Configure Switch D.

```
NAG#hostname Swi tchD
Swi tchD#confi g
Swi tchD(confi g)#i nterface port 1
Swi tchD(confi g-port)#swi tchport mode trunk
Swi tchD(confi g-port)#exi t
Swi tchD(confi g)#i nterface port 2
Swi tchD(confi g-port)#swi tchport mode trunk
Swi tchD(confi g-port)#exi t
```

Step 2 Create G.8032 protection ring.

Configure Switch A.

```
Swi tchA(confi g)#ethernet ri ng-protecti on 1 east port 1 west port 2 node-
type rpl -owner rpl east
```

Configure Switch B.

```
Swi tchB(confi g)#ethernet ri ng-protecti on 1 east port 1 west port 2 node-
type rpl -nei ghbour rpl west
```

Configure Switch C.

```
Swi tchC(confi g)#ethernet ri ng-protecti on 1 east port 1 west port 2
```

Configure Switch D.

```
Swi tchD(confi g)#ethernet ri ng-protecti on 1 east port 1 west port 2
```

Checking results

Use the **show ethernet ring-protection status** command to show configurations of the G.8032 protection ring on the SNR-S212i-8POE.

Take Switch A for example. RPL link is blocked to avoid loopback. After the WTR timer expires, information about ring status is as below.

```
SwitchA#show ethernet ring-protection status
Id/Name Bridge-Status Last Occur(ago) East-State West-State Traffic-
Vlan list
-----
1       Idle 0 day 0:0:50:750 blocked forward 1-4094
```

Manually disconnect the link between Switch B and Switch C to emulate a fault. Use the following command to show G.8032 protection ring status on Switch A again. The RPL link switches to forwarding status.

```
SwitchA#show ethernet ring-protection status
Id/Name Bridge-Status Last Occur(ago) East-State West-State Traffic-
Vlan list
-----
1       Protection 0 day 0:0:55:950 forward forward 1-4094
```

5.1.11 Example for configuring intersecting G.8032

Networking requirements

As shown in Figure 5-2, to improve Ethernet reliability, Switch A, Switch B, Switch C, Switch D, Switch E and Switch F build up an intersecting G.8032 network.

- Switch A, Switch B, Switch C and Switch D build up the master ring, Switch D is master ring RPL Owner, and Switch C is master ring RPL Neighbour. Block Port 1 on Switch D, and protocol VLAN is default value 1.
- Switch A, Switch B, Switch E, and Switch F form a sub-ring, Switch F is secondary ring RPL Owner, and Switch A is sub-ring RPL Neighbour. Block Port 1 and Switch F, protocol VLAN is 4094. The VC mode of the sub-ring is with mode by default.

The range of blocked VLANs for the master ring and sub-ring is defaulted to VLANs 1–4094.

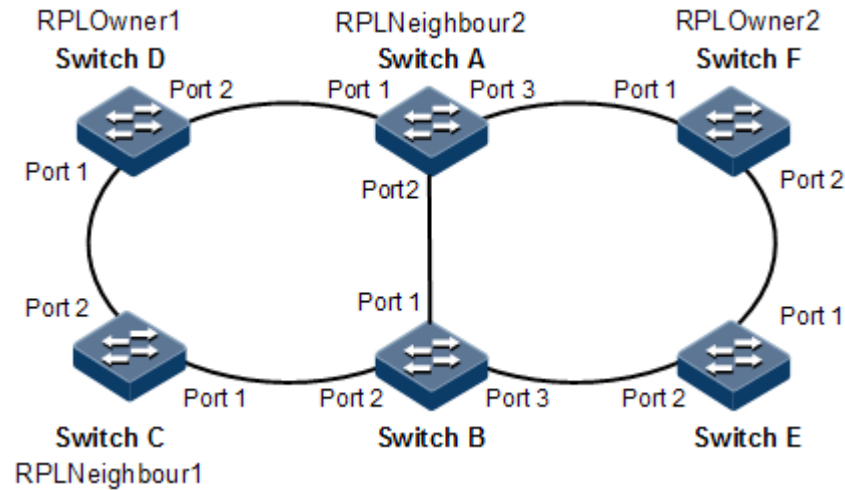


Figure 5-2 Intersecting ring G.8032 networking

Configuration steps

Step 1 Create VLAN 4094, and add interfaces into VLANs 1–4094.

Configure Switch A.

```
NAG#hostname Swit chA
Swit chA#confi g
Swit chA(confi g)#create vl an 4094 active
Swit chA(confi g)#i nterface port 1
Swit chA(confi g-port)#swi tchport mode trunk
Swit chA(confi g-port)#exi t
Swit chA(confi g)#i nterface port 2
Swit chA(confi g-port)#swi tchport mode trunk
Swit chA(confi g-port)#exi t
Swit chA(confi g)#i nterface port 3
Swit chA(confi g-port)#swi tchport mode trunk
Swit chA(confi g-port)#exi t
```

Configure Switch B.

```
NAG#hostname Swit chB
Swit chB#confi g
Swit chB(confi g)#create vl an 4094 active
Swit chB(confi g)#i nterface port 1
Swit chB(confi g-port)#swi tchport mode trunk
Swit chB(confi g-port)#exi t
Swit chB(confi g)#i nterface port 2
Swit chB(confi g-port)#swi tchport mode trunk
Swit chB(confi g-port)#exi t
Swit chB(confi g)#i nterface port 3
Swit chB(confi g-port)#swi tchport mode trunk
Swit chB(confi g-port)#exi t
```

Configure Switch C.

```
NAG#hostname Swi tchC
Swi tchC#confi g
Swi tchC(confi g)#create vl an 4094 active
Swi tchC(confi g)#i nterface port 1
Swi tchC(confi g-port)#swi tchport mode trunk
Swi tchC(confi g-port)#exi t
Swi tchC(confi g)#i nterface port 2
Swi tchC(confi g-port)#swi tchport mode trunk
Swi tchC(confi g-port)#exi t
```

Configure Switch D.

```
NAG#hostname Swi tchD
Swi tchD#confi g
Swi tchD(confi g)#create vl an 4094 active
Swi tchD(confi g)#I nterface port 1
Swi tchD(confi g-port)#swi tchport mode trunk
Swi tchD(confi g-port)#exi t
Swi tchD(confi g)#I nterface port 2
Swi tchD(confi g-port)#swi tchport mode trunk
Swi tchD(confi g-port)#exi t
```

Configure Switch E.

```
NAG#hostname Swi tchE
Swi tchE#confi g
Swi tchE(confi g)#create vl an 4094 active
Swi tchE(confi g)#i nterface port 1
Swi tchE(confi g-port)#swi tchport mode trunk
Swi tchE(confi g-port)#exi t
Swi tchE(confi g)#i nterface port 2
Swi tchE(confi g-port)#swi tchport mode trunk
Swi tchE(confi g-port)#exi t
```

Configure Switch F.

```
NAG#hostname Swi tchF
Swi tchF#confi g
Swi tchF(confi g)#create vl an 4094 active
Swi tchF(confi g)#i nterface port 1
Swi tchF(confi g-port)#swi tchport mode trunk
Swi tchF(confi g-port)#exi t
Swi tchF(confi g)#i nterface port 2
```

```
Swi tchF(confi g-port)#swi tchport mode trunk  
Swi tchF(confi g-port)#exi t
```

Step 2 Create a master ring for G.8032 protection.

Configure Switch A.

```
Swi tchA(confi g)#ethernet ri ng-protecti on 1 east port 1 west port 2
```

Configure Switch B.

```
Swi tchB(confi g)#ethernet ri ng-protecti on 1 east port 1 west port 2
```

Configure Switch C.

```
Swi tchC(confi g)#ethernet ri ng-protecti on 1 east port 1 west port 2 node-  
type rpl -nei ghbour rpl west
```

Configure Switch D.

```
Swi tchD(confi g)#ethernet ri ng-protecti on 1 east port 1 west port 2 node-  
type rpl -owner rpl east
```

Step 3 Configure the sub-ring for G.8032.

Configure Switch A.

```
Swi tchA(confi g)#ethernet ri ng-protecti on 2 east port 3 node-type rpl -  
nei ghbour protocol -vl an 4094  
Swi tchA(confi g)#ethernet ri ng-protecti on 2 propagate enable
```

Configure Switch B.

```
Swi tchB(confi g)#ethernet ri ng-protecti on 2 east port 3 protocol -vl an 4094  
Swi tchB(confi g)#ethernet ri ng-protecti on 2 propagate enable
```

Configure Switch E.

```
SwitchE(config)#ethernet ring-protection 2 east port 1 west port 2
protocol -vlan 4094
```

Configure Switch F.

```
SwitchF(config)#ethernet ring-protection 2 east port 1 west port 2 node-
type rpl -owner rpl east protocol -vlan 4094
```

Checking results

Use the **show ethernet ring-protection status** command to show configurations of the G.8032 protection ring on the SNR-S212i-8POE.

Use the command on Switch A, Switch D, and Switch F respectively. The result should be as below after the WTR timer expires.

```
SwitchA#show ethernet ring-protection status
Id/Name Bridge-Status Last Occur(ago) East-State West-State Traffic-
vlan list
-----
1       idle        0 day 0: 0: 50: 750   forward   forward   1-4094
-----
2       idle        0 day 0: 0: 50: 750   forward   forward   1-4094
```

```
SwitchD#show ethernet ring-protection status
Id/Name Bridge-Status Last Occur(ago) East-State West-State Traffic-
vlan list
-----
1       idle        0 day 0: 0: 50: 750   block     forward   1-4094
```

```
SwitchF#show ethernet ring-protection status
Id/Name Bridge-Status Last Occur(ago) East-State West-State sc
Traffic-vlan list
-----
2       idle        0 day 0: 0: 50: 750   block     forward   1-4094
```

5.2 RRPS

5.2.1 Introduction

With the development of Ethernet to the MAN, voice, video and multicast services have come up with higher requirements to the Ethernet redundancy protection and fault recovery time. The fault recovery convergence time of original STP mechanism is in the second level, which is far from meeting the fault recovery time requirements of MAN.

Redundant Ring Protection Switching (RRPS) technology is SNR independent research and development protocol, which can ensure that there is data loop in Ethernet by blocking some interface on the ring. Once there is link failure, the node immediately sends link failure packets to other nodes. The primary node will restore the blocked interface to implement fast switching upon link failure. When the failed link is restored, the primary node obtains the link restoration information, and then reblocks the backup interface. Then, all links work normally as before.

RRPS solves the problems of weak protection to traditional data network and long time to fault recovery, which, in theory, can provide 50ms rapid protection features.

According to RRPS, the node where the blocked interface is is called the primary node while other nodes are transmission nodes. The primary node is elected. The two interfaces on two rings on each node can be respectively assigned as the primary interface and secondary interface.

Principle of RRPS

RRPS generates the primary node by election, so each node needs to collect device information on RRPS, only the right collection leads to correct election. Topology collection is completed by Hello packets, which contain all nodes information collected from the other interface.

- RRPS normal state

The normal state of RRPS is shown in Figure 5-3. Each node on the ring sends Hello packets birectionally and periodically to collect node information, thus electing for the primary node. At the beginning, each node considers itself as the primary node, so one of the two interfaces on each node is blocked and there is no loop. When the two interfaces on a node receive the same Hello packet, the node considers that the ring network is stable and ready for electing for the primary node. Other non-primary nodes will restore blocked interfaces, so only one interface is blocked on the ring and node connectivity is guaranteed. As shown in Figure 5-3, Switch D is elected as the RRPS primary node.

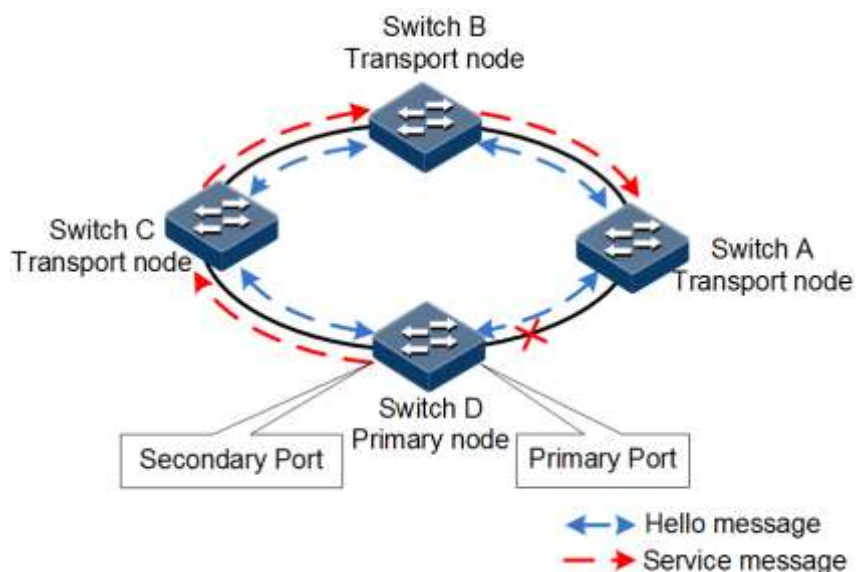


Figure 5-3 RRPS normal status

RRPS switching status is as shown in Figure 5-4. When the faulty link is restored, the faulty node will not immediately restore the blocked interface. When the new topology collection is

stable, nodes on the ring elect for the primary node. The new master ring finds itself the primary node, and then block the primary interface after a delay. It sends the Change packet to the primary node to notify the primary node of switching the link. After receiving the Change packet, the primary node immediately restores the blocked primary interface, and sends the Flush packet to notify other nodes and links of changing the transmission direction and refreshing Forwarding Database (FDB). Traffic is switched back to the normal link.

As shown in Figure 5-4, the link between Switch A and Switch B fails. After the primary node Switch D restores the blocked interface, Switch A and Switch B consider themselves as the primary node respectively, so they block their secondary interfaces. After the new topology collection is stable, one of the two faulty nodes is elected as the primary node. Since the other node is not the primary node any more, it restores the blocked interface. Thus, node connectivity on the ring is guaranteed.

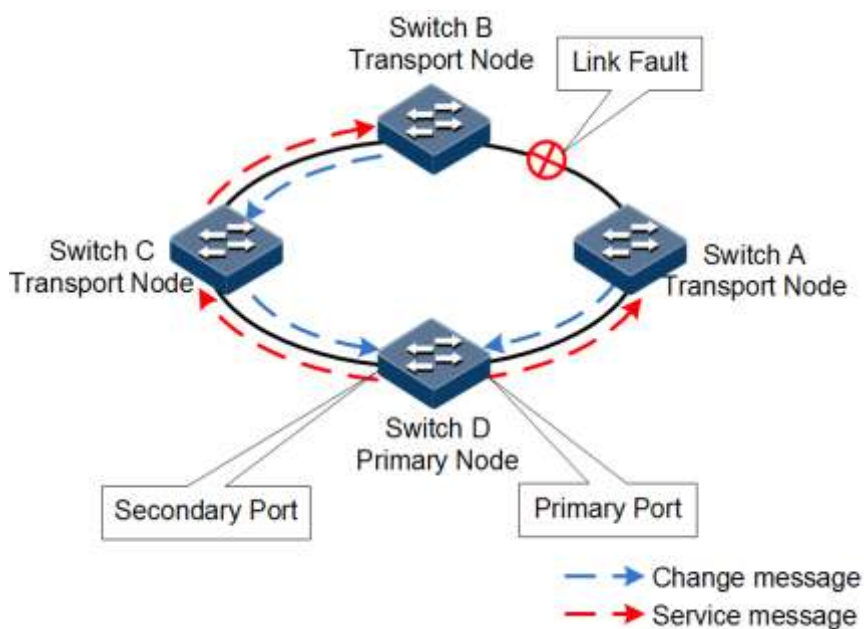


Figure 5-4 RRPS switching status

- RRPS link restoration

RRPS link restoration is as shown in Figure 5-5. When the faulty link is restored, the faulty node will not immediately restore the blocked interface. When the new topology collection is stable, nodes on the ring elect for the primary node. The new master ring finds itself the primary node, and then block the primary interface after a delay. It sends the Change packet to the faulty node to restores the blocked interface, and sends the Change_Relay packet to notify neighbor nodes of sending the Change packet to the faulty node.

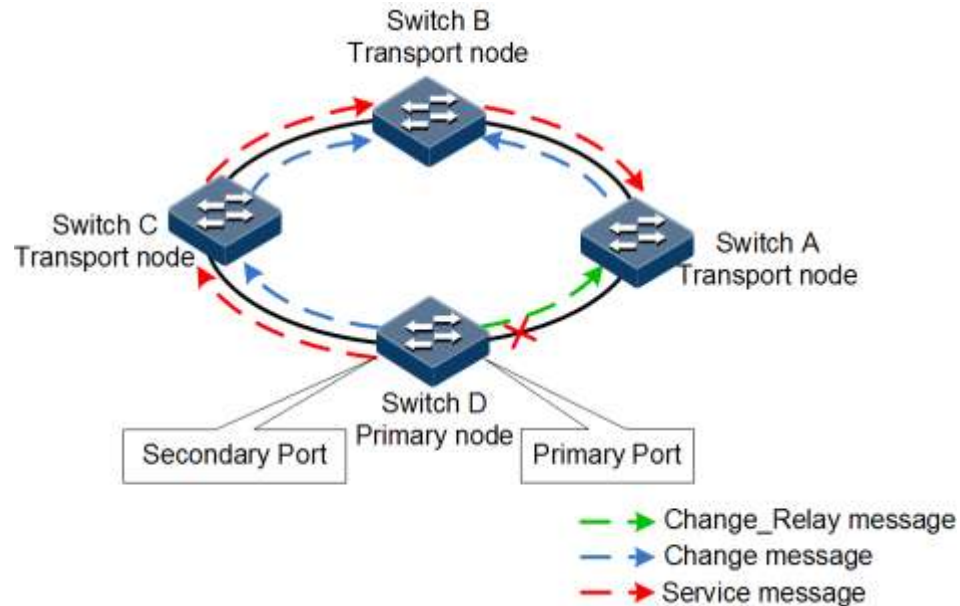


Figure 5-5 RRPS link restoration

Ring node status

According to the interface state of node ring, the ring node statuses can be divided into three types:

- Down: if at least one of the two interfaces on the RRPS node is Down, the node is Down.
- Block: if at least one of the two interfaces on the RRPS node is Block, the node is Block.
- Two-Forwarding: if two interfaces on the RRPS node are Forwarding, the node is Two-Forwarding.

Rules for electing for primary node

Rules for electing for the primary node are as below:

- In all nodes on the ring, the node with Down state is prior for the primary node, followed by Block and Two-Forward.
- If the nodes are in the same state, the node with high priority RRPS is the primary node.
- If the nodes have the same state and priority, the node with the large MAC address is the primary node.

Rules for blocking interfaces

Rules for blocking interfaces are as below:

- All Down interfaces are blocked.
- If the node is not the primary node, its Up interfaces on the ring are forwarding.
- If the node is the primary node, then one of two interfaces is blocked, the other is forwarding. Rules are as below:
 - If both interfaces are Up, the primary interface is blocked.
 - If one is Down, then it is blocked.

For other nodes on the RRPS, the primary interface ID and secondary interface ID are the same.

5.2.2 Preparing for configurations

Scenario

RRPS technology is NAG independent research and development protocol, which through simple configuration implements the elimination of ring loop, fault protection switching, and automatic fault restoration and makes the fault APS time less than 50ms.

RRPS technology supports both single ring and tangent ring networking modes, instead of intersecting ring networking. The tangent ring is actually two separate single rings, which has same configurations with those of a common single ring.

Prerequisite

N/A

5.2.3 Default configurations of RRPS

Default configurations of RRPS are as below.

Function	Default value
RRPS status	Disable
Hello packets transmitting time	1s
Fault recovery delay time	5s
RRPS description information	Ethernet ring X. X indicates RRPS ID.
Bridge priority	1
Ring interface aging time	15s
Ring protocol packets VLAN	4093

5.2.4 Creating RRPS



Note

The RRPS ring supports being configured on a physical interface and LAG interface.

Create a RRPS ring as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# I nterface <i>i nterface-type p rimary-</i> <i>i nterface-number</i>	Enter physical layer interface configuration mode. This interface is the primary interface on the ring node.

Step	Command	Description
3	NAG(config-port)# ethernet ring ring-id interface-type secondary-interface-number	Create a ring and configure corresponding ring interface. This interface is the second interface of ring node.
4	NAG(config-port)# exit NAG(config)# ethernet ring ring-id enable	Enable the Ethernet ring.

5.2.5 Configuring basic functions of RRPS




Caution

- For all devices in the same ring, we recommend configuring the fault recovery time and Hello packets interval, ring protocol VLAN, and aging time of ring interface separately for the same value.
- The aging time of an interface must be greater than twice of Hello time.

Configure basic functions of RRPS for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(config)# ethernet ring ring-id hel lo-ti me hel lo-ti me	(Optional) configure the interval for sending Hello packets in RRPS.
3	NAG(config)# ethernet ring ring-id restore-del ay del ay-ti me	(Optional) configure fault restoration delay time for RRPS. The link can be restored to the original current link until the restoration delay time expires.
4	NAG(config)# ethernet ring ring-id pri ori ty pri ori ty	(Optional) configure the bridge priority for RRPS.
5	NAG(config)# ethernet ring ring-id descri ption string	(Optional) configure ring description.
6	NAG(config)# ethernet ring ring-id hol d-ti me hol d-ti me	(Optional) configure the aging time of the interface for RRPS. If a RRPS interface has not received Hello packets in the aging time, the system ages this interface and considers that the link circuit on link ring is fault. If the node interface is in Block state, it will enable the blocked interface temporarily to ensure the normal communication of all nodes on RRPS.
7	NAG(config)# ethernet ring ring-id protocol -vl an vl an-id	(Optional) configure RRPS VLANs.

Step	Command	Description
8	<code>NAG(config)#ethernet ring upstream-group group-list</code>	(Optional) configure RRPS uplink interface group.  Note The uplink interface group must be used with failover. It supports dual homing topology. The uplink interface group corresponds to the failover group in one-to-one relationship.

5.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>NAG#show ethernet ring [ring-id]</code>	Show RRPS configurations.
2	<code>NAG#show ethernet ring port</code>	Show configurations of the RRPS interface.
3	<code>NAG#show ethernet ring port statistic</code>	Show statistics of packets on the RRPS interface.

5.2.7 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	<code>NAG(config)#clear ethernet ring ring-id statistics</code>	Clear RRPS interface statistics.

5.2.8 Example for configuring RRPS

Networking requirements

As shown Figure 5-6, to improve the reliability of Ethernet, Switch A, Switch B, Switch C, Switch D form an Ethernet single ring Ring 1.

MAC addresses of four switches are as below:

- Switch A: 000E.5E00.000A
- Switch B: 000E.5E00.000B
- Switch C: 000E.5E00.000C
- Switch D: 000E.5E00.000D

The statuses and priorities of four switches are the same. The MAC address of Switch D is the biggest, so Switch D is the primary node of RRPS.

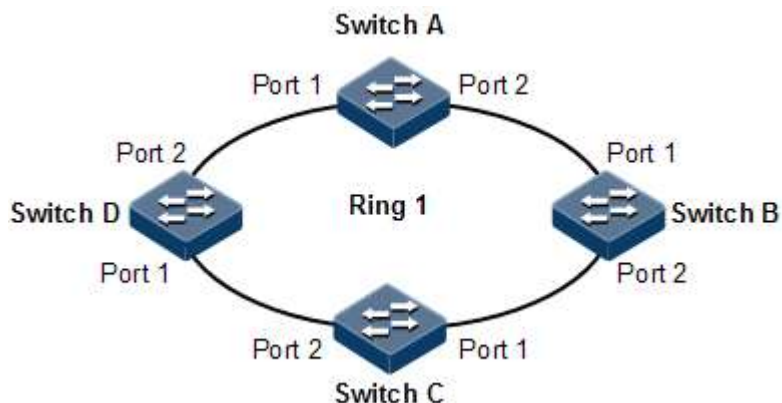


Figure 5-6 RRPS networking

Configuration steps

Step 1 Configure Switch A.

```
NAG#hostname SwitchA
SwitchA#config
SwitchA(config)#interface port 1
SwitchA(config-port)#ethernet ring 1 port 2
SwitchA(config-port)#exit
SwitchA(config)#ethernet ring 1 enable
```

Step 2 Configure Switch B, Switch C, and Switch D. Their configurations are the same as configurations of Switch A.

Checking results

Use the **show ethernet ring** command to show RRPS configurations.

Take Switch D for example. When the loop is normal, the first ring interface of the primary node Switch D is Port 1, and data loop is cleared.

```
SwitchD#show ethernet ring
Ethernet Ring Upstream PortList: --
Ethernet Ring 1:
Ring Admin:      Enable
Ring State:      Enclosed
Bridge State:    Block
Ring state duration: 0 days, 3 hours, 30 minutes, 15 seconds
Bridge Priority: 1
Bridge MAC:      000E.5E00.000D
Ring DB State:   Block
Ring DB Priority: 1
```

```
Ring DB:          000E. 5E00. 000D
Hello Time:      1
Restore delay:   5
Hold Time:       15
Protocol Vlan:   4093
```

Disconnect the link to emulate a fault between Switch A and Switch B manually, so Port 1 on Switch D will change its status from Block to Forwarding, Port 1 on Switch B will change its status from Forwarding to Block. Use the command to check RRPS status again.

```
SwitchD#show ethernet ring
Ethernet Ring Upstream PortList: --
Ethernet Ring 1:
Ring Admin:      Enable
Ring State:      Unenclosed
Bridge State:    Two-Forward
Ring state duration: 0 days, 3 hours, 30 minutes, 15 seconds
Bridge Priority: 1
Bridge MAC:      000E. 5E00. 000D
Ring DB State:   Block
Ring DB Priority: 1
Ring DB:         000E. 5E00. 000B
Hello Time:     1
Restore delay:  5
Hold Time:      15
Protocol Vlan:  4093
```


6 IP services

This chapter describes basic principle and configuration of routing features, and provides the related configuration examples, including the following sections:

- Layer 3 interface
- Loopback interface
- ARP
- DHCP Client
- DHCP Server
- DHCP Relay
- DHCP Snooping
- DHCP Options

6.1 Layer 3 interface

6.1.1 Introduction

The Layer 3 interface refers to the IP interface, and it is the virtual interface based on VLAN. Configuring Layer 3 interface is generally used for network management or routing link connection of multiple devices. Associating a Layer 3 interface to VLAN requires configuring IP address; each Layer 3 interface will correspond to an IP address and associate with at least one VLAN.

If only one IP address is configured on Layer 3 interface of the SNR-S212i-8POE, only part of hosts can communicate with external networks through the switch. To enable all hosts to communicate with external networks, configure the secondary IP address of the interface. To enable hosts in two network segments to interconnect with each other, set the switch as the gateway for all hosts.

6.1.2 Preparing for configurations

Scenario

You can connect a Layer 3 interface for VLAN when configuring its IP address. Each Layer 3 interface will correspond to an IP address and connects to a VLAN.

Prerequisite

Configure the VLAN associated with interface and make it activated.

6.1.3 Default configurations of Layer 3 interface

Default configurations of the Layer 3 interface are as below.

Function	Default value
Management VLAN TPID	0x8100
Management VLAN inner VLAN	1
Management VLAN CoS	0
IP address of IP interface 0	192.168.0.1
Mapping between the Layer 3 interface and VLAN	IP interface 0 is mapped to VLAN 1.

6.1.4 Configuring Layer 3 interface

Configure the IP address of the Layer 3 interface for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i nterface i p i f- <i>number</i>	Enter Layer 3 interface configuration mode.
3	NAG(confi g-i p)# i p address <i>i p-address [i p-mask]</i> <i>[sub] [v lan-list]</i>	Configure the IP address of the Layer 3 interface, and associate it with a VLAN.



Note

- Configure the VLAN associated with the Layer 3 interface, and the VLAN must be activated. Use the **state { active | suspend }** command to activate and then configure the suspended VLAN.
- Up to 15 Layer 3 interfaces can be configured, and they range from 0 to 14.

6.1.5 Configuring mapping between Layer 3 interface and VLAN

Configure mapping between the Layer 3 interface and VLAN for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i nterface i p i f- <i>number</i>	Enter Layer 3 interface configuration mode.

Step	Command	Description
3	NAG(config-g-i-p)#ip vlan <i>vlan-list</i>	Configure mapping between the Layer 3 interface and VLAN.

6.1.6 Configuring mapping between Layer 3 interface and physical interface

Configure mapping between the Layer 3 interface and physical interface for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(config)#i nterface i p <i>if-number</i>	Enter Layer 3 interface configuration mode.
3	NAG(config-g-i-p)#i p address <i>ip-address</i> [<i>ip-mask</i>] [<i>sub</i>] [<i>vlan-list</i>]	Configure the IP address of the Layer 3 interface, and associate it with a VLAN.
4	NAG(config-g-i-p)#i p vlan <i>vlan-list</i> NAG(config-g-i-p)#exi t	(Optional) configure mapping between the Layer 3 interface and physical interface.
5	NAG(config)#i nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
6	NAG(config-g-port)#swi tchport mode access NAG(config-g-port)#swi tchport access vlan <i>vlan-id</i>	Configure the interface to Access mode, and configure the Access VLAN of the interface.
	NAG(config-g-port)#swi tchport mode trunk NAG(config-g-port)#swi tchport trunk nati ve vlan <i>vlan-id</i>	Configure the interface to Trunk mode, and configure the Native VLAN of the interface.

6.1.7 Configuring management VLAN attributes

Configure management VLAN attributes for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(config)#i nterface i p <i>if-number</i>	Enter Layer 3 interface configuration mode.
3	NAG(config-g-i-p)#i p management-traffic cos <i>cos-value</i>	Configure CoS of the management VLAN.
4	NAG(config-g-i-p)#i p management-traffic tpid <i>tp-id</i>	Configure outer TPID of the management VLAN.

Step	Command	Description
5	<code>NAG(config-ip)#ip management-traffic mode double-tagging [inner-vlan <i>vlan-id</i> inner-cos <i>cos-value</i>]</code>	Configure double Tag mode for management packets.

6.1.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>NAG#show ip interface brief</code>	Show configurations of the IP address of the Layer 3 interface.
2	<code>NAG#show interface ip vlan</code>	Show mapping between the Layer 3 interface and VLAN.
3	<code>NAG#show ip management-traffic</code>	Show configurations of management VLAN.

6.1.9 Example for configuring Layer 3 interface to interconnect with host

Networking requirements

As shown in Figure 6-1, configure the Layer 3 interface to the switch so that the host and the SNR-S212i-8POE can Ping each other.

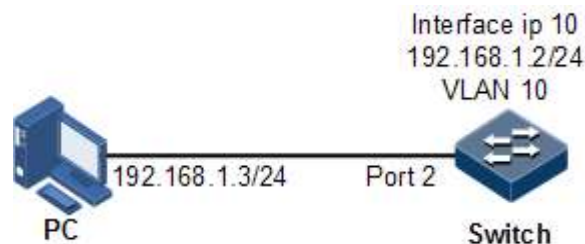


Figure 6-1 Layer 3 interface configuration networking

Configuration steps

Step 1 Create a VLAN and add the interface into the VLAN.

```

NAG#confi g
NAG(config)#create vlan 10 active
NAG(config)#interface port 2
NAG(config-port)#switchport access vlan 10
NAG(config-port)#exit
  
```

- Step 2 **Configure Layer 3 interface on the SNR-S212i-8POE, configure its IP address, and associate the interface with the VLAN.**

```
NAG(confi g)#I nterface I p 10
NAG(confi g-i p)#I p address 192. 168. 1. 2 255. 255. 255. 0 10
```

Checking results

Use the **show vlan** command to show mapping between the physical interface and VLAN.

```
NAG#show vl an 10
Swi tch Mode: --
VLAN: 10
Name: VLAN0010
State: acti ve
Status: stati c
Pri ori ty: --
Member-Ports: port-l ist2
```

Use the **show ip interface brief** to show configurations of the Layer 3 interface.

```
NAG#show I p I nterface bri ef
I F    Address          NetMask          Source          Catagory
-----
10    192. 168. 1. 2    255. 255. 255. 0    assi gned      pri mary
```

Use the **show interface ip vlan** command to show mapping between the Layer 3 interface and VLAN.

```
NAG#show I nterface I p vl an
I p I nterface  Vl an I st
-----
0              1
...
10             10
...
```

Use the **ping** command to check whether the SNR-S212i-8POE and PC can ping each other.

```
NAG#pi ng 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.
```

6.2 Loopback interface

6.2.1 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 that 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.

Loopback interface status is free from physical interface status (Up/Down). As long as the SNR-S212i-8POE is operating normally, the loopback interface will not become Down. Thus, it is used to identify the physical device as a management address.

6.2.2 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.

Prerequisite

N/A

6.2.3 Default configurations of loopback interface

N/A

6.2.4 Configuring IP address of loopback interface

Configure the IP address of the loopback interface for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#I nterface l oopback l b-number</code>	Enter loopback interface configuration mode.
3	<code>NAG(confi g-l oopback)#l p address i p-address [i p- mask]</code>	Configure the IP address of the loopback interface.

6.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>NAG#show i nterface l oopback</code>	Show loopback interface configurations.

6.3 ARP

6.3.1 Introduction

In TCP/IP network environment, each host is assigned with a 32-bit IP address that is a logical address used to identify hosts between networks. To transmit packets in physical link, you must know the physical address of the destination host, which requires mapping the IP address to the physical address. In Ethernet environment, the physical address is 48-bit MAC address. The system has to translate the 32-bit IP address of the destination host into the 48-bit Ethernet address for transmitting packet to the destination host correctly. Then Address Resolution Protocol (ARP) is applied to resolve IP address to MAC address and set mapping relationship between IP address and MAC address.

ARP address table includes the following two types:

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

The SNR-S212i-8POE supports the following two modes of dynamically learning ARP address entries:

- Learn-all: in this mode, the SNR-S212i-8POE learns both ARP request packets and response packets. When device A sends its ARP request, it writes mapping between its IP address and physical address in ARP request packets. When device B receives ARP

request packets from device A, it learns the mapping in its address table. In this way, device B will no longer send ARP request when sending packets to device A.

- learn-reply-only mode: in this mode, the SNR-S212i-8POE learns ARP response packets 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, network load is heavier but some network attacks based on ARP request packets can be prevented.

6.3.2 Preparing for configurations

Scenario

The mapping of IP address and MAC address is saved in the ARP address table.

Generally, the ARP address table is dynamically maintained by the SNR-S212i-8POE. The SNR-S212i-8POE searches for the mapping between IP address and MAC address automatically according to ARP. You just need to configure the SNR-S212i-8POE manually for preventing ARP dynamic learning from cheating and adding static ARP address entries.

Prerequisite

N/A

6.3.3 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-reply-only

6.3.4 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 SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#arp <i>ip-address</i> <i>mac-address</i>	Configure static ARP entry.

6.3.5 Configuring dynamic ARP entries

Configure dynamic ARP entries for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# arp mode { learn-all learn-reply-only }	(Optional) configure dynamic ARP entry learning mode.
3	NAG(confi g)# interface ip <i>if-number</i>	Enter Layer 3 interface configuration mode.
4	NAG(confi g-ip)# arp max- learni ng-num <i>number</i>	(Optional) configure the maximum number of dynamic ARP entries allowed to learn on the Layer 3 interface.

6.3.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG# show arp	Show information about ARP entries.
2	NAG# show arp <i>ip-address</i>	Show ARP entries related to the specified IP address.
3	NAG# show arp ip <i>if-number</i>	Show ARP entries related to the Layer 3 interface.
4	NAG# show arp stati c	Show information about static ARP entries.

6.3.7 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	NAG(confi g)# cl ear arp	Clear all entries in the ARP address table.

6.3.8 Configuring ARP

Networking requirements

As shown in Figure 6-2, the SNR-S212i-8POE connects to the host, and connects to upstream Router by Port 1. For the Router, the IP address is 192.168.1.10/24, the subnet mask is 255.255.255.0, and the MAC address is 0050-8d4b-fd1e.

To improve communication security between Device and Router, you need to configure related static ARP entry on the SNR-S212i-8POE.

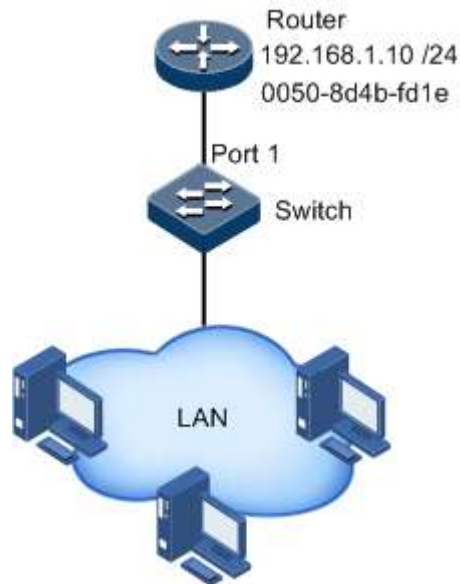


Figure 6-2 Configuring ARP networking

Configuration steps

Add an static ARP entry.

```
NAG#confi g
NAG(confi g)#arp 192.168.1.10 0050.8d4b.fd1e
```

Checking results

Use the **show arp** command to show configurations of the ARP address table.

```
NAG#show arp
ARP mode: Learn reply only
Ip Address      Mac Address      Interface  Type  Age(s)
-----
192.168.1.10    0050.8d4b.fd1e   0          stati c  --
192.168.100.1   000F.E212.5CA0   1          dynami c  3

Total : 2
Stati c : 1
Dynami c : 1
```

6.4 DHCP Client

6.4.1 Introduction

Dynamic Host Configuration Protocol (DHCP) refers to assign IP address configurations dynamically for users in TCP/IP network. It is based on BOOTP (Bootstrap Protocol) protocol, and automatically adds functions such as automatically assigning available network addresses, reusing network addresses, and other extended configuration options.

With 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 notebooks 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 IP address for the client and other related configurations to implement dynamic configurations of IP address, etc.

Typical applications of DHCP usually include a set of DHCP server and multiple clients (for example PC or Notebook), as shown in Figure 6-7.

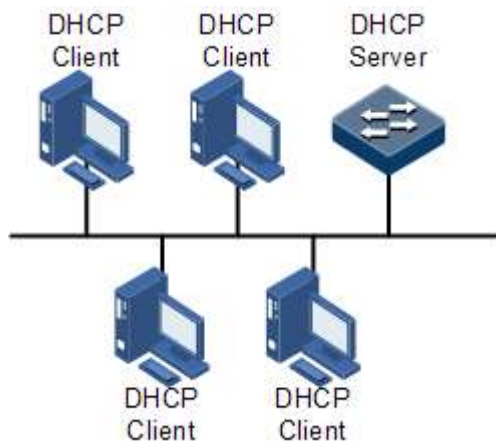


Figure 6-3 DHCP typical networking

DHCP technology ensures rational allocation, avoid waste and improve the utilization rate of IP addresses in the entire network.

Figure 6-4 shows structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

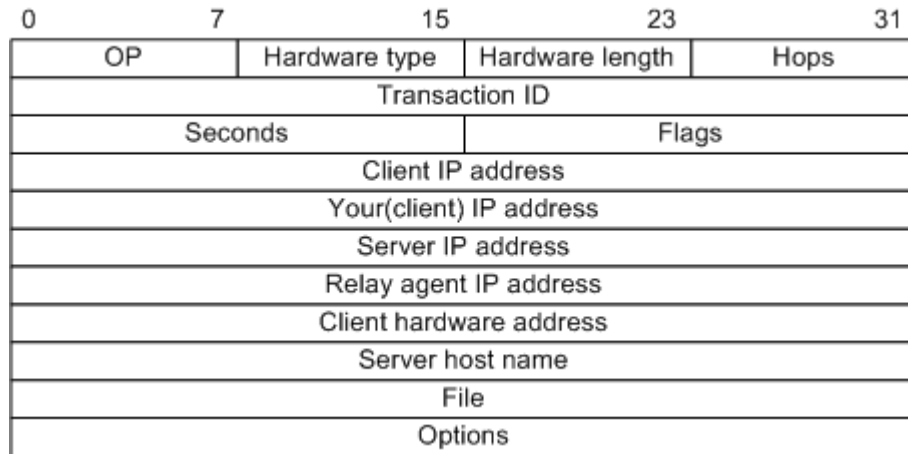


Figure 6-4 Structure of DHCP packet

Table 6-1 describes fields of DHCP packets.

Table 6-1 Fields of 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 size of a DHCP client.
Hops	1	DHCP hops number passed from DHCP packet. This field increases 1 every time DHCP request packet passes a DHCP hop.
Transaction ID	4	The client chooses a number at random when starting a request, used to mark process of address request.
Seconds	2	Passing time for the DHCP client after starting DHCP request. It is unused now, fixed as 0.
Flags	2	Bit 1 is the broadcast reply flag, used to mark whether the DHCP server replies packets in unicast or broadcast mode. <ul style="list-style-type: none"> • 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

Field	Length	Description
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 leased period, Domain Name System (DNS) server IP address, Windows Internet Name Server (WINS) IP address, etc. information.

The SNR-S212i-8POE can be used as DHCP client to get IP address from the DHCP server for future management, as shown in Figure 6-5.

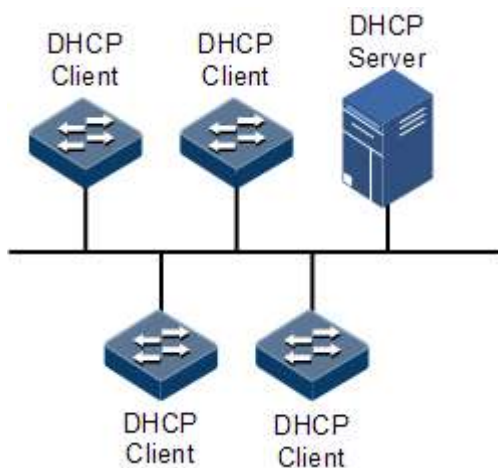


Figure 6-5 DHCP Client networking

6.4.2 Preparing for configurations

Scenario

As a DHCP client, the SNR-S212i-8POE obtains its IP address from the DHCP server.

The IP address assigned by the DHCP client is limited with a certain lease period when adopting dynamic assignment of IP addresses. The DHCP server will take back the IP address when it is expired. The DHCP client has to relet 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 setting 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 a VLAN and add Layer 3 interface to it.
- DHCP Snooping is disabled.

6.4.3 Default configurations of DHCP Client

Default configurations of DHCP Client are as below.

Function	Default value
hostname	NAG
class-id	NAG-ROS
client-id	NAG-SYSMAC-IF0

6.4.4 Configuring DHCP Client

Only interface IP 0 on the SNR-S212i-8POE supports DHCP Client.


When applying for an IP address, the DHCP client needs to create a VLAN firstly, and add the interface with the IP address to the VLAN. Meanwhile configure DHCP server; otherwise the interface will fail to obtain IP address through DHCP.

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

**Note**

- If the SNR-S212i-8POE is enabled with DHCP Server or DHCP Relay, DHCP Client cannot be enabled. Vice versa.
- By default, the SNR-S212i-8POE is enabled with DHCP Client. Use the **no ip address dhcp** command to disable DHCP Client.
- If the SNR-S212i-8POE 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 SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i nterface i p 0	Enter Layer 3 interface configuration mode.
3	NAG(confi g-i p)# i p dhcp client { class-id <i>class-id</i> client-id <i>client-id</i> hostname <i>hostname</i> }	<p>(Optional) configure DHCP client information, including type identifier, client identifier, and host name.</p> <p> Caution</p> <p>After the IP address is obtained through DHCP, client information cannot be modified.</p>

Step	Command	Description
4	NAG(config-i p)# ip address dhcp [server-ip ip-address]	Configure obtaining IP address through DHCP.
5	NAG(config-i p)# ip dhcp client renew	(Optional) relet IP address. If the Layer 3 interface of device has obtained IP address through DHCP, the IP address will automatically renew when the lease expires.
6	NAG(config-i p)# no ip address dhcp	(Optional) release the IP address.

6.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG# show ip dhcp client	Show configurations of DHCP Client.

6.4.6 Example for configuring DHCP Client

Networking requirements

As shown in Figure 6-6, the Switch is used as DHCP client, and the host name is **NAG**. The Switch is connected to the DHCP server and NMS platform. The DHCP server should assign IP addresses to the SNMP interface of the Switch and make NMS platform to manage the Switch.

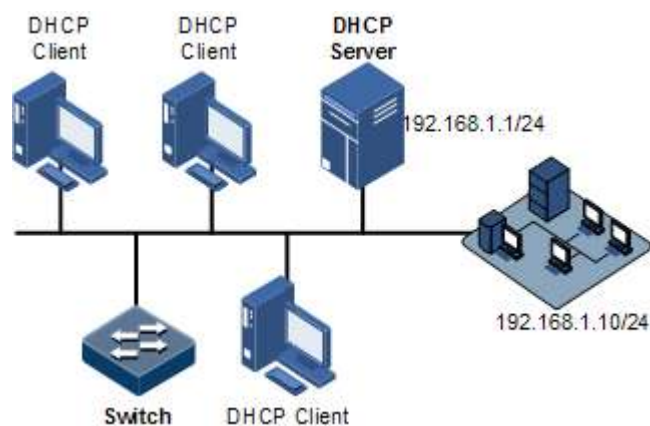


Figure 6-6 DHCP client networking

Configuration steps

Step 1 Configure DHCP client information.

```
NAG#confi g
NAG(confi g)#i nterface i p 0
NAG(confi g-i p)#i p dhcp client hostname NAG
```

Step 2 Configure applying for IP address through DHCP.

```
NAG(confi g-i p)#i p address dhcp server-i p 192.168.1.1
```

Checking results

Use the **show ip dhcp client** command to show configurations of DHCP Client.

```
NAG#show i p dhcp client
Hostname:                NAG
Class-ID:                NAG-ROS
Client-ID:               NAG-000e5e000000-IF0
DHCP Client is requesti ng 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:     --
Startup_confi g filename: --
NTP server IP Addr:     --
Root path:               --
```

6.5 DHCP Server

6.5.1 Introduction

DHCP works in client/server mode, so a specified server assigns network addresses and transmits configured parameters to hosts on the network. The specified server is called the the DHCP server.

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 the number of IP addresses, which make it unable to assign a fixed IP address for each host, and restrict the number of users connected to network simultaneously.

- A large number of users must obtain their own IP address dynamically through DHCP service.
- Only the minority of hosts on the network need fixed IP addresses, most of hosts have no requirement for fixed IP address.

The SNR-S212i-8POE can work as the DHCP server to assign dynamic IP addresses for clients, as shown in Figure 6-7.

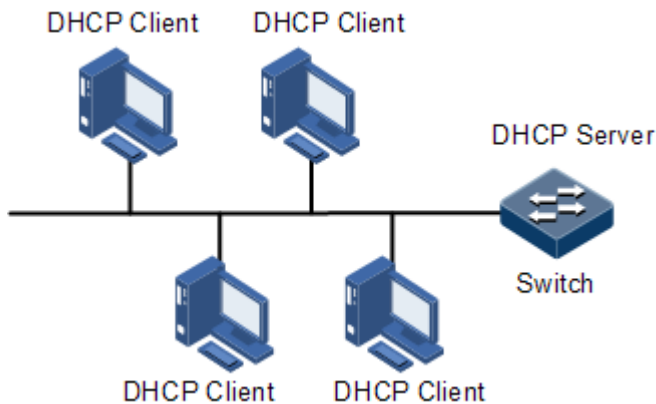


Figure 6-7 DHCP Server networking

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 leased period. You can specify the duration of the leased period.

6.5.2 Preparing for configurations

Scenario

DHCP works in client/server mode, so a specified server assigns network addresses and transmits configured parameters to hosts on the network.

You need to configure DHCP Server when using SNR-S212i-8POE to provide dynamic IP address for other devices.

Prerequisite

DHCP Server is exclusive to DHCP Client or DHCP Snooping. Namely, you cannot configure DHCP Client or DHCP Snooping on the device to be configured with DHCP Server.

6.5.3 Default configurations of DHCP Server

Default configurations of DHCP Server are as below.

Function	Default value
Global DHCP Server	Disable
IP port DHCP Server	Disable
Address pool	N/A

Function	Default value
Global leased period	<ul style="list-style-type: none"> • Maximum leased period: 10080 minutes • Minimum leased period: 30 minutes • Default leased period: 30 minutes
Address pool leased period	<ul style="list-style-type: none"> • Maximum leased period: 10080 minutes • Minimum leased period: 30 minutes • Default leased period: 30 minutes
Trusted relay address	N/A

6.5.4 Configuring DHCP Server

Configure DHCP Server for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#i p dhcp server</code>	Enable global DHCP Server.
3	<code>NAG(confi g)#i p dhcp server default -lease { minute infinite }</code>	(Optional) configure global default leased period.
4	<code>NAG(confi g)#i p dhcp server min-lease { minute infinite }</code>	(Optional) configure global minimum leased period. The value infinite indicates an infinite leased period.
5	<code>NAG(confi g)#i p dhcp server max-lease { minute infinite }</code>	(Optional) configure global maximum leased period. The value infinite indicates an infinite leased period.

6.5.5 Configuring address pool

To enable the DHCP server to assign IP addresses and network parameters for clients, you must create an address pool on the DHCP server.

Configure the address pool for the SNR-S212i-8POE as below.


Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#i p dhcp server pool pool-name</code>	Create an address pool, and enter address pool mode.
3	<code>NAG(dhcp-pool)#address start-ip-address end-ip-address mask { ip-mask mask-length }</code>	Configure the range of IP addresses and mask of the address pool.

Step	Command	Description
4	NAG(dhcp-pool)#lease default { minute infinite } [min { minute infinite }] [max { minute infinite }]	(Optional) configure the default, minimum, maximum leased period for the address pool. The value infinite indicates an infinite leased period.
5	NAG(dhcp-pool)#dns-server ip-address	(Optional) configure the DNS server address of the address pool.
	NAG(dhcp-pool)#dns-server secondary ip-address	(Optional) configure the IP address of the secondary DNS server of the address pool.
6	NAG(dhcp-pool)#gateway ip-address	(Optional) configure the default gateway of the address pool.
7	NAG(dhcp-pool)#tftp-server ip-address	(Optional) configure the TFTP server address of the address pool.
	NAG(dhcp-pool)#bootfile file-name	(Optional) configure the boot file name of the address pool.

6.5.6 Configuring DHCP Server on IP interface

Only when the global and IP interfaces are enabled with DHCP Server and the address pools are bound to the IP interface, can the IP interface receives and processes DHCP request packets from clients.

Configure DHCP Server on the IP interface for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#i nterface ip ip-number	Enter Layer 3 interface configuration mode.
3	NAG(confi g-i p)#i p dhcp server	Enable DHCP Server on the IP interface.
4	NAG(confi g-i p)#i p address ip-address	Configure the IP address of the interface.
5	NAG(confi g-i p)#i p vlan vlan-id	Configure VLAN related to the IP interface.  Note If the IP interface is not related to any VLAN, create a VLAN and make them associated.
6	NAG(confi g-i p)#i p dhcp server pool pool-name	Bind the address pool to the IP interface.



Note

- After an address pool is bound to an interface, its parameters cannot be modified. If you have to modify its parameters, unbind it in advance.
- An address pool can be bound to only one IP interface; however, an IP interface can be related to up to 5 address pools.

6.5.7 (Optional) configuring trusted DHCP relay device

When DHCP clients and the server are in different network segments, a DHCP relay device is required to forward DHCP packets. Under this situation, you need to configure the IP address of the trusted DHCP relay device on the DHCP server.

Configure the trusted DHCP relay device for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i p dhcp server relay-i p <i>ip-address</i> { <i>ip-mask</i> <i>mask-length</i> }	Configure the IP address of the trusted DHCP relay device.

6.5.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG# show i p dhcp server	Show configurations of DHCP Server.
2	NAG# show i p dhcp server pool [<i>pool-name</i>]	Show configurations of the address pool of DHCP Server.
3	NAG# show i p dhcp server relay-i p	Show Relay information about the DHCP Server.
4	NAG# show i p dhcp server lease	Show assigned IP addresses and clients information.
5	NAG# show i p dhcp server stati sti cs	Show packet statistics of DHCP Server.

6.5.9 Example for configuring DHCP Server

Networking requirements

As shown in Figure 6-8, Switch A, as the DHCP server, assigns dynamic IP addresses for clients on the same network. Detailed requirements are as below:

- Enable global DHCP Server, and configure the address pool NAG1.
- Set the DHCP client to obtain IP address and other configurations through DHCP. Set the default leased period to 60min.

- Set the IP address of the TFTP server of the address pool to 192.168.1.2, and name of the startup configuration file to bootFileName.
- Enable DHCP Server on the IP interface, and bind it to the address pool NAG1. Set the IP address of the interface to 192.168.1.3. Bind the interface with VLAN 3.

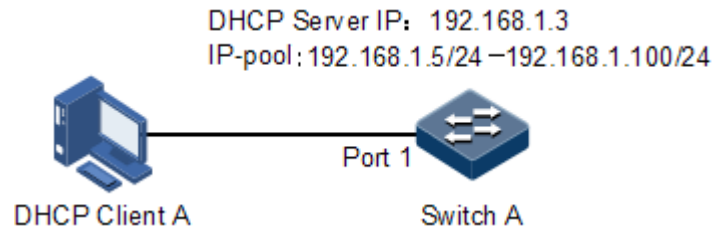


Figure 6-8 DHCP Server networking

Configuration steps

Step 1 Enable global DHCP Server.

```
NAG#confi g
NAG(confi g)#i p dhcp server
```

Step 2 Configure the address pool of DHCP Server.

```
NAG(confi g)#i p dhcp server pool NAG1
NAG(dhcp-pool)#address 192.168.1.5 192.168.1.100 mask 24
NAG(dhcp-pool)#dns-server 192.168.1.10
NAG(dhcp-pool)#dns-server secondary 192.168.1.11
NAG(dhcp-pool)#gateway 192.168.1.1
NAG(dhcp-pool)#tftp-server 192.168.1.2
NAG(dhcp-pool)#bootfile bootFileName
NAG(dhcp-pool)#lease default 60
NAG(dhcp-pool)#exi t
```

Step 3 Configure the IP interface.

```
NAG(confi g)#create vl an 3 acti ve
NAG(confi g)#i nterface port 1
NAG(confi g-port)#swi tchport access vl an 3
NAG(confi g-port)#qui t
NAG(confi g)#i nterface i p 0
NAG(confi g-i p)#i p dhcp server
NAG(confi g-i p)#i p dhcp server pool NAG1
NAG(confi g-i p)#i p address 192.168.1.3
NAG(confi g-i p)#i p vl an 3
```

Checking results

Use the **show ip dhcp server** command to show configurations of DHCP Server.

```
NAG#show ip dhcp server
Global DHCP Server:  Enable
Global Minimum Lease: 30 minutes
Global Default Lease: 30 minutes
Global Maximum Lease: 10080 minutes
```

Interface	Status	Pool s bind
IP0	Disable	--
IP1	Disable	--
IP2	Enable	NAG1
IP3	Disable	--
.....		

Use the **show ip dhcp server pool [pool-name]** command to show configurations of the address pool of DHCP Server.

```
NAG#show ip dhcp server pool NAG1
Pool Name:          NAG1
Associated Interface: --
Address Range:      192.168.1.5~192.168.1.100
Address Mask:       255.255.255.0
Gateway:            192.168.1.1
DNS Server:         192.168.1.10
Secondary DNS:      192.168.1.11
Tftp Server:        192.168.1.2
Bootfile:           bootFileName
Default Lease:      60 minutes
Minimum Lease:      30 minutes
Maximum Lease:      10080 minutes
```

6.6 DHCP Relay

6.6.1 Introduction

At the beginning, DHCP requires the DHCP server and clients to be in the same network segment, instead of different network segments. As a result, a DHCP server is configured for all network 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 DHCP server that are in different network segments. It relays packets across network segments to the DHCP server or clients.

Figure 6-9 shows the principle of DHCP Relay.

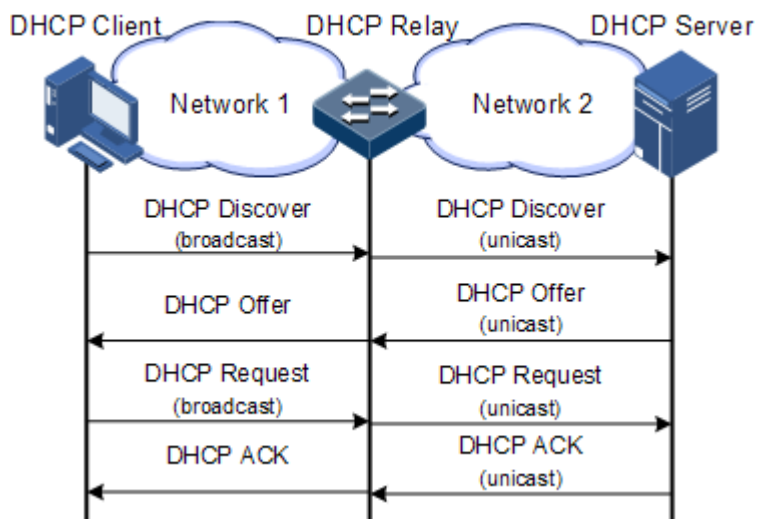


Figure 6-9 Principle of DHCP Relay

- Step 1 The DHCP client sends a request packet to the DHCP server.
- Step 2 After receiving the packet, the DHCP relay device process the packet in a certain way, and then sends it to the DHCP server on the specified network segment.
- Step 3 The DHCP server sends acknowledgement packet to the DHCP client through the DHCP relay device according to the information contained in the request packet. In this way, the configuration of the DHCP client is dynamically configured.

6.6.2 Preparing for configurations

Scenario

When DHCP Client and DHCP Server are not in the same network segment, you can use DHCP Relay to make DHCP Client and DHCP Server in different network segment bear relay service, and relay DHCP protocol packet across network segment to destination DHCP server, so that DHCP Client in different network segment can share the same DHCP Server.

Prerequisite

DHCP Relay is exclusive to DHCP Server, DHCP Client, or DHCP Snooping. Namely, you cannot configure global DHCP Server, DHCP Client, or DHCP Snooping on the device to be configured with DHCP Relay.

6.6.3 Default configurations of DHCP Relay

Default configurations of DHCP Relay are as below.

Function	Default value
Global DHCP Relay	Disable
Interface DHCP Relay	Enable

6.6.4 Configuring global DHCP Relay

Configure global DHCP Relay for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i p dhcp rel ay	Enable global DHCP Relay.

6.6.5 Configuring DHCP Relay on interface

Configure DHCP Relay on the interface for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i nterface i p i f- number	Enter Layer 3 interface configuration mode.
3	NAG(confi g-i p)# i p dhcp rel ay	Enable DHCP Relay on the interface.

6.6.6 Configuring destination IP address for forwarding packets

Configure the destination IP address for forwarding packets for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i nterface i p i f- number	Enter Layer 3 interface configuration mode.
3	NAG(confi g-i p)# i p dhcp real y target-i p i p-address	Configure the destination IP address for Layer 3 interface to forward packets.

6.6.7 (Optional) configuring DHCP Relay to support Option 82

Configure DHCP Relay to support Option 82 for the SNR-S212i-8POE as below.

Step	Configuration	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i p dhcp rel ay i nformati on opti on	Configure DHCP Relay to support Option 82.
3	NAG(confi g)# i p dhcp rel ay i nformati on pol i cy { drop keep repl ace }	Configure the policy for DHCP Relay to process Option 82 request packets

Step	Configuration	Description
4	NAG(config)#interface port <i>port-id</i>	Enter physical layer interface configuration mode.
5	NAG(config-port)#ip dhcp relay information trust	Configure interfaces trusted by DHCP Relay.
6	NAG(config-port)#ip dhcp relay information option vlan-list <i>vlan-list</i>	Configure the lists of VLANs that support Option 82 through DHCP Relay.

6.6.8 Checking configurations

Use the following commands to check configuration results.

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

6.7 DHCP Snooping

6.7.1 Introduction

DHCP Snooping is a security feature of DHCP with the following functions:

- Make the DHCP client obtain the IP address from a legal DHCP server.

If a false DHCP server exists on the network, the DHCP client may obtain incorrect IP address and network configuration parameters, but cannot communicate normally. As shown in Figure 6-10, to make DHCP client obtain the IP address from a legal DHCP server, the DHCP Snooping security system permits to set 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.

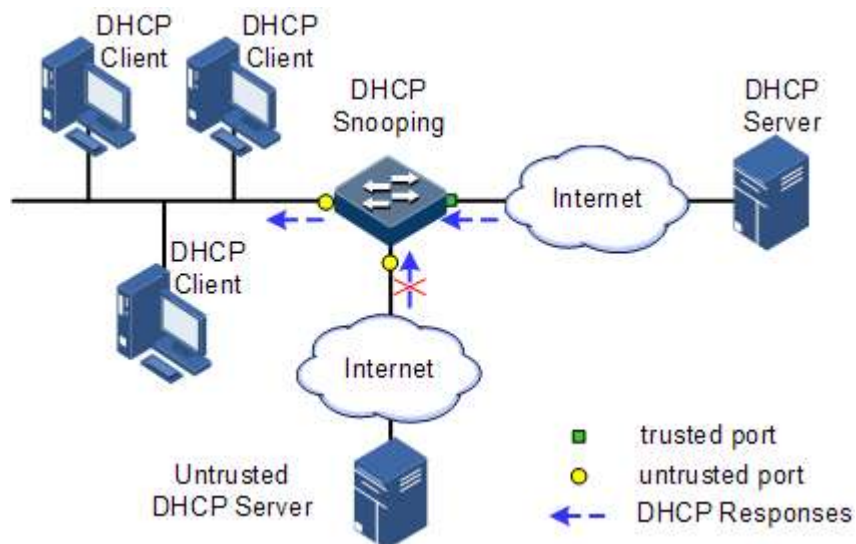


Figure 6-10 DHCP Snooping networking

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

DHCP Snooping records entries through monitor request and reply packets received by the trusted interface, including client MAC address, obtained IP address, DHCP client connected interface and VLAN of the interface, etc. Then implement following by the record information:

- ARP detection: judge legality of a user that sends ARP packet and avoid ARP attack from illegal users.
- IP Source Guard: filter packets forwarded by interfaces by dynamically getting DHCP Snooping entries to avoid illegal packets to pass the interface.
- VLAN mapping: modify mapped VLAN of packets sent to users to original VLAN by searching IP address, MAC address, and original VLAN information in DHCP Snooping entry corresponding to the mapped VLAN.

The Option field in DHCP packet records position information of DHCP clients. The Administrator can use this Option field to locate DHCP clients and control client security and accounting.

If the SNR-S212i-8POE configures DHCP Snooping to support Option function:

- When the SNR-S212i-8POE receives a DHCP request packet, it processes packets according to Option field included or not and filling mode as well as processing policy configured by user, then forwards the processed packet to DHCP server.
- When the SNR-S212i-8POE receives a DHCP reply packet, it deletes the field and forward to DHCP client if the packet does not contain Option field; it then forwards packets directly if the packet does not contain Option field.

6.7.2 Preparing for configurations

Scenario

DHCP Snooping is a security feature of DHCP, used to make DHCP client obtain its IP address from a legal DHCP server and record mapping between IP address and MAC address of a DHCP client.

The Option field of a DHCP packet records location of a DHCP client. The administrator can locate a DHCP client through the Option field and control client security and accounting. The device configured with DHCP Snooping and Option can perform related process according to Option field status in the packet.

Prerequisite

N/A

6.7.3 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 trust/untrust status	Untrust
DHCP Snooping in support of Option 82	Disable

6.7.4 Configuring DHCP Snooping

Generally, ensure that the SNR-S212i-8POE interface connected to DHCP server is in trust state, while the interface connected to user is in distrust state.

If enabling DHCP Snooping without configuring DHCP Snooping supporting Option function, the SNR-S212i-8POE will do nothing to Option fields in the packets. For packets without Option fields, the SNR-S212i-8POE still does not do insertion operation.

By default, DHCP Snooping of all interfaces is enabled, but only when global DHCP Snooping is enabled, interface DHCP Snooping can take effect.

Configure DHCP Snooping for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#i p dhcp snoopi ng</code>	Enable global DHCP Snooping.
3	<code>NAG(confi g)#i p dhcp snoopi ng port-l ist port-l ist</code>	(Optional) enable interface DHCP Snooping.
4	<code>NAG(confi g)#i nterface port port-i d</code>	Enter physical layer interface configuration mode.
5	<code>NAG(confi g-port)#i p dhcp snoopi ng trust</code>	Configure the trusted IPv4 interface of DHCP Snooping.
6	<code>NAG(confi g-port)#i p dhcp snoopi ng i nformati on opti on vl an-l ist vl an-l ist</code>	(Optional) configure the lists of VLANs that support Option 82 through DHCP Snooping.

Step	Command	Description
7	<code>NAG(config-port)#exit</code>	Return to global configuration mode.
8	<code>NAG(config)#ip dhcp snooping option option-id</code>	(Optional) configure DHCP Snooping to support user-defined Option fields.
9	<code>NAG(config)#ip dhcp snooping option client-id</code>	(Optional) configure DHCP Snooping to support Option 61 field.
10	<code>NAG(config)#ip dhcp snooping information option</code>	(Optional) configure DHCP Snooping to support Option 82 field.

6.7.5 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	<code>NAG#show ip dhcp snooping</code>	Show configurations of DHCP Snooping.
2	<code>NAG#show ip dhcp snooping binding</code>	Show configurations of the DHCP Snooping binding table.

6.7.6 Example for configuring DHCP Snooping

Networking requirements

As shown in Figure 6-11, 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 circuit ID sub-option information on Port 3, and remote ID sub-option as user01.

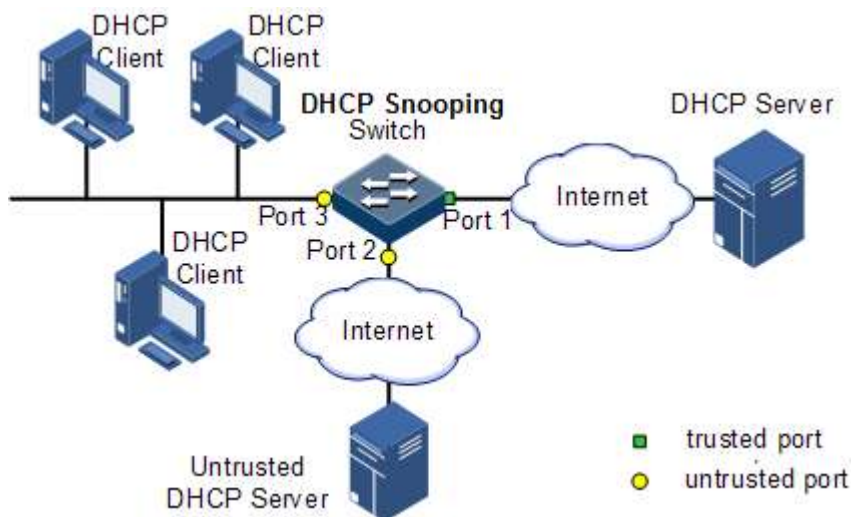


Figure 6-11 DHCP Snooping networking

Configuration steps

Step 1 Configure global DHCP Snooping.

```
NAG#confi g
NAG(confi g)#i p dhcp snoopi ng
```

Step 2 Configure the trusted interface.

```
NAG(confi g)#i nterface port 1
NAG(confi g-port)#i p dhcp snoopi ng trust
NAG(confi g-port)#qui t
```

Step 3 Configure DHCP Relay to support Option 82 field and configure Option 82 field.

```
NAG(confi g)#i p dhcp snoopi ng i nformati on opti on
NAG(confi g)#i p dhcp i nformati on opti on remote-i d string user01
NAG(confi g)#i nterface port 3
NAG(confi g-port)#i p dhcp i nformati on opti on ci rcui t-i d NAG
```

Checking results

Use the **show ip dhcp snooping** command to show configurations of DHCP Snooping.

```
NAG#show i p dhcp i nformati on opti on
DHCP Opti on Confi g I nformati on
  Ci rcui t-ID : default
  Remote-ID Mode: string
  Remote-ID String: user01
  P3 Ci rcui t ID: NAG
i pv4GI obal
i pv4Port
port1:
port2:
port3:
.....
```

6.8 DHCP Options

6.8.1 Introduction

DHCP transmits control information and network configuration parameters through Option field in packet to realize address dynamical distribution to provide abundant network configurations for client. DHCP protocol has 255 kinds of options, the final option is 255. Table 6-2 lists frequently used DHCP options.

Table 6-2 Common DHCP options

Options	Description
3	Router option, to assign gateway for DHCP client
6	DNS server option, to assign DNS server address distributed by the DHCP client
18	IPv6-based DHCP client flag option, to assign interface information for DHCP client
51	IP address lease option
53	DHCP packet type, to mark type for DHCP packets
55	Request parameter list option. Client uses this optical to indicate network configuration parameters need to obtain from server. The content of this option is values corresponding to client requested parameters.
61	DHCP client flag option, to assign device information for DHCP clients.
66	TFTP server name, to assign domain name for TFTP server distributed by DHCP clients.
67	Startup file name, to assign startup file name distributed by DHCP clients.
82	DHCP client flag option, user-defined, mainly used to mark position of DHCP client, including Circuit ID and remote ID.
150	TFTP server address, to assign TFTP server address distributed by DHCP clients.
184	DHCP reserved option, at present Option184 is used to carry information required by voice calling. Through Option184 it can distribute IP address for DHCP client with voice function and meanwhile provide voice calling related information.
255	Complete option

Options 18, 61, and 82 in DHCP Option are relay information options in DHCP packets. When request packets from DHCP clients arrive 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, 61, and 82 implement record DHCP client information on the DHCP server. By cooperating with other software, it can implement functions such as limit on IP address

distribution and accounting. For example, by cooperating with IP Source Guard, Options 18, 61, 82 can defend deceiving through IP address+MAC address.

Option 82 can include at most 255 sub-options. If defined field Option 82, at least one sub-option must be defined. The SNR-S212i-8POE supports the following two sub-options:

- Sub-Option 1 (Circuit ID): it contains interface number, interface VLAN, and the additional information about DHCP client request packet.
- Sub-Option 2 (Remote ID): it contains interface MAC address (DHCP Relay), or bridge MAC address (DHCP snooping device) of the SNR-S212i-8POE, or user-defined string of DHCP client request packets.

6.8.2 Preparing for configurations

Scenario

Options 18, 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, 61, and 82 implement record DHCP client information on the DHCP server. By cooperating with other software, it can implement functions such as limit on IP address distribution and accounting.

Prerequisite

N/A

6.8.3 Default configurations of DHCP Option

Default configurations of DHCP Option are as below.

Function	Default value
attach-string in global configuration mode	N/A
remote-id in global configuration mode	Switch-mac
circuit-id in interface configuration mode	N/A

6.8.4 Configuring DHCP Option fields

Configure DHCP Option fields for the SNR-S212i-8POE as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.

Step	Command	Description
2	NAG(config)#ip dhcp information option attach-string <i>attach-string</i>	(Optional) configure additional information for Option 82 field.
	NAG(config)#interface port <i>port-id</i> NAG(config-port)#ip dhcp information option circuit-id <i>circuit-id</i> [prefix-mode]	(Optional) configure circuit ID sub-option information for Option 82 field on the interface.
	NAG(config-port)#exit NAG(config)#ip dhcp information option remote-id { client-mac client-mac-string hostname switch-mac switch-mac-string string <i>string</i> }	(Optional) configure remote ID sub-option information for Option 82 field.
3	NAG(config)#ip v4 dhcp option <i>option-id</i> { ascii <i>ascii-string</i> hex <i>hex-string</i> ip-address <i>ip-address</i> }	(Optional) create user-defined IPv4 Option field information.
	NAG(config)#interface port <i>port-id</i> NAG(config-port)#ip v4 dhcp option <i>option-id</i> { ascii <i>ascii-string</i> hex <i>hex-string</i> ip-address <i>ip-address</i> }	(Optional) create user-defined IPv4 Option field information on the interface.
4	NAG(config-port)#exit NAG(config)#ip v4 dhcp option client-id { ascii <i>ascii-string</i> hex <i>hex-string</i> ip-address <i>ip-address</i> }	(Optional) configure Option 61 field information.
	NAG(config)#interface port <i>port-id</i> NAG(config-port)#ip v4 dhcp option client-id { ascii <i>ascii-string</i> hex <i>hex-string</i> ip-address <i>ip-address</i> }	(Optional) configure Option61 field information on the interface.

6.8.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show ip dhcp information option	Show configurations of DHCP Option fields.

7 IP routing

This chapter describes basic information and configuration procedures of IP routing, as well as related configuration examples, including the following sections:

- Routing management
- Static routing

7.1 Routing management

7.1.1 Introduction

Routing management is used to manage the routing table, static routing, and various dynamic routing protocols centralizedly.

7.1.2 Preparing for configurations

Scenario

Routing management is used to manage the routing table centralizedly.

Prerequisite

N/A

7.1.3 Default configurations

N/A

7.1.4 Configuring routing management

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# router id ip-address	(Optional) configure the router ID.

7.1.5 Showing routing table

No.	Command	Description
1	NAG# <code>show ip route [detail]</code>	Show IPv4 routing information.
2	NAG# <code>show ip route ip-access-list acl-number [detail]</code>	Show IPv4 routing information after filtering with ACL rules.
3	NAG# <code>show ip route ip-address [ip-mask] [longer-prefixes] [detail]</code>	Show information about a route to a specified IP address.
4	NAG# <code>show ip route start-ip-address start-ip-mask end-ip-address end-ip-mask [detail]</code>	Show information about a route to a specified IP address range.
5	NAG# <code>show ip route protocol { static direct } [detail]</code>	Show information about a route of a protocol.
6	NAG# <code>show ip route statistics</code>	Show route statistics.
7	NAG# <code>show router id</code>	Show the router ID.

7.2 Static routing

7.2.1 Introduction

Routing is required for communication among different devices in one VLAN, or different VLANs. Routing is to transmit packets through network to destination, which adopts the routing table for packets forwarding.

There are three modes to execute routing function:

- **Default routing:** the default routing enables the system to send a packet that fails to reach its destination to a specified default router.
- **Static routing:** manually configured. Static routing enables the system to send packets from the specified interface. This caters for networks with simple topology.
- **Dynamic route:** by dynamically learning routes through routing protocols, the system dynamically calculates the optimal route on the cost of using much bandwidth and network resources.

The SNR-S212i-8POE supports default routing and static routing only.

Default routing

Default routing is a special routing that only be used when there is no matched item in the routing table. Default routing appears as a route to network 0.0.0.0 (with mask 0.0.0.0) in the routing table. You can show default routing configuration by using the **show ip route** command. If destination address of packet cannot match with any item in the routing table, the packet will choose default routing. If the SNR-S212i-8POE has not configured default routing and the destination IP of packet is not in the routing table, the SNR-S212i-8POE will

discard the packet and return an ICMP packet to the Tx end to inform that the destination address or network is unavailable.

Static routing

Static routing is routing configured manually. 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.

7.2.2 Preparing for configurations

Scenario

For a simple topology network, you can configure a static routing. The static routing needs to be configured manually. You can create an intercommunication network by configuring the static routing.

Prerequisite

Configure the IP address of the Layer 3 interface properly.

7.2.3 Default configurations of static routing

Function	Default value
Static routing management distance	1

7.2.4 Configuring static routing

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i p route <i>ip-address ip-mask next-hop-ip-address</i> [di stance value] [descri ption <i>description</i>] [tag <i>tag-id</i>]	Configure the static routing.
3	NAG(confi g)# i p route static di stance <i>value</i>	(Optional) configure the default IPv4 management distance.

7.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG# show i p route	Show the routing table information.

7.2.6 Examples for configuring static routing

Networking requirements

Configure the static routing to make any 2 PCs or the SNR-S212i-8POE devices can communicate with each other, as shown in Figure 7-1.

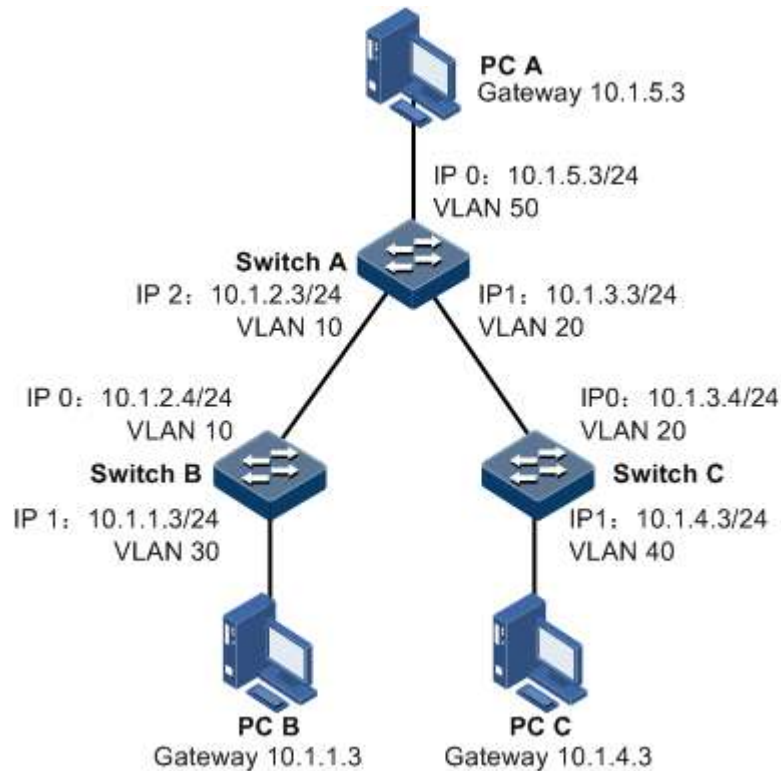


Figure 7-1 Configuring static routing

Configuration steps

Step 1 Configure IP addresses of all devices. The detailed configuration steps are not described here.

Step 2 Configure the static routing on Switch A.

```
NAG#hostname Swit chA
Swit chA#confi g
Swit chA(confi g)#i p route 10.1.1.0 255.255.255.0 10.1.2.4
Swit chA(confi g)#i p route 10.1.4.0 255.255.255.0 10.1.3.4
```

Step 3 Configure the default route on Switch B.

```
NAG#hostname Swit chB
Swit chB#confi g
Swit chB(confi g)#i p route 0.0.0.0 0.0.0.0 10.1.2.3
```

Step 4 Configure the default route on Switch C.

```
NAG#hostname Swi tchC
Swi tchC#confi g
Swi tchC(confi g)#i p route 0.0.0.0 0.0.0.0 10.1.3.3
```

Step 5 Configure the default gateway (10.1.5.3) on PC A. The detailed configuration steps are not described in this guide.

Step 6 Configure the default gateway (10.1.1.3) on PC B. The detailed configuration steps are not described in this guide.

Step 7 Configure the default gateway (10.1.4.3) on PC A. The detailed configuration steps are not described in this guide.

Checking results

Use the **ping** command to check whether all devices can communicate with each other.

```
Swi tchA#pi ng 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.
```

8 QoS

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

- Introduction
- ACL
- Configuring basic QoS
- Configuring congestion management
- Configuring traffic classification and traffic policy
- Configuring rate limiting based on interface and VLAN
- Configuring examples

8.1 Introduction

Users bring forward different service quality demands for network applications, then the network should distribute and schedule resources for different network applications according to user demands. Quality of Service (QoS) can ensure service in real time and integrity when network is overloaded or congested and guarantee that the whole network runs efficiently.

QoS is composed of a group of flow management technologies:

- ACL
- Service model
- Priority trust
- Traffic classification
- Traffic policy
- Priority mapping
- Congestion management

8.1.1 ACL

Access Control List (ACL) is a set of ordered rules, which can control the SNR-S212i-8POE to receive or refuse some data packets.

You need to configure rules on the network to prevent illegal packets from influencing network performance and determine the packets allowed to pass. These rules are defined by ACL.

ACL is a series of rule composed of permit | deny sentences. The rules are described according to source address, destination address, and port ID of data packets. The SNR-S212i-8POE judges receiving or rejecting packets according to the rules.

8.1.2 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 Best-effort service, the network will send packets as possible as it can, but cannot guarantee the delay and reliability.

Best-effort is the default Internet service model now, applying to most network applications, such as FTP and E-mail, which is implemented by First In First Out (FIFO) queue.

DiffServ

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

DiffServ model does not need to maintain state for each flow. It provides differentiated services according to the QoS classification of each packet. Many different methods can be used for classifying QoS packets, such as IP packet priority (IP precedence), the packet source address or destination address.

Generally, DiffServ is used to provide end-to-end QoS services for a number of important applications, which is implemented through the following techniques:

- Committed Access Rate (CAR): CAR refers to classifying the packets according to the pre-set packets matching rules, such as IP packets priority, the packet source address or destination address. The system continues to send the packets if the flow complies with the rules of token bucket; otherwise, it discards the packets or remarks IP precedence, DSCP, EXP, etc. CAR can not only control the flows, but also mark and remark the packets.
- Queue technology: the queue technologies of Strict Priority (SP), (Weight Round Robin) WRR, (Deficit Round Robin) DRR, SP+WRR, and SP+DRR cache and schedule the congestion packets to implement congestion management.

8.1.3 Priority trust

Priority trust refers that the SNR-S212i-8POE uses priority of packets for classification and performs QoS management.

The SNR-S212i-8POE supports packet priority trust based on interface, including:

- Differentiated Services Code Point (DSCP) priority

- Class of Service (CoS) priority
- Interface priority

8.1.4 Traffic classification

Traffic classification refers to recognizing packets of certain types according to configured rules, conducting different QoS policies for packets matching with different rules. It is the prerequisite of differentiated services.

The SNR-S212i-8POE supports traffic classification by IP priority, DSCP priority, and CoS priority over IP packets, as well as traffic classification by Access Control List (ACL) rule and VLAN ID. Figure 8-1 shows the principle of traffic classification.

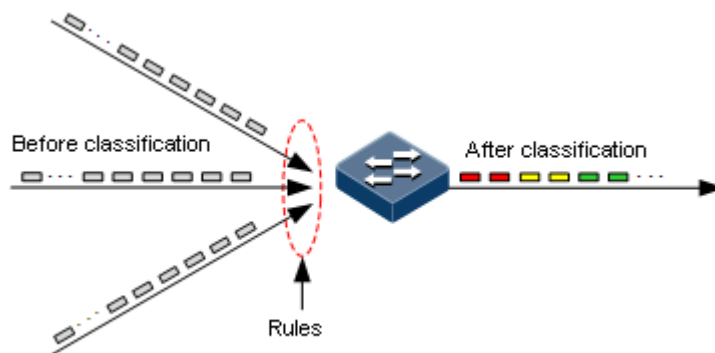


Figure 8-1 Traffic classification

IP priority and DSCP priority

Figure 8-2 shows the structure of the IP packet head. The head contains a 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 priority with value range 0–63, the last 2 bits (bit-6 and bit-7) are reserved. Figure 8-3 shows the structure of two priority types.

4	8	16	32
Version	IHL	ToS	Total Length
Identification		Flags	Fragment Offset
Time-to-Live	Protocol	Header Checksum	
Source Address			
Destination Address			

Figure 8-2 Structure of IP packet head

Bits:	0	1	2	3	4	5	6	7
RFC1122:	Precedence			Type of Service			0	
RFC2474:	DSCP						Unused	

Figure 8-3 Structure of packets with IP priority and DSCP priority

CoS priority

The format of Ethernet packets is modified to make VLAN packets based on IEEE 802.1Q. IEEE 802.1Q adds 4-Byte 802.1Q tag between the source address field and protocol type field, as shown in Figure 8-4. The tag includes a field of 2-Byte TPID (Tag Protocol Identifier, value being 0x8100) and a field of 2-Byte Tag Control Information (TCI).

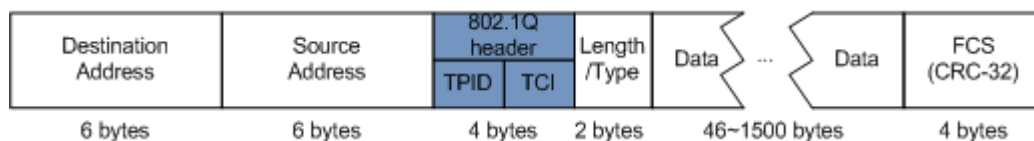


Figure 8-4 Structure of VLAN packets

The CoS priority is included in the first 3 bits of the TCI field, ranging from 0 to 7, as shown in Figure 8-5. It is used when QoS needs to be guaranteed on the Layer 2 network.

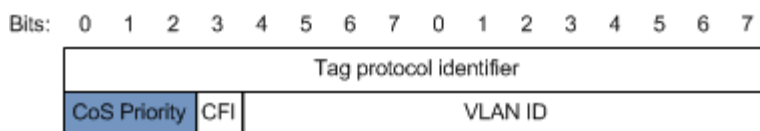


Figure 8-5 Structure of packets with CoS priority

8.1.5 Traffic policy

After classifying packets, the SNR-S212i-8POE needs to take different actions for different packets. The binding of traffic classification and an action forms a traffic policy.

Rate limiting

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 SNR-S212i-8POE supports rate limiting based on traffic policy in the ingress direction on the interface.

The SNR-S212i-8POE supports using token bucket for rate limiting.

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 SNR-S212i-8POE supports redirecting packets to the specified interface for forwarding in the ingress direction of an interface.

Remark

Remark refers to setting some priority fields in packet again and then classifying packets by user-defined standard. Besides, downstream nodes on the network can provide differentiated QoS service according to remark information.

The SNR-S212i-8POE supports remarking packets by local priority and VLAN ID.

Traffic statistics

Traffic statistics is used to take statistics of data packets of a specified service flow, namely, the number of packets and Bytes matching traffic classification that pass the network or are discarded.

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

8.1.6 Priority mapping

Priority mapping refers when the SNR-S212i-8POE receives packets, it sends them in queues with different local priorities in accordance with mapping from external priority to local priority, thus scheduling packets in the egress direction of packets.

The SNR-S212i-8POE supports priority mapping based on DSCP priority or CoS priority.

Table 8-1 lists the default mapping of local priority, DSCP, and CoS.

Table 8-1 Default mapping of local priority, DSCP, and CoS

Local priority	0	1	2	3	4	5	6	7
DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS	0	1	2	3	4	5	6	7

Local priority refers to a kind of packet priority with internal function assigned by the SNR-S212i-8POE, namely, the priority corresponding to queue in QoS queue scheduling.

Local priority ranges from 0 to 7. The SNR-S212i-8POE supports 8 queues. Local priority and queue is 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

8.1.7 Congestion management

Queue scheduling is necessary when there is intermittent congestion on the network or delay sensitive services require higher QoS service than non-sensitive services.

Queue scheduling adopts different schedule algorithms to transmit packets in queues. The SNR-S212i-8POE supports SP, WRR, DRR, SP+WRR and SP+DRR algorithm. Each algorithm solves specific network traffic problems, and has different influences on distribution, delay, and jitter of bandwidth resource.

- SP: schedule packets strictly according to queue priority order. Queues with low priority cannot be scheduled until queues with higher priority finishes schedule, as shown in Figure 8-6.

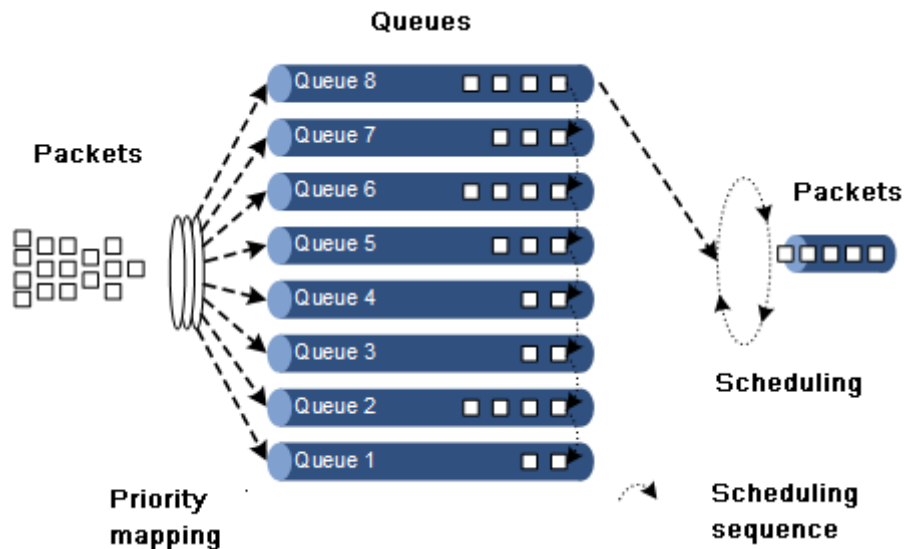


Figure 8-6 SP scheduling

- WRR: on the basis of round scheduling each queue according to queue priority, schedule packets in various queues according to weight of each queue, as shown in Figure 8-7.

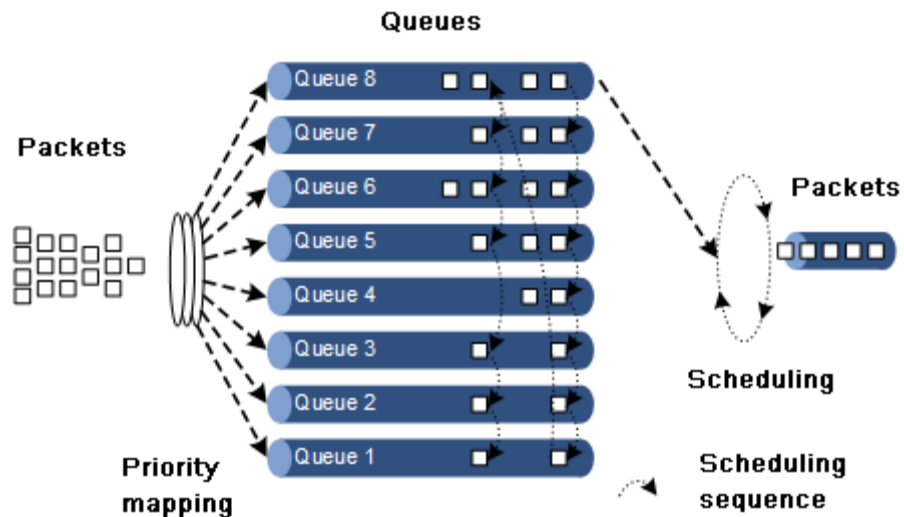


Figure 8-7 WRR scheduling

- DRR: on the basis of circular schedule each queue according to queue priority, schedule packets in each queue according to weight of each queue. Besides, the SNR-S212i-8POE lends the redundant bandwidth of a queue in one schedule to other queues in the later schedule, and the queue borrowing the bandwidth will return it back, as shown in Figure 8-8.

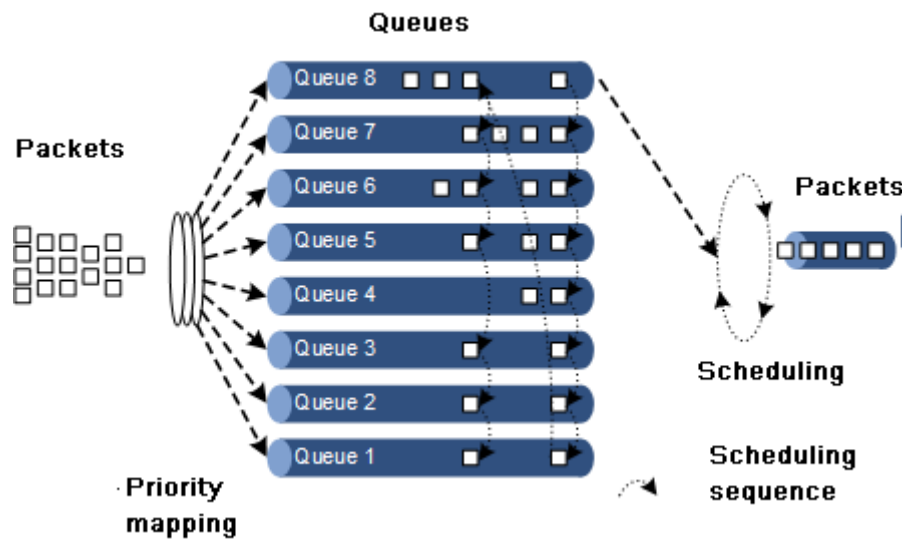


Figure 8-8 DRR scheduling

- SP+WRR: schedule queues on interfaces into two groups, you can assign some queues to conduct SP schedule and other queues to conduct WRR schedule.
- SP+DRR: schedule queues on interfaces into two groups, you can assign some queues to conduct SP schedule and other queues to perform DRR schedule.

8.1.8 Rate limiting based on interface and VLAN

The SNR-S212i-8POE supports rate limiting based on traffic policy, based on interface, based on VLAN. Similar to rate limiting based on traffic policy, the SNR-S212i-8POE discards the exceeding traffic.

8.2 ACL

8.2.1 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:

- IPACL: define classification rules according to source or destination address taken by packets IP head, port ID used by TCP or UDP (being 0 by default), etc. attributes.
- MAC ACL: define classification rules according to source MAC address, destination MAC address, Layer 2 protocol type taken by packets Layer 2 frame head, etc. attributes.
- MAP ACL: MAP ACL can define more protocols and more detailed protocol fields than IPACL and MAC ACL, also can match any Bytes from Byte 22 to Byte 63 of Layer 2 data frame according to user's definition (the offset starts from 0).

There are 3 ACL modes according to difference of application environment:

- ACL based on device
- ACL based on interface
- ACL based on VLAN

Prerequisite

N/A

8.2.2 Default configurations of ACL

Default configurations of ACL are as below.

Function	Default value
Device filter status	Disable
Filter effectiveness status	Take effect
MAC address matching rules	Mismatch
CoS value matching rules	Mismatch
Ethernet frame type matching rules	Mismatch
ARP type matching rules	Mismatch
ARP packet and MAC/IP address matching rules	Mismatch
IP packet matching rules	Mismatch
TCP packet matching rules	Mismatch
UDP packet matching rules	Mismatch
IGMP packet message type matching rules	Mismatch

8.2.3 Configuring IP ACL

Configure IP ACL for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<pre>NAG(confi g)#i p-access-l i st a cl -number { deny permi t } { protocol -i d i cmp i gmp i p } { source-i p-address i p-mask any } { dest i nati on- i p-address i p-mask any } NAG(confi g)#i p-access-l i st a cl -number { deny permi t } { tcp udp } { source-i p-address i p-mask any } [source-protocol -port] { dest i nati on-i p- address i p-mask any } [dest i nati on-protocol - port]</pre>	Configure IP ACL.

8.2.4 Configuring MAC ACL

Configure MAC ACL for the SNR-S212i-8POE as below.


Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#mac-access-l i st <i>acl -number</i> { deny permi t } [<i>protocol -id</i> arp ip rarp any] { <i>source-mac-address mask</i> any } { <i>destinati on-mac-address mask</i> any }	Configure MAC ACL.

8.2.5 Configuring MAP ACL

Configure MAP ACL for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#access-l i st-map <i>acl -number</i> { deny permi t }	Create a MAP ACL, and enter ACLMAP configuration mode.
3	NAG(confi g-acl map)#match mac { <i>destinati on</i> <i>source</i> } <i>mac-address mask</i>	(Optional) define matching rule for source or destination MAC address.
4	NAG(confi g-acl map)#match cos <i>cos-val ue</i>	(Optional) define matching rule for CoS value.
5	NAG(confi g-acl map)#match ethertype <i>ethertype</i> [<i>ethertype-mask</i>]	(Optional) define matching rule for Ethernet frame type. By default, the Ethernet frame type is not matched. The <i>ethertype</i> and <i>ethertype-mask</i> are hexadecimal digits in HHHH format.
6	NAG(confi g-acl map)#match { arp cvl an eapol flowcontrol ip ipv6 loopback mpl s-mul ti cast mpl s-uni cast pppoe pppoedi sc sl owprotocol svl an x25 x75 }	(Optional) define matching rule for upper layer protocol type carried by laryer-2 packets head.
7	NAG(confi g-acl map)#match arp opcode { reply request }	(Optional) define matching rule for ARP type (reply packet/request packet).
8	NAG(confi g-acl map)#match arp { <i>sender-mac</i> <i>target-mac</i> } <i>mac-address</i>	(Optional) define matching rule for MAC address of ARP packet.
9	NAG(confi g-acl map)#match arp { <i>sender-ip</i> <i>target-ip</i> } <i>ip-address</i> [<i>ip-mask</i>]	(Optional) define matching rule for IP address of ARP packet.

Step	Command	Description
10	NAG(config-acl-map)#match ip { destination-address source-address } ip-address [ip-mask]	(Optional) define matching rule for source or destination IP address.
11	NAG(config-acl-map)#match ip precedence { precedence-value critical flash flash- override immediate internet network priority routine }	(Optional) define matching rule for IP packet priority.
12	NAG(config-acl-map)#match ip tos { tos-value max- reliability max-throughput min-delay min-monetary-cost normal }	(Optional) define matching rule for ToS value of IP packet priority.
13	NAG(config-acl-map)#match ip dscp { dscp-value af11 af12 af13 af21 af22 af23 af31 af32 af33 af41 af42 af43 cs1 cs2 cs3 cs4 cs5 cs6 cs7 default ef }	(Optional) define matching rule for DSCP value of IP packets.
14	NAG(config-acl-map)#match ip protocol { protocol-id ahp esp gre icmp igmp igmp ipinip ospf pcp pim tcp udp }	(Optional) define matching rule for protocol value of IP packets.
15	NAG(config-acl-map)#match ip tcp { destination-port source-port } { port-id bgp domain echo exec finger ftp ftp-data gopher hostname ident irc klogin kshell login lpd nntp pim-auto-rp pop2 pop3 smtp sunrpc syslog tacacs talk telnet time uucp whois www }	(Optional) define matching rule for port ID of TCP packet.
16	NAG(config-acl-map)#match ip tcp { ack fin psh rst syn urg }	(Optional) define matching rule for TCP Tag bit.
17	NAG(config-acl-map)#match ip udp { destination-port source-port } { port-id biff bootpc bootps domain echo mobile-ip netbios-dgm netbios-ns netbios-ss ntp pim-auto-rp rip snmp snmptrap sunrpc syslog tacacs talk tftp time who }	(Optional) define matching rule for port ID of UDP packets.

Step	Command	Description
18	<code>NAG(config g-acl map)#match ip icmp icmp-type-id [icmp-code]</code>	(Optional) define matching rule for message type of ICMP packets.
19	<code>NAG(config g-acl map)#match ip no-fragments</code>	(Optional) define matching rules for message type of non-fragment packets.
20	<code>NAG(config g-acl map)#match ip igmp { igmp-type-id dvmrp leave-v2 pim-v1 query report-v1 report-v2 report-v3 }</code>	(Optional) define matching rule for message type of IGMP packets.
21	<code>NAG(config g-acl map)#match user-define rule-string rule-mask offset</code>	<p>(Optional) configure matching rule for user-defined field; that is, two parameters of rule mask and offset take any Byte from Byte 22 to Byte 63 of data frame (the offset starts from 0), and then compares with user-defined rule to filter out matched data frame for processing.</p> <p>For example, to filter all TCP packets, you can define the rule as "06", rule mask as "FF", and offset as 27. The rule mask and offset value work together to filter out content of TCP protocol ID field, and then compares with rule and match with all TCP packets.</p> <p> Note</p> <p>The rule number must be an even hex number. Offset includes the 802.1q VLAN Tag field though the SNR-S212i-8POE receives Untag packets.</p>

8.2.6 Applying ACL

Configure ACL for the SNR-S212i-8POE as below.



Note

ACL cannot take effect until ACL is added into a filter. Multiple ACL matching rules can be added into a filter to form multiple filter rules. When you configure the filter, the order to add ACL matching rule decides priority of the rule. The later the rules are added, the higher the priority is. If multiple rules are conflicted in matching calculation, take the higher priority rule as standard. Pay attention to the order of rules when setting the commands to filter packets correctly.

Applying ACL based on device

Apply ACL based on device as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#fi lter { access- list-map ip-access-list mac- access-list } { all acl-list } [stati stics]	Configure the filter for the device. If the statistics parameter is configured, the system will take statistics according to filter rules.
3	NAG(confi g)#fi lter enable	Enable filter to make rules take effect. Enabling the filter not only activates the filter rules, but also makes the filter rules set later take effect.

Applying ACL based on interface

Apply ACL based on interface as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#fi lter { access- list-map ip-access-list mac- access-list } { all acl-list } ingress port-list port-list [stati stics]	Configure filter on the interface. If the statistics parameter is configured, the system will take statistics according to filtering rules.
3	NAG(confi g)#fi lter enable	Enable filter to make rules take effect. Enabling the filter not only activates the filter rules, but also makes the filter rules set later take effect.

Applying ACL based on VLAN

Apply ACL based on VLAN as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#fi lter { access- list-map ip-access-list mac- access-list } { all acl-list } vl an vl an-id [doubl e-taggi ng inner] [stati stics]	Configure filter on interface. If the statistics parameter is configured, the system will take statistics according to filtering rules.

Step	Command	Description
3	NAG(config)# filter enable	Enable filter to make rules take effect. Enabling the filter not only activates the filter rules, but also makes the filter rules set later take effect.

8.2.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show ip-access-list [<i>acl-list</i>]	Show configurations of IP ACL.
2	NAG#show mac-access-list [<i>acl-list</i>]	Show configurations of MAC ACL.
3	NAG#show access-list-map [<i>acl-number</i>]	Show configurations MAP ACL.
4	NAG#show filter	Show filter configurations.
5	NAG(#show filter { access-list-map ip-access-list mac-access-list } { all <i>acl-list</i> }	Show configurations of the filter based on device.
6	NAG#show filter { access-list-map ip-access-list mac-access-list } { all <i>acl-list</i> } ingress port-list <i>port-list</i>	Show configurations of the filter based on interface.
7	NAG#show filter { access-list-map ip-access-list mac-access-list } { all <i>acl-list</i> } vlan <i>vlan-id</i> [double-tagging inner]	Show configurations of the filter based on VLAN.

8.2.8 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	NAG(config)# clear filter statistics	Clear filter statistics.
2	NAG(config)# clear filter { access-list-map ip-access-list mac-access-list } { all <i>acl-list</i> } statistics	Clear statistics of the filter based on device.

No.	Command	Description
3	<code>NAG(config)#clear filter { access-list-map ip-access-list mac-access-list } { all acl-list } ingress port-list port-list statistics</code>	Clear statistics of the filter based on interface.
4	<code>NAG(config)#clear filter { access-list-map ip-access-list mac-access-list } { all acl-list } vlan vlan-id [double-tagging inner] statistics</code>	Clear statistics of the filter based on VLAN.

8.3 Configuring basic QoS

8.3.1 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 SNR-S212i-8POE processes packets according to their priorities and provides services accordingly.

To specify local priority for packets is the prerequisite for queue scheduling. For packets from the upstream device, you can not only map the external priority carried by packets to different local priorities, but also configure local priority for packets based on interface. Then the SNR-S212i-8POE will conduct queue scheduling according to local priority of packets. Generally, IP packets need to be configured with mapping relationship between IP priority/DSCP priority and local priority; while VLAN packets need to be configured with mapping relationship between CoS priority and local priority.

Prerequisite

N/A

8.3.2 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 priority
Mapping from CoS to local priority	See Table 8-3.
Mapping from DSCP to local priority	See Table 8-4.
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	1	2	3	4	5	6	7

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	1	2	3	4	5	6	7

8.3.3 Enabling global QoS

Enable global QoS for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# ml s qos enabl e	Enable global QoS.

8.3.4 Configuring priority type of interface trust

Configure priority type of interface trust for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i nterface port port-id	Enter physical layer interface configuration mode.
3	NAG(confi g-port)# ml s qos port-pri ori ty pri ori ty	Configure default priority on the interface.
4	NAG(confi g-port)# ml s qos trust { cos dscp port-pri ori ty }	Configure priority type of interface trust.

8.3.5 Configuring mapping from CoS to local priority

Configure mapping from CoS to local priority for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.

Step	Command	Description
2	NAG(config)#mls qos mapping cos <i>cos-queue</i> to local -priority <i>priority</i>	Create mapping from CoS to local priority.
3	NAG(config)#mls qos cos-remark enable	Enable CoS Remark. Change priority of packets to local priority.

Caution

- To configure matching rules for CoS in ACL, use the **mls qos cos-remark enable** command to enable CoS Remark.
- In selective QinQ, when the global TPID is 8100, you have to use the **mls qos cos-remark enable** command to enable CoS Remark if you do not wish to change priority of packets.
- In selective QinQ, when the global TPID is 9100, you have to use the **mls qos cos-remark enable** command to enable CoS Remark if you do not wish to change priority of packets.

8.3.6 Configuring mapping from DSCP to local priority

Configure mapping from DSCP to local priority for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#config	Enter global configuration mode.
2	NAG(config)#mls qos mapping dscp <i>dscp-queue</i> to local -priority <i>priority</i>	Create mapping from DSCP to local priority.

8.3.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show mls qos	Show global QoS, CoS Remark status, and scheduling mode information.
2	NAG#show mls qos port-list <i>port-list</i>	Show QoS priority, trust mode on the interface.
3	NAG#show mls qos mapping cos	Show information about mapping from CoS to local priority.
4	NAG#show mls qos mapping dscp	Show information about mapping from DSCP to local priority.
5	NAG#show mls qos mapping local -priority	Show information about mapping from local priority to queue.

8.4 Configuring congestion management

8.4.1 Preparing for configurations

Scenario

When a network is congested, you need to balance delay and delay jitter of various packets. Packets of key services (such as video and voice) can be preferentially processed while packets of common services (such as E-mail) with identical priority can be fairly processed. Packets with different priorities can be processed according to its weight value. You can configure queue scheduling in this situation. Choose a schedule algorithm according to service condition and customer requirements.

Prerequisite

Enable global QoS.

8.4.2 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 64. • DRR weight for scheduling 8 queues is 8.

8.4.3 Configuring SP queue scheduling

Configure SP queue scheduling for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#ml s qos queue schedul er sp	Configure queue scheduling mode as SP on the interface.

8.4.4 Configuring WRR or SP+WRR queue scheduling

Configure WRR or SP+WRR for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#ml s qos queue schedul er wrr	Configure queue scheduling mode as WRR on the interface.

Step	Command	Description
3	NAG(config-port)#ml s qos queue wrr weight1 weight2 weight3...weight8	Configure weight for various queues. Conduct SP scheduling when priority of a queue is 0.

8.4.5 Configuring DRR or SP+DRR queue scheduling

Configure DRR or SP+DRR for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(config)#ml s qos queue scheduler drr	Configure queue scheduling mode as DRR on the interface.
3	NAG(config)#ml s qos queue drr weight1 weight2 weight3...weight8	Configure packet queue scheduling mode as DRR, and configure weight for various queues. Conduct SP scheduling when priority of a queue is 0.

8.4.6 Configuring queue bandwidth guarantee

Configure queue bandwidth guarantee for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(config)#i nterface port port-id	Enter physical layer interface configuration mode.
3	NAG(config-port)ml s qos queue queue-id shapi ng mi nband maxband	(Optional) configure queue bandwidth guarantee on the interface regardless of burst size.
4	NAG(config-port)#ml s qos queue queue-id shapi ng ci r mi nband [cbs mi nburst] ei r maxband [ebs maxburst]	(Optional) configure queue bandwidth guarantee on the interface and set burst size.

8.4.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show ml s qos port-l i st port-list	Show QoS priority and trust mode information on the interface.

No.	Command	Description
2	NAG# <code>show ml s qos queue</code>	Show queue weight information on the interface.
3	NAG# <code>show ml s qos queue shapling port-list port-list</code>	Show queue bandwidth guarantee information on the interface.

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 an upstream device by priorities or ACL rule.

A traffic classification rule will not take effect until it is bound to a traffic policy. Apply traffic policy according to current network loading conditions and period. Usually, the SNR-S212i-8POE limits the rate of transmitting packets according to configured rate 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 statistics status	Disable

8.5.3 Creating traffic classification

Create traffic classification for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# <code>confi g</code>	Enter global configuration mode.
2	NAG(<code>confi g</code>)# <code>cl ass-map class-map-name [match-all match-any]</code>	Create traffic classification and enter traffic classification cmap configuration mode.
3	NAG(<code>confi g-cmap</code>)# <code>descri ption string</code>	(Optional) describe traffic classification.

8.5.4 Configuring traffic classification rules

Configure traffic classification rules for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#cl ass-map <i>cl ass-map-name</i> [match-all match-any]	Create traffic classification and enter traffic classification cmap configuration mode.
3	NAG(confi g-cmap)# match { access-list-map ip-access-list ipv6-access-list mac-access-list } <i>acl-number</i>	(Optional) configure traffic classification over ACL rule. The ACL rule must be defined firstly and the type must be permit .
4	NAG(confi g-cmap)# match cl ass-map <i>cl ass-map-name</i>	(Optional) configure traffic classification over traffic classification rule. The pursuant traffic classification must be created and the matched type must be identical with the traffic classification type.
5	NAG(confi g-cmap)# match cos <i>cos-value</i>	(Optional) configure traffic classification over CoS priority of packets.
6	NAG(confi g-cmap)# match inner-vlan <i>inner-vlan-value</i> outer-vlan <i>outer-vlan-value</i>	(Optional) configure traffic classification based on inner and outer VLANs of packets.
7	NAG(confi g-cmap)# match ip dscp <i>dscp-value</i>	(Optional) configure traffic classification over DSCP priority or IP priority rule.
8	NAG(confi g-cmap)# match vl an <i>vl an-list</i> [double-tagging inner]	(Optional) configure traffic classification over VLAN ID rule of VLAN packets.




Note

- When the matched type of a traffic classification is **match-all**, the matched information may have conflict and the configuration may fail.
- Traffic classification rules must be created for traffic classification; namely, the **match** parameter must be configured.
- For traffic classification quoted by traffic policy, do not modify traffic classification rule; namely, do not modify the **match** parameter of traffic classification.

8.5.5 Creating rate limit rule and shapping rule

When user needs to take rate limit to packets based on traffic policy, please create token bucket and set rate limit and shaping rule to token bucket as well as quote this rule to traffic classification bound to traffic policy.

Create rate limiting rules and shapping rule for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#pol i cer <i>pol i cer-name</i> si ngl e	Create token bucket and enter traffic-policer configuration mode.
3	NAG(traffi c-pol i cer)#ci r <i>ci r</i> cbs <i>cbs</i>	(Optional) configure flow mode token bucket parameters.  Note Flow mode token bucket is single token bucket, only supporting to configure red and green packets operation.
4	NAG(traffi c-pol i cer)#ci r <i>ci r</i> cbs <i>cbs ebs ebs</i>	(Optional) configure RFC2697 mode token bucket parameters.
5	NAG(traffi c-pol i cer)#ci r <i>ci r</i> cbs <i>cbs ei r ei r ebs ebs [coupl i ng]</i>	(Optional) configure RFC4115 mode or MEF token bucket parameters.
6	NAG(traffi c-pol i cer)#drop-col or { red [ye ll ow] ye ll ow }	(Optional) configure token bucket to drop some packets in certain color.

8.5.6 Creating traffic policy

Create traffic policy for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#pol i cy-map <i>pol i cy-map-name</i>	Create traffic policy and enter traffic policy pmap configuration mode.
3	NAG(confi g-pmap)#descri pt i on <i>string</i>	(Optional) configure description of traffic policy.

8.5.7 Defining traffic policy mapping




Note

Define one or more defined traffic classifications to one traffic policy.

Define traffic policy mapping for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.



Step	Command	Description
2	NAG(confi g)# pol i cy-map <i>pol i cy-map-name</i>	Create traffic policy and enter traffic policy pmap configuration mode.
3	NAG(confi g-pmap)# cl ass-map <i>cl ass-map-name</i>	Bind traffic classification into traffic policy; only apply traffic policy to packets matching with traffic classification.  Note At least one rule is required for traffic classification to bind traffic policy, otherwise the binding will fail.

8.5.8 Defining traffic policy operation



Define different operations to different flows in policy.

Define a traffic policy operation for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# pol i cy-map <i>pol i cy-map-name</i>	Create traffic policy and enter traffic policy pmap configuration mode.
3	NAG(confi g-pmap)# cl ass-map <i>cl ass-map-name</i>	Bind traffic classification into traffic policy; only apply traffic policy to packets matching with traffic classification.  Note At least one rule is necessary for traffic classification to bind traffic policy, otherwise the binding will fail.
4	NAG(confi g-pmap-c)# pol i ce <i>pol i ce-name</i>	(Optional) apply token bucket on traffic policy and take rate limiting and shaping.  Note The token bucket needs to be created in advance and be configured with rate limiting and shaping rule; otherwise, the operation will fail.
5	NAG(confi g-pmap-c)# redl ect-to port <i>port-i d</i>	(Optional) configure redirection rule under traffic classification, forwarding classified packets from assigned interface.

Step	Command	Description
6	NAG(config-pmap-c)#set { local - priority local - priority vlan vlan-id }	(Optional) configure remark rule under traffic classification, and modify local priority or VLAN ID that matches the traffic classification.
7	NAG(config-pmap-c)#copy-to-mirror	(Optional) configure flow mirror to monitor interface.
8	NAG(config-pmap-c)#statistics enable	(Optional) configure flow statistic rule under traffic classification, statistic packets for matched traffic classification.

8.5.9 Applying traffic policy to interfaces

Apply traffic policy to the interface for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(config)#service-policy policy-name ingress port port-id	Bind the configured traffic policy with the interface.

8.5.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show service-policy statistics [port port-id]	Show traffic policy status and the statistics of the applied policy.
2	NAG#show class-map [class-map-name]	Show information about traffic classification.
3	NAG#show policy-map [policy-map-name]	Show traffic policy information.
4	NAG#show policy-map [policy-map-name] [class class-map-name]	Show information about traffic classification in traffic policy.
5	NAG#show mls qos policer [policer-name]	Show information about the assigned token bucket (rate limiting and shaping).
6	NAG#show mls qos policer-type [aggregate-policer class-policer hierarchy-policer single-policer]	Show information about the assigned type token bucket (rate limiting and shaping).

No.	Command	Description
7	NAG# <code>show policy-map port-list port-list</code>	Show application information on about traffic policy the interface.

8.5.11 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	NAG(config)# <code>clear service-policy statistics [ingress port-list port-list [class-map class-map-name] port-list port-list]</code>	Clear statistics of QoS packets.

8.6 Configuring rate limiting based on interface and VLAN

8.6.1 Preparing for configurations

Scenario

When the network is congested, you wish to restrict burst flow on some interface or some VLAN to make packets transmitted in a well-proportioned rate to remove network congestion. You need to configure rate limiting based on interface or VLAN.

Prerequisite

Create VLANs.

8.6.2 Default configurations of rate limiting based on interface and VLAN

Default configurations of rate limiting based on interface and VLAN are as below.

Function	Default value
Rate limiting based on interface	100000 kbit/s
Rate burst based on interface	0 kBytes

8.6.3 Configuring rate limiting based on interface

Configure rate limiting based on interface for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# <code>confi g</code>	Enter global configuration mode.

Step	Command	Description
2	NAG(config)#rate-limit port-list port-list { both egress ingress } rate-value [burst-value]	Configure rate limiting based on interface.

8.6.4 Configuring rate limiting based on VLAN

Configure rate limiting based on VLAN for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#config	Enter global configuration mode.
2	NAG(config)#rate-limit vlan vlan- id rate-value burst-value [statistics]	(Optional) configure rate limiting based on VLAN.

8.6.5 Configuring rate limiting based on QinQ

Configure rate limiting based on QinQ for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#config	Enter global configuration mode.
2	NAG(config)#rate-limit double-tagging- vlan outer { outer-vlan-id any } inner { inner-vlan-id any } rate-value burst-value [statistics]	(Optional) configure rate limiting based on QinQ.

8.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show rate-limit port-list port-list	Show configurations of rate limiting based on on interface.
2	NAG#show rate-limit portlist all	Show configurations of rate limiting on all interfaces.
3	NAG#show rate-limit vlan [vlan- id]	Show configurations of rate limiting based on VLAN.
4	NAG#show rate-limit double- tagging-vlan [[outer outer-vlan- id] [inner inner-vlan-id]]	Show configurations of rate limiting based on QinQ.

8.6.7 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	<code>NAG(config)#clear double-tagging-vlan statistics outer { vlan-id any } inner { vlan-id any }</code>	Clear statistics of rate limiting on double VLAN Tag packets.

8.7 Configuring examples

8.7.1 Example for configuring ACL

Networking requirements

As shown in Figure 8-9, configure ACL to prevent 192.168.1.1 from accessing the server 192.168.1.100 on Switch A and restrict users' access to the server.

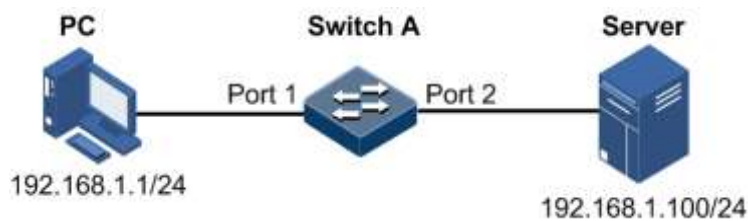


Figure 8-9 ACL networking

Configuration steps

Step 1 **Configure IP ACL.**

```
NAG#confi g
NAG(config)#ip-access-list 1 permit ip any any
NAG(config)#ip-access-list 2 deny ip 192.168.1.1 255.255.255.255
192.168.1.100 255.255.255.255
```

Step 2 **Apply ACL on Port 1 on Switch A.**

```
NAG(config)#filter ip-access-list 1-2 ingress port-list 1
NAG(config)#filter enable
```

Checking results

Use the **show ip-access-list** command to show configurations of IP ACL.

```
NAG#show ip-access-list
Src Ip: Source Ip Address
Src Ip Mask: Source Ip Address Mask
Dest Ip: Destination Ip Address
Dest Ip Mask: Destination Ip Address Mask
List Access Protocol Ref. Src Ip Src Ip Mask:Port Dest Ip Dst Ip
Mask: Port
-----
-----
1 permit IP 1 0.0.0.0 0.0.0.0:0 0.0.0.0 0.0.0.0:0
2 deny IP 1 192.168.1.1 255.255.255.255:0 192.168.1.100
255.255.255.255:0
```

Use the **show filter** command to show filter configurations.

```
NAG#show filter
Rule filter: enable
Filter list(In accordance with the priority from low to high):
ACL-Index IPort EPort VLAN VLANType Hardware Valid StatHw Pkts
-----
IP 1 port1 -- -- -- No Yes No --
IP 2 port1 -- -- -- No Yes No --
```

8.7.2 Example for configuring congestion management

Networking requirements

As shown in Figure 8-10, the user uses voice, video and data services.

CoS priority of voice service is 5, CoS priority of video service is 4, and CoS priority of data service is 2. The local priorities for these three types of services are mapping 6, 5, and 2 respectively.

Congestion occurs easily on Switch A. To reduce network congestion; make the following rules according to different services types:

- For voice service, perform SP schedule to ensure that this part of flow passes through in prior.
- For video service, perform WRR schedule, with weight value 50.
- For data service, perform WRR schedule, with weight value 20.

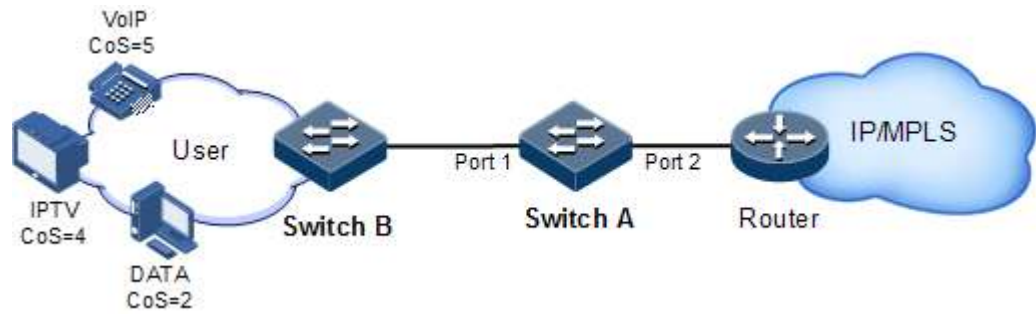


Figure 8-10 Queue scheduling networking

Configuration steps

Step 1 Configure interface priority trust mode.

```
NAG#hostname Swi tchA
Swi tchA#confi g
Swi tchA(confi g)#ml s qos enabl e
Swi tchA(confi g)#i nterface port 2
Swi tchA(confi g-port)#ml s qos trust cos
Swi tchA(confi g-port)#qui t
```

Step 2 Configure mapping profile between CoS priority and local priority.

```
Swi tchA(confi g)#ml s qos mappi ng cos 5 to local -pri ori ty 6
Swi tchA(confi g)#ml s qos mappi ng cos 4 to local -pri ori ty 5
Swi tchA(confi g)#ml s qos mappi ng cos 2 to local -pri ori ty 2
```

Step 3 Conduct SP+WRR queue scheduling.

```
Swi tchA(confi g)#ml s qos queue wrr 1 1 20 1 1 50 0 0
```

Checking results

Show interface priority trust mode.

```
NAG#show ml s qos port-l ist 1-2
Port      Pri ori ty  Trust
-----
port1     0          Cos
port2     0          Cos
```

Use the following command to show mapping relationship between Cos priority and local priority.

```
NAG#show ml s qos mappi ng cos
CoS-Mappi ng:

CoS:          0      1      2      3      4      5      6      7
-----
Local Pri ori ty: 0      1      2      3      5      6      6      7
NAG#show ml s qos mappi ng local -pri ori ty
Local Pri ori ty-Queue Mappi ng:
Local Pri ori ty: 0  1  2  3  4  5  6  7
-----
Queue:           1  2  3  4  5  6  7  8
```

Use the following command to show configurations of queue scheduling on the interface.

```
NAG#show ml s qos queue
Queue      Wei ght (WRR)
-----
1          1
2          1
3         20
4          1
5          1
6         50
7          0
8          0

Queue      Wei ght (DRR)
-----
1          8
2          8
3          8
4          8
5          8
6          8
7          8
8          8
```

8.7.3 Example for configuring rate limiting based on traffic policy

Networking requirements

As show in Figure 8-11, User A, User B, User C are respectively belonged to VLAN 1, VLAN 2, VLAN 3, and they are connected to the Switch D through Switch A, Switch B, Switch C respectively.

User A uses voice and video services, User B provides voice, video and data services, and User C provides video and data services.

According to service requirements, make rules as below.

- For User A, provide 25 Mbit/s assured bandwidth, permitting burst flow 100KB and discarding redundant flow.
- For User B, provide 35 Mbit/s assured bandwidth, permitting burst flow 100KB and discarding redundant flow.
- For User C, provide 30 Mbit/s assured bandwidth, permitting burst flow 100KB and discarding redundant flow.

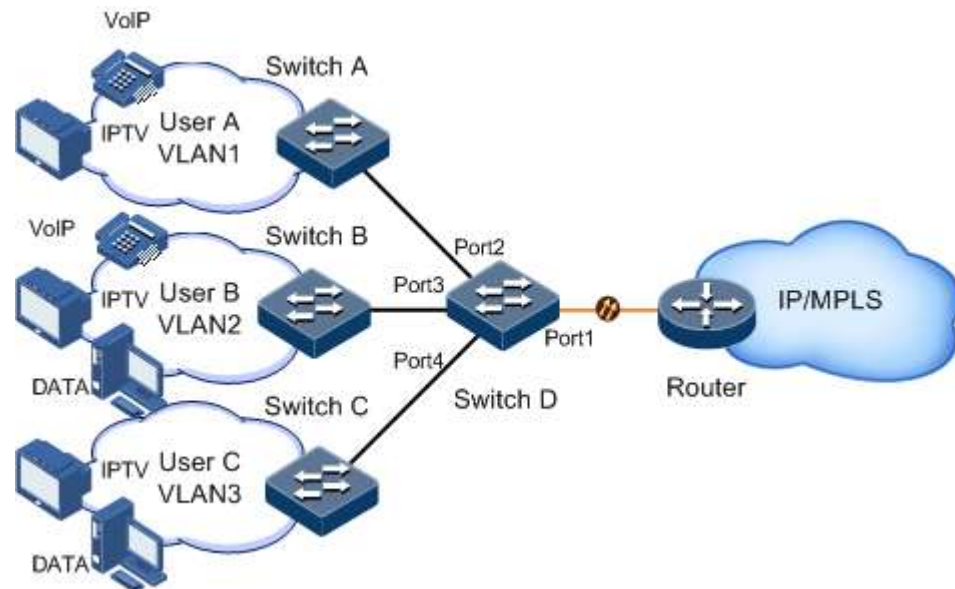


Figure 8-11 Rate limiting based on traffic policy

Configuration steps

Step 1 Create and configure traffic classification, and classify packets by VLAN for different users.

```
NAG#confi g
NAG(confi g)#ml s qos enabl e
NAG(confi g)#cl ass-map usera match-any
NAG(confi g-cmap)#match vl an 1
NAG(confi g-cmap)#qui t
NAG(confi g)#cl ass-map userb match-any
NAG(confi g-cmap)#match vl an 2
NAG(confi g-cmap)#qui t
NAG(confi g)#cl ass-map userc match-any
NAG(confi g-cmap)#match vl an 3
NAG(confi g-cmap)#qui t
```

Step 2 Create rate limiting rules.

```

NAG(confi g)#pol i cer usera si ngl e
NAG(traffi c-pol i cer)#cl r 25000 cbs 100
NAG(traffi c-pol i cer)#qui t
NAG(confi g)#pol i cer userb si ngl e
NAG(traffi c-pol i cer)#cl r 35000 cbs 100
NAG(traffi c-pol i cer)#qui t
NAG(confi g)#pol i cer userc si ngl e
NAG(traffi c-pol i cer)#cl r 30000 cbs 100
NAG(traffi c-pol i cer)#qui t

```

Step 3 Create and configure traffic policy.

```

NAG(confi g)#pol i cy-map usera
NAG(confi g-pmap)#cl ass-map usera
NAG(confi g-pmap-c)#pol i ce usera
NAG(confi g-pmap-c)#qui t
NAG(confi g-pmap)#qui t
NAG(confi g)#servi ce-pol i cy usera i ngress port 2
NAG(confi g)#pol i cy-map userb
NAG(confi g-pmap)#cl ass-map userb
NAG(confi g-pmap-c)#pol i ce userb
NAG(confi g-pmap-c)#qui t
NAG(confi g-pmap)#qui t
NAG(confi g)#servi ce-pol i cy userb i ngress port 3
NAG(confi g)#pol i cy-map userc
NAG(confi g-pmap)#cl ass-map userc
NAG(confi g-pmap-c)#pol i ce userc
NAG(confi g-pmap-c)#qui t
NAG(confi g-pmap)#qui t
NAG(confi g)#servi ce-pol i cy userc i ngress port 4

```

Checking results

Use the **show class-map** command to show configurations of traffic classification.

```

NAG#show cl ass-map usera
  Class Map match-any usera (i d 0)
    Match vl an 1
NAG#show cl ass-map userb
  Class Map match-any userb (i d 1)
    Match vl an 2
NAG#show cl ass-map userc
  Class Map match-any userc (i d 2)
    Match vl an 3

```

Use the **show mls qos policer** command to show configurations of rate limiting rules.

```

NAG#show ml s qos pol i cer
single-pol i cer: usera      mode: fl ow   col or: bl i nd
cir: 25000 kbps, cbs: 10 kB,
Used by pol i cy map usera

single-pol i cer: userb      mode: fl ow   col or: bl i nd
cir: 5000 kbps, cbs: 100 kB,
Used by pol i cy map userb

single-pol i cer: userc      mode: fl ow   col or: bl i nd
cir: 30000 kbps, cbs: 100 kB,
Used by pol i cy map userc

```

Use the **show policy-map** command to show configurations of traffic policy.

```

NAG#show pol i cy-map
Pol i cy Map usera
  Cl ass usera
    pol i ce usera

Pol i cy Map userb
  Cl ass userb
    pol i ce userb

Pol i cy Map userc
  Cl ass userc
    pol i ce userc

```

Use the **show service-policy statistics** command to show traffic policy status.

```

NAG#show servi ce-pol i cy stati stl cs port 2
Pol i cy Swi tch: enabl e
port: port2
  Di recti on: Ingress
  Cl assName: usera
  HwEnabl e: No      Uni t: Pkts
  Pol i cerName: usera
  Inprofi l ePkt64: --
  Pol i cyName: usera
  Stati stl csSwi tch: di sabl e
  Pol i cyerType: Si ngl e-pol i cer
  Outprofi l ePkt64: --

```

8.7.4 Example for configuring rate limiting based on interface

Networking requirements

As shown in Figure 8-12, User A, User B, User C are respectively connected to Switch A, Switch B, Switch C and Switch D.

User A provides voice and video services, User B provides voice, video and data services, and User C provides video and data services.

According to service requirements, user needs to make rules as below.

- For User A, provide 25Mbit/s assured bandwidth, and discard redundant flow.
- For User B, provide 35Mbit/s assured bandwidth, and discard redundant flow.
- For User C, provide 30Mbit/s assured bandwidth, and discard redundant flow.

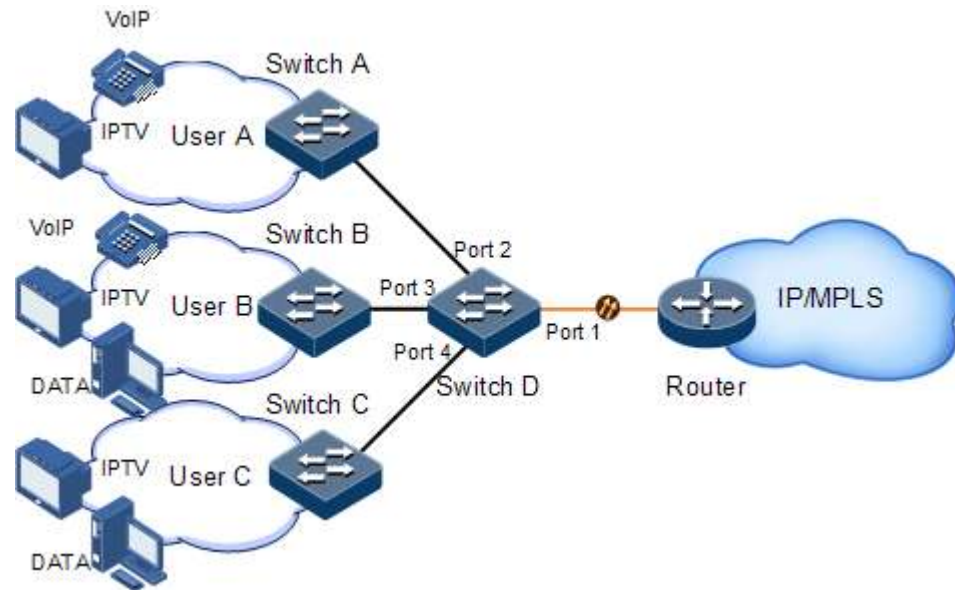


Figure 8-12 Rate limiting based on interface

Configuration steps

Step 1 Configure rate limiting based on interface.

```
NAG#confi g
NAG(confi g)#rate-limi t port-lis t 2 i ngress 25000
NAG(confi g)#rate-limi t port-lis t 3 i ngress 35000
NAG(confi g)#rate-limi t port-lis t 4 i ngress 30000
```

Checking results

Use the **show rate-limit port-list** command to show configurations of rate limiting based on interface.

```
NAG#show rate-limi t port-lis t 2-4
I-Rate: Ingress Rate
I-Burst: Ingress Burst
E-Rate: Egress Rate
E-Burst: Egress Burst
```

Port	I-Rate(kbps)	I-Burst(kB)	E-Rate(kbps)	E-Burst(kB)
port2	24992	128	100000	0

port3	34976	128	100000	0
port4	29984	128	100000	0

9 Multicast

This chapter describes basic principle and configuration of multicast and provides related configuration examples, including the following sections:

- Overview
- Basic functions of Layer 2 multicast
- Configuring IGMP Snooping
- Configuration examples

9.1 Overview

9.1.1 Multicast overview

With the continuous development of Internet, more and more various interactive data, voice, and video 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 come up with higher requirements for network bandwidth, information security, and paid feature. Traditional unicast and broadcast cannot meet these requirements well, while multicast has met them timely.

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

Comparison among unicast, broadcast and multicast

Multicast is a kind of packets transmission method which is parallel with unicast and broadcast.

- Unicast: the system establishes a data transmission path for each user who needs the information, and sends separate copy information for them. Through unicast, the amount of information transmitted over the network is proportional to the number of users, so when the number of users becomes huge, there will be more identical information on the network. In this case, bandwidth will become an important bottleneck, and unicast will not be conducive to large-scale information transmission.
- Broadcast: the system sends information to all users regardless of whether they need or not, so any user will receive it. Through broadcast, the information source delivers

information to all users in the network segment, which fails to guarantee information security and paid service. In addition, when the number of users who require this kind of information decreases, the utilization of network resources will be very low, and the bandwidth will be wasted seriously.

- Multicast: when some users in the network need specific information, the sender only sends one piece of information, then the transmitted information can be reproduced and distributed in fork junction as far as possible.

As shown in Figure 9-1, assume that User B and User C need information, you can use multicast transmission to combine User B and User C to a receiver set, then the information source just needs to send one piece of information. Each switch on the network will establish their multicast forwarding table according to IGMP packets, and finally transmits the information to the actual receiver User B and User C.

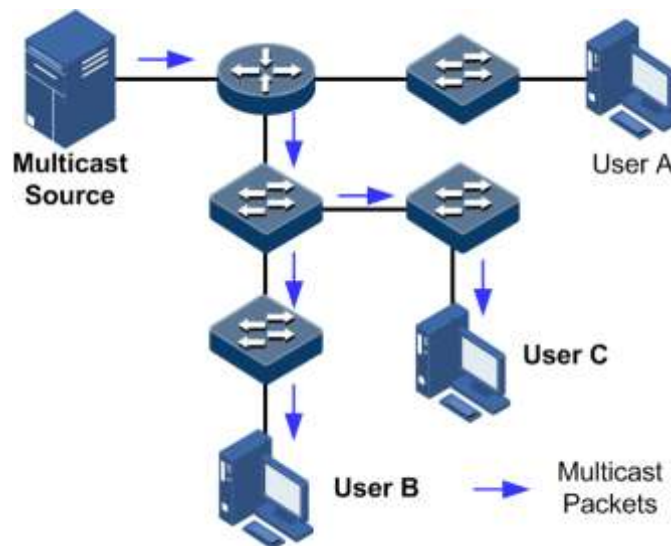


Figure 9-1 Multicast transmission networking

In summary, the unicast is for sparse network users and broadcast is for dense network users. When the number of users in the network is uncertain, unicast and broadcast will present low efficiency. When the number of users are doubled and redoubled, the multicast mode does not need to increase backbone bandwidth, but sends information to the user in need. These advantages of multicast make itself become a hotspot in study of the current network technology.

Advantages and application of multicast

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

- Improve efficiency: reduce network traffic, relieve server and CPU load.
- Optimize performance: reduce redundant traffic and guarantee information security.
- Support distributed applications: solve the problem of point-point data transmission.

The multicast technology is used in the following aspects:

- Multimedia and streaming media, such as, network television, network radio, and real-time video/audio conferencing
- Training, cooperative operations communications, such as: distance education, telemedicine

- Data warehousing, financial applications (stock)
- Any other "point-to-multipoint" applications

Basic concept in multicast

- Multicast group

A multicast group refers to the recipient set using the same IP multicast address identification. Any user host (or other receiving device) will become a member of the group after joining the multicast group. They can identify and receive multicast data with the destination address as IP multicast address.

- Multicast group members

Each host joining a multicast group will become a member of the multicast group. Multicast group members are dynamic, and hosts can join or leave multicast group at any time. Group members may be widely distributed in any part of the network.

- Multicast source

A multicast source refers to a server which regards multicast group address as the destination address to send IP packet. A multicast source can send data to multiple multicast groups; multiple multicast sources can send to a multicast group.

- Multicast router

A multicast router is a router that supports Layer 3 multicast. The multicast router can achieve multicast routing and guide multicast packet forwarding, and provide multicast group member management to distal network segment connecting with users.

- Router interface

A router interface refers to the interface toward multicast router between a multicast router and a host. The SNR-S212i-8POE receives multicast packets from this interface.

- Member interface

Known as the receiving interface, a member interface is the interface towards the host between multicast router and the host. The SNR-S212i-8POE sends multicast packets from this interface.

Figure 9-2 shows basic concepts in multicast.

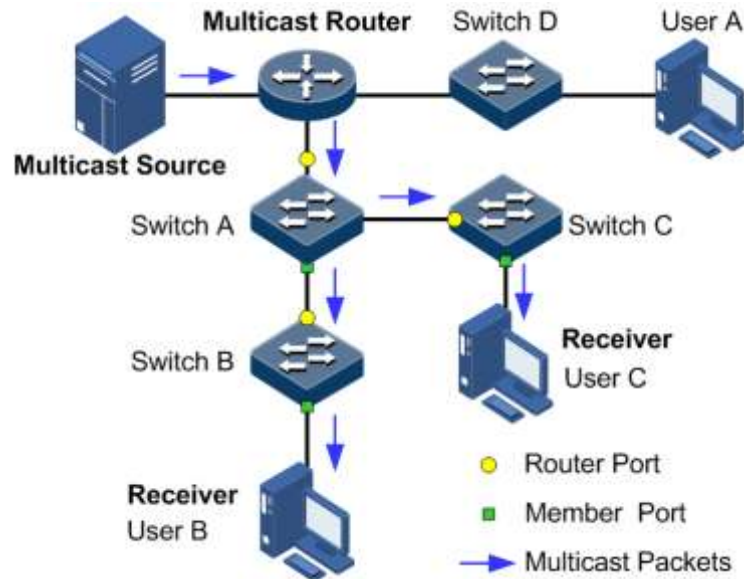


Figure 9-2 Basic concepts in multicast

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.



Note

The multicast address is the destination address instead of the source address.

- IP multicast address

Internet Assigned Numbers Authority (IANA) assigns Class D address space to IPv4 multicast; the IPv4 multicast address ranges from 224.0.0.0 to 239.255.255.255.

- Multicast MAC address

When the Ethernet transmits unicast IP packets, it uses the MAC address of the receiver as the destination MAC address. However, when multicast packets are transmitted, the destination is no longer a specific receiver, but a group with an uncertain number of members, so the Ethernet needs to use the multicast MAC address.

The multicast MAC address identifies receivers of the same multicast group on the link layer.

According to IANA, high bit 24 of the multicast MAC address are 0x01005E, bit 25 is fixed to 0, and the low bit 23 corresponds to low bit 23 of the IPv4 multicast address.

Figure 9-3 shows mapping between the IP multicast address and MAC address.

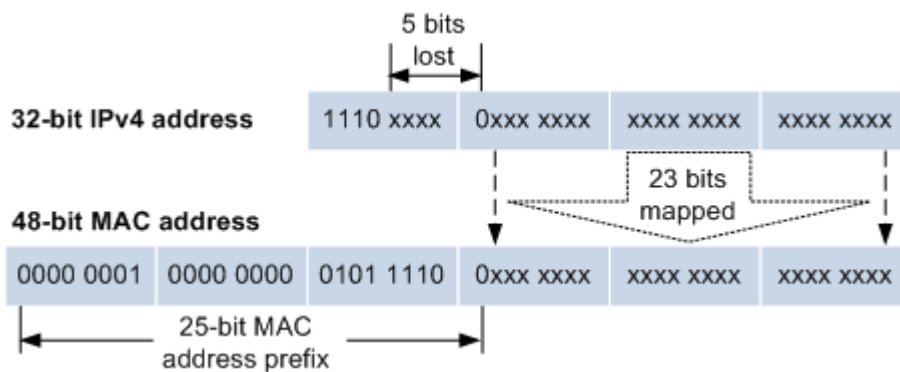


Figure 9-3 Mapping between IPv4 multicast address and multicast MAC address

The first 4 bits of IP multicast address are 1110, indicating multicast identification. In the last 28 bits, only 23 bits are mapped to the multicast MAC address, and the missing of 5 bits makes 32 IP multicast addresses mapped to the same multicast MAC address. Therefore, in Layer 2, the SNR-S212i-8POE may receive extra data besides IPv4 multicast group, and these extra multicast data needs to be filtered by the upper layer on the SNR-S212i-8POE.

Basis of multicast protocol

To implement complete set of multicast services, you need to deploy a variety of multicast protocols in various positions of network and make them cooperate with each other.

Typically, IP multicast working at network layer is called Layer 3 multicast, so the corresponding multicast protocol is called Layer 3 multicast protocol, including Internet Group Management Protocol (IGMP). IP multicast working at data link layer is called Layer 2 multicast, so the corresponding multicast protocol is called Layer 2 multicast protocol, including Internet Group Management Protocol (IGMP) Snooping.

Figure 9-4 shows operating of IGMP and Layer 2 multicast features.

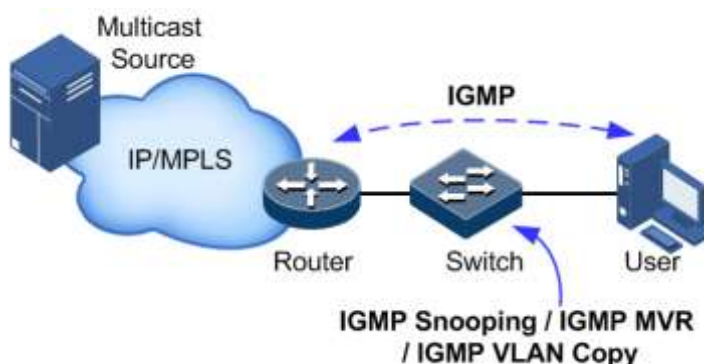


Figure 9-4 Operating of IGMP and Layer 2 multicast features

IGMP, a protocol in TCP/IP protocol suite, is responsible for managing IPv4 multicast members. IGMP runs between the multicast router and host, defines the establishment and maintenance mechanism of multicast group membership between hosts and the multicast router. IGMP is not involved in transmission and maintenance of group membership between multicast routers, which is completed by the multicast routing protocol.

IGMP manages group members through interaction of IGMP packets between the host and multicast router. IGMP packets are encapsulated in IP packets, including Query packets, Report packets, and Leave packets. Basic functions of IGMP are as below:

- The host sends Report packets to join the multicast group, sends Leave packets to leave the multicast group, and automatically decides which multicast group packets to receive.
- The multicast router sends Query packets periodically, and receives Report packets and Leave packets from hosts to understand the multicast group members in connected 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 newer version is fully compatible with the elder version. Currently the most widely used version is IGMPv2, while the Leave packet does not 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 implement forwarding multicast data at Layer 2 and suppress multicast data diffusion at Layer 2.

Supported multicast features

The SNR-S212i-8POE supports the following multicast features:

- Basic functions of IGMP
- IGMP Snooping

9.1.2 Basic functions of Layer 2 multicast

Basic functions of Layer 2 multicast are as below:

- Assign the multicast router interface.
- Enable immediate leaving.
- Set multicast forwarding entries and the aging time of router interfaces.
- Enable IGMP ring network forwarding on the interface.

Basic functions of Layer 2 multicast provide Layer 2 multicast common features, which must be used on the SNR-S212i-8POE enabled with IGMP Snooping or IGMP MVR.

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 set 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 IGMP Snooping aging time. 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 forwarding 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 forwarding entry when receiving IGMP Report packets. The timer of the multicast forwarding entry will be updated when an IGMP Report packet is received.

Immediate leaving

On Layer 2 switch running multicast function, the system will not delete the corresponding multicast forwarding entry immediately, but wait until the entry is aged after sending Leave packets. Enable this function to delete the corresponding multicast forwarding entry quickly when there are a large number of downstream users and adding or leaving is more frequently required.



Note

Only IGMP v2/v3 version supports immediate leaving.

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, etc.

9.1.3 IGMP Snooping

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 SNR-S212i-8POE to monitor IGMP sessions between the host and multicast router. When monitoring a group of IGMP Report from host, the SNR-S212i-8POE will add host-related interface to the forwarding entry of this group. Similarly, when a forwarding entry reaches the aging time, the SNR-S212i-8POE will delete host-related interface from forwarding entry.

IGMP Snooping forwards multicast data through Layer 2 multicast forwarding entry. When receiving multicast data, the SNR-S212i-8POE will forward them directly according to the corresponding receiving interface of the multicast forwarding entry, instead of flooding them to all interfaces, to save bandwidth of the SNR-S212i-8POE effectively.

IGMP Snooping establishes a Layer 2 multicast forwarding table, of which entries can be learnt dynamically or configured manually.



Note

Currently, the SNR-S212i-8POE supports up to 1024 Layer 2 multicast entries.

9.2 Configuring IGMP basis

9.2.1 Preparing for configurations

Scenario

Basic functions of Layer 2 multicast provide common features of Layer 2 multicast, and must be used on the SNR-S212i-8POE enabled with IGMP Snooping or IGMP MVR.

Prerequisite

- Create VLANs.
- Add related interfaces to VLANs.

9.2.2 Default configurations of Layer 2 multicast basic functions

Default configurations of Layer 2 multicast basic functions are as below.

Function	Default value
IGMP immediate leaving status	Disable
Multicast forwarding entry aging time	300s
Interface IGMP ring network forwarding status	Disable

9.2.3 Configuring basic functions of Layer 2 multicast

Configure basic functions of Layer 2 multicast for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#i gmp mrouter vl an vl an- i d i nterface- type i nterface- number</code>	(Optional) configure the multicast route interface.
3	<code>NAG(confi g)#i gmp i mmedi ate- l eave i nterface- type i nterface- number vl an vl an- l i st</code>	(Optional) configure immediate leaving on the interface+VLAN.
4	<code>NAG(confi g)#i gmp t i meout { <i>period</i> <i>i nfi ni te</i> }</code>	(Optional) configure the aging time of multicast forwarding entries. The aging time configured takes effect on all dynamically learnt router interfaces and multicast forwarding entries.
5	<code>NAG(confi g)#i gmp r i ng i nterface- type i nterface- number- l i st</code>	(Optional) enable IGMP ring network forwarding on the interface.

Step	Command	Description
6	<code>NAG(config)#mac-address-table static multicast mac-address vlan vlan-id interface-type interface-number-list</code>	(Optional) configure the interface to join static multicast group. An interface is added to the multicast group through the IGMP Report packet send by a host. You can also manually add it to a multicast group.

9.2.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>NAG#show igmp mrouter</code>	Show configurations of the multicast route interface.
2	<code>NAG#show igmp immediate-leave [interface-type interface- number]</code>	Show configuration of immediate leaving on Layer 2 multicast.
3	<code>NAG#show igmp statistics [interface-type interface- number]</code>	Show IGMP statistics.

9.3 Configuring IGMP Snooping

9.3.1 Preparing for configurations

Scenario

As shown in Figure 9-5, multiple hosts belonging to a VLAN receive data from the multicast source. 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.

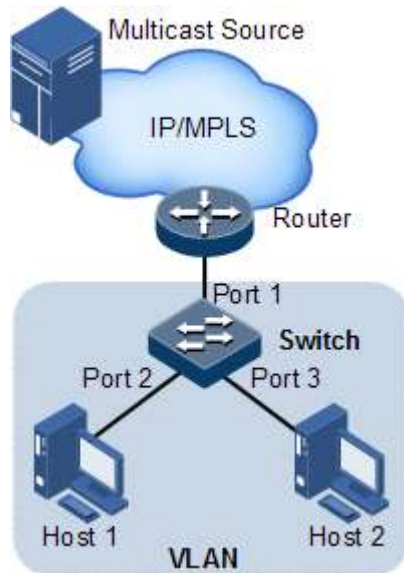


Figure 9-5 IGMP Snooping networking

Prerequisite

- Create VLANs
- Add related interfaces to VLANs.

9.3.2 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

9.3.3 Configuring IGMP Snooping

Configure IGMP Snooping for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#1 gmp snoopi ng</code>	Enable global IGMP Snooping.
3	<code>NAG(confi g)#1 gmp snoopi ng vl an vl an- list</code>	Enable VLAN-based IGMP Snooping.

Step	Command	Description
4	<code>NAG(config)#mac-address-table static multicast mac-address vlan vlan-id interface-type interface-number-list</code>	(Optional) configure the static multicast forwarding table. An interface is added to the multicast group through the IGMP Report packet send by a host. You can also manually add it to a multicast group.

9.3.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>NAG#show igmp snooping [vlan vlan-list]</code>	Show configurations of IGMP Snooping.
2	<code>NAG#show igmp snooping member [interface-type interface-number vlan vlan-id]</code>	Show information about multicast group members of IGMP Snooping.

9.4 Configuration examples

9.4.1 Example for configuring IGMP Snooping

Networking requirements

As shown in Figure 9-6, Port 1 on the Switch connects with the multicast router; Port 2 and Port 3 connect users. All multicast users belong to the same VLAN 10; you need to configure IGMP Snooping on the switch to receive multicast data with the address 234.5.6.7.

When the PC and set-top box are added into the same multicast group, the switch receives two IGMP Report packets and only sends one of them to the multicast router. The IGMP Query packet sent by multicast will no longer be forwarded downstream, but the switch periodically forwards IGMP Query packets.

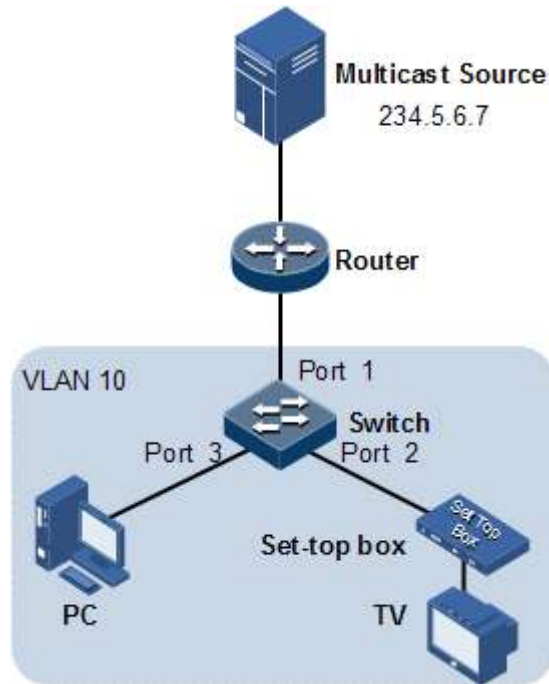


Figure 9-6 IGMP Snooping networking

Configuration steps

Step 1 Create VLANs and add interfaces to VLANs.

```
NAG#confi g
NAG(confi g)#create vl an 10 active
NAG(confi g)#i nterface port 1
NAG(confi g-port)#swi tchport mode trunk
NAG(confi g-port)#swi tchport trunk native vl an 10
NAG(confi g-port)#exi t
NAG(confi g)#i nterface port 2
NAG(confi g-port)#swi tchport access vl an 10
NAG(confi g-port)#exi t
NAG(confi g)#i nterface port 3
NAG(confi g-port)#swi tchport access vl an 10
NAG(confi g-port)#exi t
```

Step 2 Enable IGMP Snooping.

```
NAG(confi g)#i gmp snoopi ng
NAG(confi g)#i gmp snoopi ng vl an 10
```

Checking results

Use the following command to show configurations of IGMP Snooping.

```
NAG#show i gmp snoopi ng
```

```
igmp snooping          : Enable
igmp snooping active vlan : 10
igmp aging time(s)    : 300
igmp ring              : --
```

Use the following command to show information about IGMP Snooping multicast group members.

```
NAG#show igmp snooping member vlan 10
*: ring port
Port          GroupID          Live-time
-----
port 2        234.5.6.7        270
port 3        234.5.6.7        270
```

9.4.2 Example for configuring ring network multicast

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 9-7, Port 1 and Port 2 on Switch A, Port 2 and Port 3 on Switch B, Port 2 and Port 4 on Switch C form a physical ring. Multicast traffic is input from Port 1 on Switch B. The user demands multicast stream through Port 5 and Port 6 on Switch C. By doing this, whichever links fail in the Switch, it will not affect user's on-demand multicast stream.

When using single Ethernet ring to provide multicast services, you can adopt IGMP Snooping to receive the multicast stream.

The following example shows that STP provides ring network detection and IGMP Snooping provides multicast function.

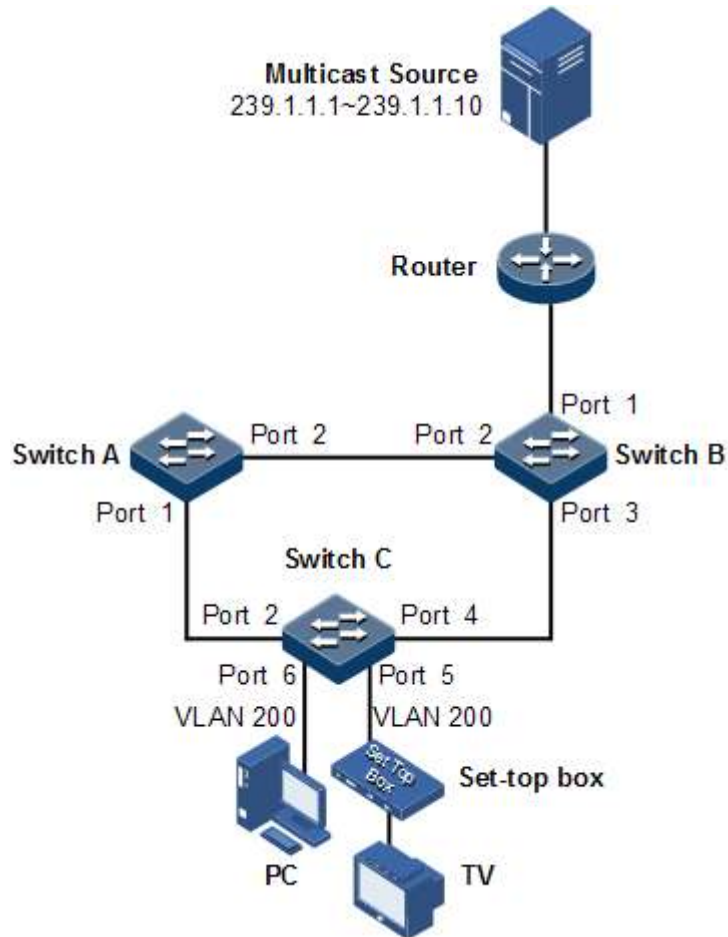


Figure 9-7 Ring network multicast networking

Configuration steps

Step 1 Enable STP function, create a VLAN, and add interfaces into the VLAN.

Configure Switch A.

```

SwitchA#confi g
SwitchA(config)#spanning-tree enable
SwitchA(config)#spanning-tree mode stp
SwitchA(config)#I nterface port 1
SwitchA(config-port)#swi tchport mode trunk
SwitchA(config-port)#swi tchport trunk nati ve vl an 200
SwitchA(config-port)#exi t
SwitchA(config)#I nterface port 2
SwitchA(config-port)#swi tchport mode trunk
SwitchA(config-port)#swi tchport trunk nati ve vl an 200

```

Configure Switch B.

```
SwitchB#confi g
SwitchB(config)#spanning-tree enable
SwitchB(config)#spanning-tree mode stp
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk native vlan 200
SwitchB(config-port)#exit
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk native vlan 200
```

Configure Switch C.

```
SwitchC#confi g
SwitchC(config)#spanning-tree enable
SwitchC(config)#spanning-tree mode stp
SwitchC(config)#interface port 2
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#switchport trunk native vlan 200
SwitchC(config-port)#exit
SwitchC(config)#interface port 4
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#switchport trunk native vlan 200
```

Step 2 Enable IGMP Snooping and IGMP ring network forwarding.

Configure Switch A.

```
SwitchA(config)#igmp ring port-list 1,2
SwitchA(config)#igmp snooping
SwitchA(config)#igmp snooping vlan 200
```

Configure Switch B.

```
SwitchB(config)#igmp ring port-list 2,3
SwitchB(config)#igmp snooping
SwitchB(config)#igmp snooping vlan 200
```

Configure Switch C.

```
SwitchC(config)#igmp ring port-list 2,4
SwitchC(config)#igmp snooping
SwitchC(config)#igmp snooping vlan 200
```

Checking results

Disconnect any link in the ring, and check whether the multicast flow can be received normally.

10 Security

This chapter describes basic principle and configuration of security and provides related configuration examples, including the following sections.

- Secure MAC address
- Dynamic ARP inspection
- RADIUS
- TACACS+
- Storm control
- 802.1x
- IP Source Guard
- PPPoE+

10.1 Secure MAC address

10.1.1 Introduction

Port security MAC is used for the switching device on the edge of the network user side, which can ensure the security of access data in some interface, control the input packets according to source MAC address.

You can enable port security MAC to limit and distinguish which users can access the network through secure interfaces. Only secure MAC addresses can access the network, unsecure MAC addresses will be dealt with as configured interface access violation mode.

Secure MAC address classification

Secure MAC addresses supported by the device are divided into the following three categories:

- Static secure MAC address

Static secure MAC address is configured by user on secure interface manually; this MAC address will take effect when port security MAC is enabled. Static secure MAC address does not age and supports loading configuration.

- Dynamic secure MAC address

The dynamic secure MAC address is learnt by the device. You can set the learnt MAC address to secure MAC address in the range of the maximum number of learnt MAC address. The dynamic secure MAC addresses ages and does not support configuration load.

Dynamic secure MAC address can be converted to Sticky secure MAC address if necessary, so as not to be aged and support configuration auto-loading.

- Sticky secure MAC address

Sticky secure MAC address is generated from the manual configuration of user in secure interface or converted from dynamic secure MAC address. Different from static secure MAC address, Sticky secure MAC address needs to be used in conjunction with Sticky learning. The system supports loading configurations:

- When Sticky learning is enabled, Sticky secure MAC address will take effect and this address will not be aged.
- When Sticky learning is disabled, Sticky secure MAC address will lose effectiveness and be saved only in the system.



Note

- When Sticky learning is enabled, all dynamic secure MAC addresses learnt from an interface will be converted to Sticky secure MAC addresses.
- When Sticky learning is disabled, all Sticky secure MAC addresses (including dynamic secure MAC addresses and manually configured Sticky secure MAC addresses) on an interface will be converted to dynamic secure MAC addresses.

Processing mode for violating secure MAC address

When the number of secure MAC addresses has already reached the maximum number, the strange source MAC address packets inputting will be regarded as violation operation. For the illegal user access, there are different processing modes to configure the switch according to secure MAC violation policy:

- Protect mode: for illegal access users, secure interface will discard the user's packets directly.
- Restrict mode: for illegal access users, secure interface will discard the user's packets, and the console will print Syslog information and send alarm to the network management system.
- Shutdown mode: for illegal access users, secure interface will discard the user's packets, and the console will print Syslog information and send alarm to the network management system and then shutdown the secure interface.



Caution

When the MAC address is in drift, that is, the secure interface A receives one user access corresponding a secure MAC address on secure interface B, secure interface A will take it as violation processing.

10.1.2 Preparing for configurations

Scenario

To ensure the security of data accessed by the interface of the switch, you can control the input packets according to source MAC address. With secure MAC address, you can

configure permitting specified users to access the interface, or permitting specified number of users to access from this interface only. However, when the number of users exceeds the limit, the accessed packets will be processed in accordance with secure MAC address violation policies.

Prerequisite

N/A

10.1.3 Default configurations of secure MAC address

Default configurations of port security MAC are as below.

Function	Default value
Interface secure MAC	Disable
Aging time of dynamic secure MAC address	300s
Restoration time of port security MAC	Disable, namely, no restoration
Dynamic secure MAC Sticky learning	Disable
Port secure MAC Trap	Disable
Port secure MAC violation processing mode	Protect
Maximum number of port security MAC	1

10.1.4 Configuring basic functions of secure MAC address



Caution

- We do not recommend enabling port security MAC on member interfaces of the LAG.
- We do not recommend using MAC address management function to configure static MAC addresses when port security MAC is enabled.
- When the 802.1x interface adopts a MAC address-based authentication mode, port security MAC and 802.1x are mutually exclusive. We do not recommend co-configuring them concurrently.
- Port security MAC and interface-/interface VLAN-based MAC number limit are mutually exclusive, which cannot be configured concurrently.

Configure basic functions of secure MAC address for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#i nterface port port-id</code>	Enter physical layer interface configuration mode.
3	<code>NAG(confi g-port)#swi tchport port-securi ty</code>	Enable port security MAC.

Step	Command	Description
4	NAG(config-port)#swi tchport port-securi ty maxi mum <i>maxi mum</i>	(Optional) configure the maximum number of secure MAC addresses.
5	NAG(config-port)#swi tchport port-securi ty vi ol ati on { protect restri ct shutdown }	(Optional) configure secure MAC violation mode.
6	NAG(config-port)#no port- securi ty shutdown	(Optional) re-enable the interface which is shut down due to violating the secure MAC address.
7	NAG(config)#port-securi ty recovery-ti me <i>second</i>	(Optional) configure the restoration time of port security MAC.



Note

When secure MAC violation policy is in Shutdown mode, you can use this command to re-enable this interface which is shut down due to violating secure MAC address. When the interface is Up, the configured secure MAC violation mode will continue to be valid.

10.1.5 Configuring static secure MAC address

Configure static secure MAC address for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(config)#i nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(config-port)#swi tchport port-securi ty	Enable port security MAC.
4	NAG(config-port)#swi tchport port-securi ty mac-address <i>mac-address vl an vl an-id</i>	Configure static secure MAC address.

10.1.6 Configuring dynamic secure MAC address

Configure dynamic secure MAC address for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(config)#port-securi ty agi ng-ti me <i>peri od</i>	(Optional) configure the aging time of dynamic secure MAC address.
3	NAG(config)#i nterface port <i>port-id</i>	Enter physical layer interface configuration mode.

Step	Command	Description
4	NAG(config-port)#switchport port-security	(Optional) enable port dynamic security MAC learning.
5	NAG(config-port)#switchport port-security aging-type { absolute inactivity }	(Optional) configure the aging type of port security MAC addresses.
6	NAG(config-port)#switchport port-security trap enable	(Optional) enable port security MAC Trap.



Note

The **switchport port-security** command can enable port security MAC as well as dynamic secure MAC learning at the same time.


10.1.7 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 in anomaly.

Configure Sticky secure MAC address for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#config	Enter global configuration mode.
2	NAG(config)#interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(config-port)#switchport port-security	Enable port security MAC.
4	NAG(config-port)#switchport port-security mac-address sticky	Enable Sticky secure MAC learning.  Note After Sticky secure MAC address learning is enabled, dynamic secure MAC address will be converted to Sticky secure MAC address; the manually configured Sticky secure MAC address will take effect.
5	NAG(config-port)#switchport port-security mac-address sticky <i>mac-address</i> vlan <i>vlan-id</i>	(Optional) manually configure Sticky secure MAC addresses.

10.1.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show port-security [port-list port-list]	Show configurations of port security MAC on the interface.
2	NAG#show port-security mac-address [port-list port-list]	Show configurations of secure MAC address and secure MAC address learning.

10.1.9 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	NAG(config-port)#clear port-security { all configured dynamic sticky }	Clear a specified secure MAC address type on a specified interface.

10.1.10 Example for configuring secure MAC address

Networking requirements

As shown Figure 10-1, the switch connects 3 user networks. To ensure the security of switch interface access data, the configuration is as below.

- Port 1 permits 3 users to access network at most. The MAC address of one user is specified to 0000.0000.0001. The other 2 users dynamically learn the MAC addresses; the NView NNM system will receive Trap information once the user learns a MAC address. Violation mode is set to Protect and the aging time of the two learned MAC addresses is set to 10min.
- Port 2 permits 2 users to access network at most. The 2 user MAC addresses are confirmed through learning; once they are confirmed, they will not be aged. Violation mode is set to Restrict mode.
- Port 3 permits 1 user to access network at most. The specified user MAC address is 0000.0000.0002. Whether to age user MAC addresses can be controlled. Violation mode adopts Shutdown mode, and the violated interface cannot be automatically restored.

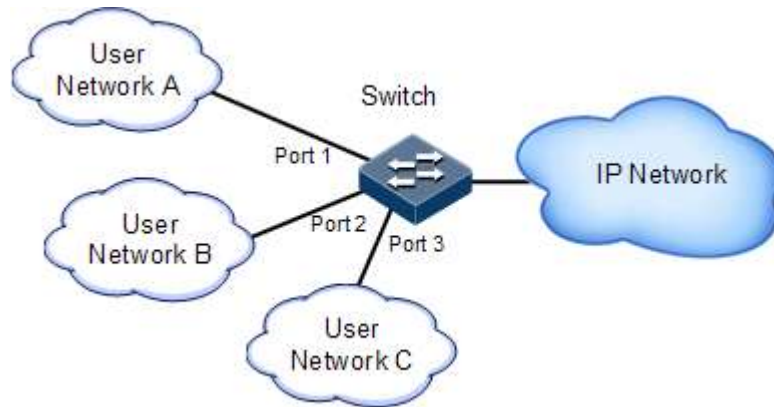


Figure 10-1 Configuring secure MAC address

Configuration steps

Step 1 Configure the secure MAC address of Port 1.

```

NAG#confi g
NAG(confi g)#I nterface port 1
NAG(confi g-port)#swi tchport port-securi ty
NAG(confi g-port)#swi tchport port-securi ty maxi mum 3
NAG(confi g-port)#swi tchport port-securi ty mac-address 0000.0000.0001 vi an
1
NAG(confi g-port)#swi tchport port-securi ty vi ol ati on protect
NAG(confi g-port)#swi tchport port-securi ty trap enable
NAG(confi g-port)#exi t
NAG(confi g)#port-securi ty agl ng-ti me 10
  
```

Step 2 Configure the secure MAC address of Port 2.

```

NAG(confi g)#I nterface port 2
NAG(confi g-port)#swi tchport port-securi ty
NAG(confi g-port)#swi tchport port-securi ty maxi mum 2
NAG(confi g-port)#swi tchport port-securi ty mac-address sti cky
NAG(confi g-port)#swi tchport port-securi ty vi ol ati on restri ct
NAG(confi g-port)#exi t
  
```

Step 3 Configure the secure MAC address of Port 3.

```

NAG(confi g)#I nterface port 3
NAG(confi g-port)#swi tchport port-securi ty
NAG(confi g-port)#swi tchport port-securi ty maxi mum 1
NAG(confi g-port)#swi tchport port-securi ty mac-address sti cky
0000.0000.0002 vi an 1
NAG(confi g-port)#swi tchport port-securi ty mac-address sti cky
  
```

```
NAG(config-port)#switchport port-security violation shutdown
```

Checking results

Use the **show port-security [port-list port-list]** command to show configurations of port security MAC.

```
NAG#show port-security port-list 1-3
Port security aging time: 10 (mins)
Port security recovery time: Disable (s)
port status Max-Num Cur-Num His-MaxNum vi o-Count vi o-acti on Dynami c-
Trap Agi ng-Type
-----
port1  Enable  3      1      0      0      protect  Enable
--
port2  Enable  2      0      0      0      restri ct  Di sable
--
port3  Enable  1      1      0      0      shutdown  Di sable
--
```

Use the **show port-security mac-address** command to show secure MAC address and configurations of secure MAC address learning on an interface.

```
NAG#show port-security mac-address
VLAN  Securi ty-MAC-Address  Flag  Port  Age(mi n)
-----
2     0000.0000.0001         stati c  port1  --
2     0000.0000.0002         stick y  port3  --
```

10.2 Dynamic ARP inspection

10.2.1 Introduction

Dynamic ARP inspection is used for ARP protection of unsecure interface and prevents from responding ARP packets which do not meet the requirements, thus preventing ARP spoofing attack on the network.

There are 2 modes for dynamic ARP inspection:

- Static binding mode: set the binding manually.
- Dynamic binding mode: in cooperation with the DHCP snooping to generate dynamic binding. When DHCP Snooping entry is changed, the dynamic ARP inspection will also update dynamic binding entry synchronously.

The ARP inspection table, which is used for preventing ARP attacks, consists of DHCP snooping entries and statically configured ARP inspection rules, including IP address, MAC

address, and VLAN binding information. In addition, the ARP inspection table associates this information with specific interfaces. The dynamic ARP inspection binding table supports the combination of following entries:

- Interface+IP
- Interface+IP+MAC
- Interface+IP+VLAN
- Interface+IP+MAC+VLAN

Dynamic ARP inspection interfaces are divided into the following two types according to trust status:

- Trusted interface: the interface will stop ARP inspection, which conducts no ARP protection on the interface. All ARP packets are allowed to pass.
- Untrusted interface: the interface takes ARP protection. Only ARP packets that match the binding table rules are allowed to pass. Otherwise, they are discarded.

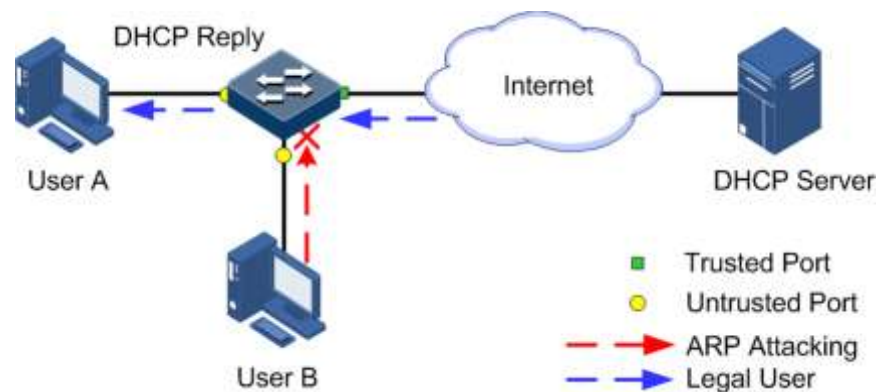


Figure 10-2 Principle of dynamic ARP inspection

Figure 10-2 shows the principle of dynamic ARP inspection. When the SNR-S212i-8POE receives an ARP packet, it compares the source IP address, source MAC address, interface number, and VLAN information of the ARP packet with the DHCP Snooping entry information. If matched, it indicates that it is a legal user and the ARP packets are permitted to pass. Otherwise, it is an ARP attack and the ARP packet is discarded.

Dynamic ARP inspection also provides rate limiting on ARP packets to prevent unauthorized users from attacking the SNR-S212i-8POE by sending a large number of ARP packets to the SNR-S212i-8POE.

- When the number of ARP packets received by an interface every second exceeds the threshold, the system will regard that the interface receives an ARP attack, and then discard all received ARP packets to avoid 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.

10.2.2 Preparing for configurations

Scenario

Dynamic ARP inspection is used to prevent the common ARP spoofing attacks on the network, which isolates the ARP packets with unsafe sources. Trust status of an interface depends whether it trust ARP packets. However, the binding table decides whether the ARP packets meet requirement.

Prerequisite

Enable DHCP Snooping if there is a DHCP user.

10.2.3 Default configurations of dynamic ARP inspection

Default configurations of dynamic ARP inspection are as below.

Function	Default value
Dynamic ARP inspection interface trust status	Untrusted
Dynamic ARP inspection static binding	Disable
Dynamic ARP inspection dynamic binding	Disable
Dynamic ARP inspection static binding table	N/A
Dynamic ARP inspection protection VLAN	All VLANs
Interface rate limiting on ARP packets	Disable
Interface rate limiting on ARP packets	60 pps
Auto-recovery rate limiting on ARP packets	Disable
Auto-recovery time for rate limiting on ARP packets	30s

10.2.4 Configuring trusted interfaces of dynamic ARP inspection

Configure trusted interfaces of dynamic ARP inspection for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#i nterface port port-id</code>	Enter physical layer interface configuration mode.
3	<code>NAG(confi g-port)#i p arp- i nspecti on trust</code>	Set the interface to a trusted interface. Use the no ip arp-inspection trust command to set the interface to an untrusted interface, that is, the interface does not trust the ARP packet.

10.2.5 Configuring static binding of dynamic ARP inspection

Configure static binding of dynamic ARP inspection for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#i p arp-i nspecti on stati c-confi g	Enable global static ARP binding.
3	NAG(confi g)#i p arp-i nspecti on bi ndi ng ip-address [mac-address] [vl an vlan-id] port port-id	Configure the static binding.

10.2.6 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 SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#i p arp-i nspecti on dhcp-snoopi ng	Enable global dynamic ARP binding.

10.2.7 Configuring protection VLAN of dynamic ARP inspection

Configure protection VLAN of dynamic ARP inspection for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#i p arp-i nspecti on dhcp-snoopi ng	Enable global dynamic ARP binding.
3	NAG(confi g)#i p arp-i nspecti on vl an vlan-li st	Configure protection VLAN of dynamic ARP inspection.

10.2.8 Configuring rate limiting on ARP packets on interface

Configure rate limiting on ARP packets on the interface for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.

Step	Command	Description
2	NAG(config)# interface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(config-port)# ip arp-rate- limit enable	Enable interface ARP packet rate limiting.
4	NAG(config-port)# ip arp-rate- limit rate <i>rate-value</i>	Configure rate limiting on ARP packets on the interface.

10.2.9 Configuring auto-recovery time for rate limiting on ARP packets

Configure the auto-recovery time for rate limiting on ARP packets for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(config)# ip arp-rate-limi t recover enable	Enable auto-recovery for rate limiting on ARP packets.
3	NAG(config)# ip arp-rate-limi t recover time <i>seconds</i>	Configure the auto-recovery time for rate limiting on ARP packets.

10.2.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG# show ip arp-i nspecti on	Show configurations of dynamic ARP inspection.
2	NAG# show ip arp-i nspecti on bi ndi ng [port <i>port-id</i>]	Show information about the dynamic ARP inspection binding table.
3	NAG# show ip arp-rate-limi t	Show configurations of rate limiting on ARP packets.

10.2.11 Example for configuring dynamic ARP inspection

Networking requirements

To prevent ARP attacks, configure dynamic ARP inspection function on Switch A, as shown in Figure 10-3.

- Uplink Port 3 permits all ARP packets to pass.

- Uplink Port 1 permits ARP packets with specified IP address 10.10.10.1 to pass.
- Other interfaces permit ARP packets meeting DHCP Snooping learnt dynamic binding to pass.
- Downlink Port 2 configures rate limiting on ARP packets. The rate threshold is set to 20 pps and rate limiting recovery time is set to 15s.

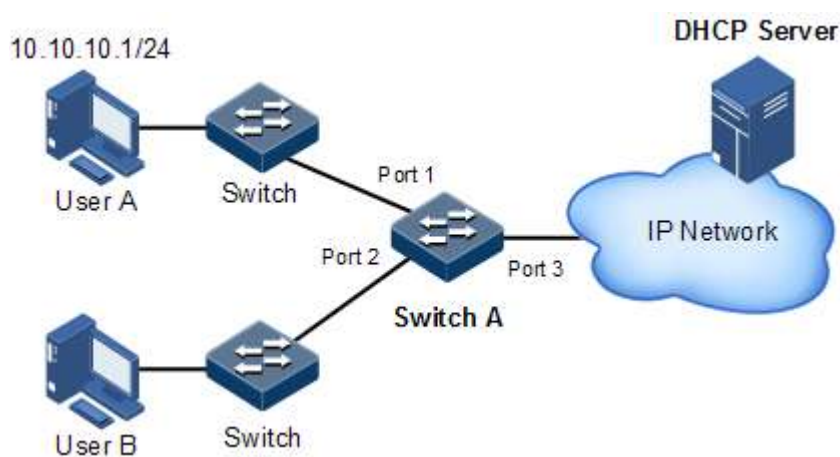


Figure 10-3 Configuring dynamic ARP inspection

Configuration steps

Step 1 Set Port 3 to the trusted interface.

```
NAG#confi g
NAG(confi g)#i nterface port 3
NAG(confi g-port)#i p arp-i nspecti on trust
NAG(confi g-port)#exi t
```

Step 2 Configure static binding.

```
NAG(confi g)#i p arp-i nspecti on stati c-confi g
NAG(confi g)#i p arp-i nspecti on bi ndi ng 10. 10. 10. 1 port 1
```

Step 3 Enable dynamic ARP binding.

```
NAG(confi g)#i p dhcp snoopi ng
NAG(confi g)#i p arp-i nspecti on dhcp-snoopi ng
```

Step 4 Configure rate limiting for ARP packets on an interface.

```
NAG(confi g)#i nterface port 2
```

```
NAG(config-port)#ip arp-rate-limit rate 20
NAG(config-port)#ip arp-rate-limit enable
NAG(config-port)#exit
```

Step 5 Configure auto-recovery for rate limiting on ARP packets.

```
NAG(config)#ip arp-rate-limit recover time 15
NAG(config)#ip arp-rate-limit recover enable
```

Checking results

Use the **show ip arp-inspection** command to show configurations of interface trust status static/dynamic ARP binding.

```
NAG#show ip arp-inspection
Static Config ARP Inspection: Enable
DHCP Snooping ARP Inspection: Enable
ARP Inspection Protect VLAN : all
Bind Rule Num          : 0
Vlan Rule Num          : 0
Bind Acl Num           : 0
Vlan Acl Num           : 0
Remained Acl Num       : 512
Port      Trust
-----
port1     no
port2     no
port3     yes
port4     no
.....
```

Use the **show ip arp-inspection binding** command to show information about the dynamic ARP binding table.

```
NAG#show ip arp-inspection binding
Ip Address      Mac Address  VLAN  Port      Type      Inhw
-----
10.10.10.1     --          --    port1     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.

```

NAG#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
-----
1      Disabled        60               No
2      Enabled         20               Yes
3      Disabled        60               No
4      Disabled        60               No
.....

```

10.3 RADIUS

10.3.1 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 client of 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 to authenticate users through RADIUS. When logging in, a user sends a starting account packet to the RADIUS accounting server, according to the accounting policy to send update packet to the RADIUS server. When logging off, the user sends a stopping account packet to the RADIUS accounting server, and the packet includes user online time. The RADIUS accounting server can record the access time and operations for each user through packets.

10.3.2 Preparing for configurations

Scenario

You can deploy RADIUS server on the network to take authentication and accounting to control user access to device and network. This device can be used as agent of RADIUS server, which authorizes user accessing according to feedback from RADIUS.

Prerequisite

N/A

10.3.3 Default configurations of RADIUS

Default configurations of RADIUS are as below.

Function	Default value
RADIUS accounting	Disable
IP address of RADIUS server	0.0.0.0
IP address of RADIUS accounting server	0.0.0.0
Port ID of RADIUS authentication server	1812
Port ID of RADIUS accounting server	1813
Shared key used for communication with RADIUS accounting server	N/A
Accounting failure processing policy	Online
Period for sending update packet	0

10.3.4 Configuring RADIUS authentication

Configure RADIUS authentication for the SNR-S212i-8POE as below.


Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#I nterface i p i f- number	Enter Layer 3 interface configuration mode.
3	NAG(confi g-i p)#I p address i p- address [i p-mask] [v l a n- l i s t]	Configure an IPv4 address.
4	NAG(confi g-i p)#end	Return to privileged EXEC mode.
5	NAG#radi us [backup] i p- address [auth-port port- number]	Assign the IP address and port ID for RADIUS authentication server. Configure the backup parameter to assign the backup RADIUS authentication server.
6	NAG#radi us-key string	Configure the shared key for RADIUS authentication.
7	NAG#user l o g i n { l o c a l -radi us l o c a l -user radi us-l o c a l [server-no-response] radi us-user }	Configure users to perform login authentication through RADIUS.

Step	Command	Description
8	NAG#enable login { local -radius local -user radius-local [server-no-response] radius-user }	Set the authentication mode for users to enter privileged EXEC mode to RADIUS.

10.3.5 Configuring RADIUS accounting

Configure RADIUS accounting for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#I nterface i p <i>if-number</i>	Enter Layer 3 interface configuration mode.
3	NAG(confi g-i p)#I p address <i>ip-address</i> [sub] [<i>ip-mask</i>] [<i>vlan-list</i>]	Configure an IPv4 address.
4	NAG(confi g-i p)#end	Return to privileged EXEC mode.
5	NAG#aaa accounti ng logi n enable	Enable RADIUS accounting.
6	NAG#radi us [backup] accounti ng-server <i>ip-</i> <i>address</i> [<i>account-port</i>]	Assign the IP address and UDP port ID for the RADIUS accounting server. Configure the backup parameter to assign the backup RADIUS accounting server.
7	NAG#radi us accounti ng- server key <i>string</i>	Configure the shared key to communicate with the RADIUS accounting server. The shared key must be identical to the one configured on the RADIUS accounting server. Otherwise, accounting will fail.
8	NAG#aaa accounti ng fail { offli ne onli ne }	Configure the processing policy for accounting failure.
9	NAG#aaa accounti ng update <i>period</i>	Configure the period for sending accounting update packets. If it is configured as 0, no accounting update packet is sent. By default, it is 0.



Note

The RADIUS accounting server can record access time and operation for each user through accounting starting packets, update packets and accounting end packets.

10.3.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show radi us-server	Show configurations of the RADIUS server.
2	NAG#show aaa	Show configurations of the accounting server.

10.3.7 Example for configuring RADIUS

Networking requirements

As shown in Figure 10-4, you need to configure RADIUS authentication and accounting on switch A to authenticate login users and record their operations. The period for sending update packets is 2 set to minutes. The user will be offline if the accounting fails.

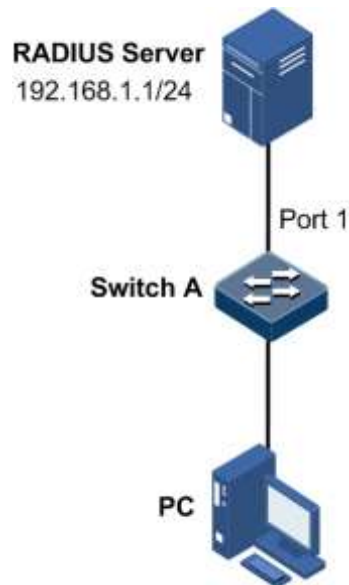


Figure 10-4 Configuring RADIUS

Configuration steps

Step 1 Authenticate login users through RADIUS.

```
NAG#radi us 192.168.1.1
NAG#radi us-key NAG
NAG#user login radi us-user
NAG#enabl e login local -radi us
```

Step 2 Account login users through RADIUS.

```
NAG#aaa accounting login enable
NAG#radius accounting-server 192.168.1.1
NAG#radius accounting-server key NAG
NAG#aaa accounting fail offline
NAG#aaa accounting update 2
```

Checking results

Use the **show radius-server** command to show configurations of the RADIUS server.

```
NAG#show radius-server
Authentication server IP      : 192.168.1.1 port: 1812
Backup authentication server IP: 0.0.0.0 port: 1812
Authentication server key    : abcd
Accounting server IP        : 192.168.1.1 port: 1813
Backup accounting server IP  : 0.0.0.0 port: 1813
Accounting server key       : abcd
```

Use the **show aaa** command to show configurations of RADIUS accounting.

```
NAG#show aaa
Authentication server IP:      192.168.1.1 port: 1812
Accounting login           : enable
Update interval (m)       : 2
Accounting fail policy    : offline
dot1x user login method: radius
```

10.4 TACACS+

10.4.1 Introduction

Terminal Access Controller Access Control System (TACACS+) is a kind of network access authentication protocol similar to RADIUS. The differences between them are:

- TACACS+ uses TCP port 49, which has higher transmission reliability compared with UDP port used by RADIUS.
- TACACS+ encrypts the holistic of packets except the standard head of TACACS+, and there is a field to show whether the data packets are encrypted in the head of packet. Compared to RADIUS user password encryption, the TACACS+ is much safer.
- TACACS+ authentication function is separated from authorization and accounting functions; it is more flexible in deployment.

In a word, TACACS+ is safer and more reliable than RADIUS. However, as an open protocol, RADIUS is more widely used.

10.4.2 Preparing for configurations

Scenario

To control users accessing to the SNR-S212i-8POE and the network, you can authenticate and account users by deploying the TACACS+ server on the network. Compared with RADIUS, TACACS+ is safer and more reliable. The SNR-S212i-8POE can be used as the agent of the TACACS+ server, controlling users according to feedback result from the TACACS+ server.

Prerequisite

N/A

10.4.3 Default configurations of TACACS+

Default configurations of TACACS+ are as below.

Function	Default value
TACACS+ function	Disable
Login mode	local-user
IP address of TACACS+ authentication server	0.0.0.0, shown as "--"
IP address of TACACS+ accounting server	0.0.0.0, shown as "--"
Shared key used for communication with TACACS+ accounting server	N/A
Accounting failure processing policy	Online
Period for sending update packet	0

10.4.4 Configuring TACACS+ authentication

Configure TACACS+ authentication for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#tacacs-server [backup] ip-address</code>	Assign the IP address and port ID for the TACACS+ authentication server. Configure the backup parameter to assign the backup TACACS+ authentication server.
2	<code>NAG#tacacs-server key string</code>	Configure the shared key for TACACS+ authentication.
3	<code>NAG#user login { local - tacacs local-user tacacs-local [server-no- response] tacacs-user }</code>	Configure users to perform login authentication through TACACS+.

Step	Command	Description
4	<code>NAG#enable login { local - tacacs local -user tacacs-local [server-no-response] tacacs-user }</code>	Set the authentication mode for users to enter privileged EXEC mode to TACACS+.

10.4.5 Configuring TACACS+ accounting

Configure TACACS+ accounting for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#aaa accounting login enable</code>	Enable TACACS+ accounting.
2	<code>NAG#tacacs [backup] accounting-server ip-address</code>	Assign the IP address and UDP port ID for the TACACS+ accounting server. Configure the backup parameter to assign the backup TACACS+ accounting server.
3	<code>NAG#tacacs-server key string</code>	Configure the shared key to communicate with the TACACS+ accounting server.
4	<code>NAG#aaa accounting fail { offline online }</code>	Configure the processing policy for accounting failure.
5	<code>NAG#aaa accounting update period</code>	Configure the period for sending accounting update packets.

10.4.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>NAG#show tacacs-server</code>	Show configurations of the TACACS+ authentication server.
2	<code>NAG#show aaa</code>	Show configurations of the accounting server.

10.4.7 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	<code>NAG#clear tacacs statistics</code>	Clear TACACS+ statistics.

10.4.8 Example for configuring TACACS+

Networking requirements

As shown in Figure 10-5, configure TACACS+ authentication on Switch A to authenticate users who log in to the SNR-S212i-8POE.

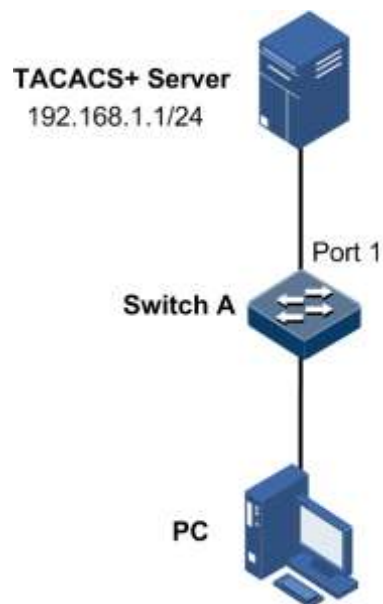


Figure 10-5 Configuring TACACS+

Configuration steps

Authenticate login users through TACACS+.

```
NAG#tacacs-server 192.168.1.1
NAG#tacacs-server key NAG
NAG#user login tacacs-user
NAG#enable login local -tacacs
```

Checking results

Use the **show tacacs-server** command to show TACACS+ configurations.

```
NAG#show tacacs-server
Server Address           : 192.168.1.1
Backup Server Address    : --
Sever Shared Key         : NAG
Accounting server Address : --
Backup Accounting server Address: --
Total Packet Sent        : 0
Total Packet Recv        : 0
```

Num of Error Packet : 0

10.5 Storm control

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 occupies much network bandwidth. Broadcast storm can degrade network performance and impact forwarding of unicast packets or even lead to communication halt.

Restricting broadcast flow generated from network on Layer 2 device can suppress broadcast storm and ensure common unicast forwarding normally.

Occurrence of broadcast storm

The following flows may cause broadcast flow:

- Unknown unicast packets: unicast packets of which the destination MAC is not in the MAC address table, namely, the Destination Lookup Failure (DLF) packets. If these packets are excessive in a period, the system floods them and broadcast storm may occur.
- Unknown multicast packets: the SNR-S212i-8POE does not support multicast nor have 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.

Principle of storm control

Storm control allows an interface to filter broadcast packets received by the interface. After storm control is enabled, when the number of received broadcast packets reaches the pre-configured threshold, the interface will automatically discard the received packets. If storm control is disabled or if the number of received broadcast packets does not reach the pre-configured threshold, the broadcast packets are broadcasted to other interfaces of the switch properly.

Types of storm control

Storm controls is performed in the following forms:

- Ratio (bandwidth ratio): the allowed percentage of broadcast, unknown multicast, or unknown unicast traffic to total bandwidth
- Bits Per Second (BPS): the number of bits allowed to pass per second
- Packet Per Second (PPS): the number of packets allowed to pass per second

The SNR-S212i-8POE supports BPS storm control only.

10.5.2 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, the unicast packets can be properly forwarded.

Prerequisite

Connect the interface and configure physical parameters of it, and make it Up at the physical layer.

10.5.3 Default configurations of storm control

Default configurations of storm control are as below.

Function	Default value
Broadcast storm control status	Enable
Unknown unicast storm control status	Disable
Unknown multicast storm control status	Disable
Number of allowed storm packets per second (BPS)	64 Kbit/s
DLF packet forwarding	Enable

10.5.4 Configuring storm control

Configure storm control for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#storm-control { broadcast dl f mul ti cast } enable port-list port-list</code>	Enable storm control over broadcast traffic, multicast traffic, and unknown unicast traffic.
3	<code>NAG(confi g)#I nterface port port-id</code>	Enter physical layer interface configuration mode.
4	<code>NAG(confi g-port)#storm-control { broadcast mul ti cast dl f al l } bps value</code>	Configure the number of bits that are allowed to pass every second.

10.5.5 Configuring DLF packet forwarding

Configure DLF packet forwarding for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#dl f-forwardi ng enable	Enable DLF packet forwarding on an interface.

10.5.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show storm-control [port-list port-list]	Show configurations of storm control.
2	NAG#show dl f-forwardi ng	Show DLF packet forwarding status.

10.5.7 Example for configuring storm control

Networking requirements

As shown in Figure 10-6, when Port 1 and Port 2 on Switch receive excessive unknown unicast or multicast packets, Switch A will forward these packets to all interfaces except the receiving interface, thus causing broadcast storm and deteriorating forwarding performance of Switch A.

To restrict influence on Switch A caused by broadcast storm, you need to configure storm control on Port 1 and Port 2 on Switch A to control broadcast packets and unknown unicast packets from User network 1 and User network 2. The control threshold is set to 640 Kbit/s.

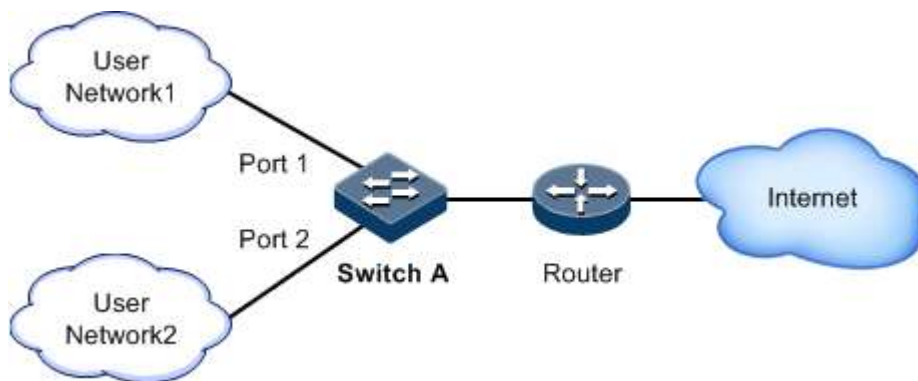


Figure 10-6 Storm control networking

Configuration steps

Step 1 Configure broadcast storm control on Port 1 and Port 2.

```
NAG#confi g
```



```
NAG(confi g)#storm-control broadcast enable port-list 1-2
```

Step 2 Configure unknown unicast storm control on Port 1 and Port 2.

```
NAG(confi g)#storm-control dl f enable port-list 1-2
```

Step 3 Configure storm control threshold.

```
NAG(confi g)#interface port-list 1-2
NAG(confi g-range)#storm-control broadcast bps 640
NAG(confi g-range)#storm-control dl f bps 640
```

Checking results

Use the **show storm-control** command to show configurations of storm control.

```
NAG#show storm-control
Interface          Packet-Type      Status           Threshold      Unit
-----
port1              Broadcast        Enable          640            kbps
                  Multicast        Disable         64             kbps
                  Df              Enable          640            kbps
port2              Broadcast        Enable          640            kbps
                  Multicast        Disable         64             kbps
                  Df              Enable          640            kbps
port3              Broadcast        Enable          64             kbps
                  Multicast        Disable         64             kbps
                  Df              Disable         64             kbps
.....
```

10.6 802.1x

10.6.1 Introduction

802.1x, based on IEEE 802.1x, is a VLAN-based network access control technology. It is used to solve authentication and security problems for LAN users.

It is used to authenticate and control access devices at the physical layer of the network device. It defines a point-to-point connection mode between the device interface and user devices. User devices, connected to the interface, can access resources in the LAN if they are authenticated. Otherwise, they cannot access resources in the LAN through the switch.

802.1x structure

As shown in Figure 10-7, 802.1x authentication uses C/S mode, including the following 3 parts:

- **Supplicant:** a user-side device installed with the 802.1x client software (such as Windows XP 802.1x client), such as a PC
- **Authenticator:** an access control device supporting 802.1x authentication, such as a switch
- **Authentication Server:** a device used for authenticating, authorizing, and accounting users. Generally, the RADIUS server is taken as the 802.1x authentication server.

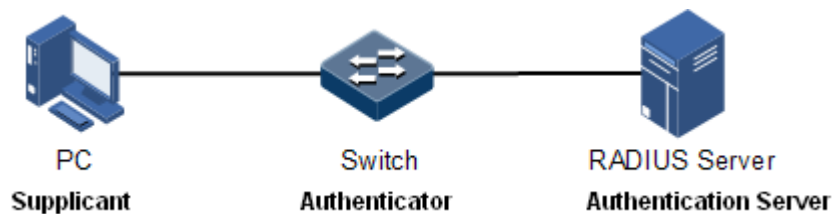


Figure 10-7 802.1x structure

Interface access control modes

The authenticator uses the authentication server to authenticate clients that need to access the LAN and controls interface authorized/ unauthorized status through the authentication results. You can control the access status of an interface by configuring access control modes on the interface. 802.1x authentication supports the following 3 interface access control modes:

- **Protocol authorized mode (auto):** the protocol state machine decides the authorization and authentication results. Before clients are successfully authenticated, only EAPoL packets are allowed to be received and sent. Users are disallowed to access network resources and services provided by the switch. If clients are authorized, the interface is switched to the authorized state, allowing users to access network resources and services provided by the switch.
- **Force interface authorized mode (authorized-force):** the interface is in authorized state, allowing users to access network resources and services provided by the switch without being authorized and authenticated.
- **Force interface unauthorized mode (unauthorized-force):** the interface is in unauthorized mode. Users are disallowed to access network resources and services provided by the switch, that is, users are disallowed to be authenticated.

802.1x authentication procedure

The 802.1x system supports finishing authentication procedure between the RADIUS server through EAP relay and EAP termination.

- **EAP relay**

The supplicant and the authentication server exchange information through the Extensible Authentication Protocol (EAP) packet while the supplicant and the authenticator exchange information through the EAP over LAN (EAPoL) packet. The EAP packet is encapsulated with authentication data. This authentication data will be encapsulated into the RADIUS protocol packet to be transmitted to the authentication server through a complex network. This procedure is call EAP relay.

Both the authenticator and the supplicant can initiate the 802.1x authentication procedure. This guide takes the supplicant for an example, as shown below:

- Step 1 The user enters the user name and password. The supplicant sends an EAPoL-Start packet to the authenticator to start the 802.1x authentication.
- Step 2 The authenticator sends an EAP-Request/Identity to the supplicant, asking the user name of the supplicant.
- Step 3 The supplicant replies an EAP-Response/Identity packet to the authenticator, which includes the user name.
- Step 4 The authenticator encapsulates the EAP-Response/Identity packet to the RADIUS protocol packet and sends the RADIUS protocol packet to the authentication server.
- Step 5 The RADIUS server determines whether the user is authorized according to user information, and then sends the authentication successful/failed packet to the authenticator.
- Step 6 The authentication server compares with received encrypted password with the one generated by itself. If identical, the authenticator modifies the interface state to authorized state, allowing users to access the network through the interface and sends an EAP-Success packet to the supplicant. Otherwise, the interface is in unauthorized state and sends an EAP-Failure packet to the supplicant.

- EAP termination

Terminate the EAP packet at the device and map it to the RADIUS packet. Use standard RADIUS protocol to finish the authorization, authentication, and accounting procedure. The device and RADIUS server adopt Password Authentication Protocol (PAP)/Challenge Handshake Authentication Protocol (CHAP) to perform authentication.

In the EAP termination mode, the random encryption character, used for encrypting the password, is generated by the device. And then the device sends the user name, random encryption character, and encrypted password to the RADIUS server for authentication.

802.1x timers

During 802.1x authentication, the following 5 timers are involved:

- Reauth-period: re-authorization timer. After the period is exceeded, the SNR-S212i-8POE re-initiates authorization.
- Quiet-period: quiet timer. When user authorization fails, the SNR-S212i-8POE needs to keep quiet for a period. After the period is exceeded, the SNR-S212i-8POE re-initiates authorization. During the quiet time, the SNR-S212i-8POE does not process authorization packets.
- Tx-period: transmission timeout timer. When the SNR-S212i-8POE sends a Request/Identity packet to users, the SNR-S212i-8POE will initiate the timer. If users do not send an authorization response packet during the tx-period, the SNR-S212i-8POE will re-send an authorization request packet. The SNR-S212i-8POE sends this packet three times in total.
- Supp-timeout: Supplicant authorization timeout timer. When the SNR-S212i-8POE sends a Request/Challenge packet to users, the SNR-S212i-8POE will initiate supp-timeout timer. If users do not send an authorization response packet during the supp-timeout, the SNR-S212i-8POE will re-send the Request/Challenge packet. The SNR-S212i-8POE sends this packet twice in total.
- Server-timeout: Authentication server timeout timer. The timer defines the total timeout period of sessions between authorizer and the RADIUS server. When the configured time

is exceeded, the authenticator will end the session with RADIUS server and start a new authorization process.

10.6.2 Preparing for configurations

Scenario

To realize access authentication on LAN users and ensure access user security, you need to configure 802.1x authentication on the SNR-S212i-8POE.

If users are authenticated, they are allowed to access network resources. Otherwise, they cannot access network resources. By performing authentication control on user access interface, you can manage the users.

Prerequisite

If RADIUS authentication server is used, you need to perform following operations before configuring 802.1x authentication:

- Configure the IP address of the RADIUS server and the RADIUS shared key.
- The SNR-S212i-8POE can ping through the RADIUS server successfully.

10.6.3 Default configurations of 802.1x

Default configurations of 802.1x are as below.

Function	Default value
Global 802.1x	Disable
Interface 802.1x	Disable
Global authentication mode	Chap
Interface access control mode	Auto
Authentication method	Portbased
Re-authentication	Disable
802.1x re-authentication timer	3600s
802.1x quiet timer	60s
transmission timeout timer	30s
Supplicant authorization timeout timer	30s

10.6.4 Configuring basic functions of 802.1x



Caution

- 802.1x and STP are exclusive on the same interface. You cannot enable them concurrently.

- Only one user authentication request is processed on an interface at a time.

Configure basic functions of 802.1x for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#dot1x enabl e	Enable global 802.1x.
3	NAG(confi g)#dot1x authenti cation-method { chap pap eap }	Configure global authentication mode.
4	NAG(confi g)#i nterface port <i>port-i d</i>	Enter physical layer interface configuration mode.
5	NAG(confi g-port)#dot1x enabl e	Enable interface 802.1x.
6	NAG(confi g-port)#dot1x auth- control { auto authori zed- force unauthori zed-force }	Configure access control mode on the interface.
7	NAG(confi g-port)#dot1x auth- method { portbased macbased }	Configure access control mode of 802.1x authentication on the interface.



Note

If 802.1x is disabled in global/interface configuration mode, the interface access control mode of 802.1x is set to force interface authorized mode.

10.6.5 Configuring 802.1x re-authentication



Caution

Re-authentication is initiated for authorized users. Before enabling re-authentication, you must ensure that global/interface 802.1x is enabled. Authorized interfaces are still in this mode during re-authentication. If re-authentication fails, the interfaces are in unauthorized state.

Configure 802.1x re-authentication for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#i nterface port <i>port- i d</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)#dot1x reauthenti cation enabl e	Enable 802.1x re-authentication.

10.6.6 Configuring 802.1x timers

Configure 802.1x timers for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#I nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)#dot1x ti mer reauth- <i>period reauth-period</i>	Configure the time of the re-authentication timer.
4	NAG(confi g-port)#dot1x ti mer quiet- <i>period quiet-period</i>	Configure the time of the quiet timer.
5	NAG(confi g-port)#dot1x ti mer tx- <i>period tx-period</i>	Configure the time of the transmission timeout timer.
6	NAG(confi g-port)#dot1x ti mer supp- <i>timeout supp-timeout</i>	Configure the time of the supplicant authorization timeout timer.
7	NAG(confi g-port)#dot1x ti mer server- <i>timeout server-timeout</i>	Configure the time of the Authentication server timeout timer.

10.6.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show dot1x port- <i>list port-list</i>	Show 802.1x configurations on the interface.
2	NAG#show dot1x port- <i>list statistics</i>	Show 802.1x statistics on the interface.
3	NAG#show dot1x port- <i>list user</i>	Show user information of 802.1x authentication on the interface.

10.6.8 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	NAG(confi g)#clear dot1x port- <i>list statistics</i>	Clear interface 802.1x statistics.

10.6.9 Example for configuring 802.1x

Networking requirements

To make users access external network, you need to configure 802.1x authentication on the switch, as shown in Figure 10-8.

- Configure the switch.
 - IP address: 10.10.0.1
 - Subnet mask: 255.255.0.0
 - Default gateway: 10.10.0.2
- Perform authorization and authentication through the RADIUS server.
 - IP address of the RADIUS server: 192.168.0.1
 - Password of the RADIUS server: NAG
- Set the interface access control mode to protocol authorized mode.
- After authorized successfully, the user can initiate re-authentication in 600 seconds.

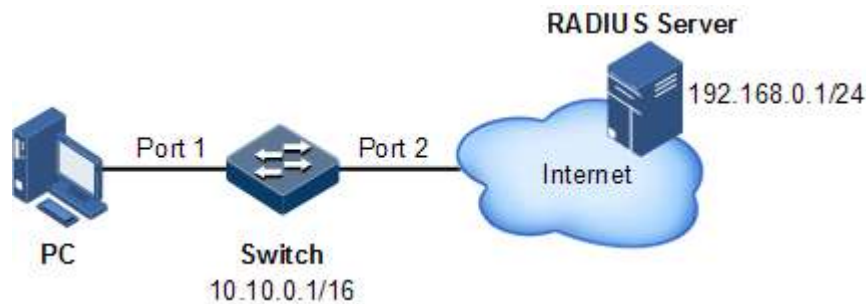


Figure 10-8 Configuring 802.1x

Configuration steps

Step 1 Configure the IP addresses of the Switch and RADIUS server.

```
NAG#confi g
NAG(confi g)#i nterface i p 0
NAG(confi g-i p)#i p address 10. 10. 0. 1 255. 255. 0. 0 1
NAG(confi g-i p)#exi t
NAG(confi g)#i p route 0. 0. 0. 0 0. 0. 0. 0 10. 10. 0. 2
NAG(confi g)#exi t
NAG#radi us 192. 168. 0. 1
NAG#radi us-key NAG
```

Step 2 Enable global 802.1x and interface 802.1x.

```
NAG#confi g
NAG(confi g)#dot1x enable
NAG(confi g)#i nterface port 1
```

```
NAG(config-port)#dot1x enable
```

Step 3 Set the authorization mode to protocol authorization mode.

```
NAG(config-port)#dot1x auth-control auto
```

Step 4 Enable re-authentication and set the re-authentication time to 600s.

```
NAG(config-port)#dot1x reauthentication enable  
NAG(config-port)#dot1x timer reauth-period 600
```

Checking results

Use the **show dot1x port-list** *port-list* command to show 802.1x configurations.

```
NAG#show dot1x port-list 1  
802.1x Global Admin State: enable  
802.1x Authentication Method: chap  
Port port1  
-----  
802.1X Port Admin State: Enable  
PAE: Authenticator  
PortMethod: Portbased  
PortControl: Auto  
PortStatus: Authorized  
Authenticator PAE State: Initialize  
Backend Authenticator State: Initialize  
ReAuthentication: Enable  
QuietPeriod: 60(s)  
ServerTimeout: 100(s)  
SuppTimeout: 30(s)  
ReAuthPeriod: 600(s)  
TxPeriod: 30(s)
```

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 the packets characteristics, including source IP address, source MAC address, and VLAN tags, and can support the interface to combine 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 entry, 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.

Principle of IP Source Guard

The principle of IP Source Guard is to build an IP source binding table within the SNR-S212i-8POE. The IP source binding table is taken as the basis for each interface to test received data packets. Figure 10-9 shows the principle of IP Source Guard.

- If the received IP packets meet the relationship of Port/IP/MAC/VLAN binding entries in IP source binding table, forward these packets.
- If the received IP packets are DHCP data packets, forward these packets.
- Otherwise, discard these packets.

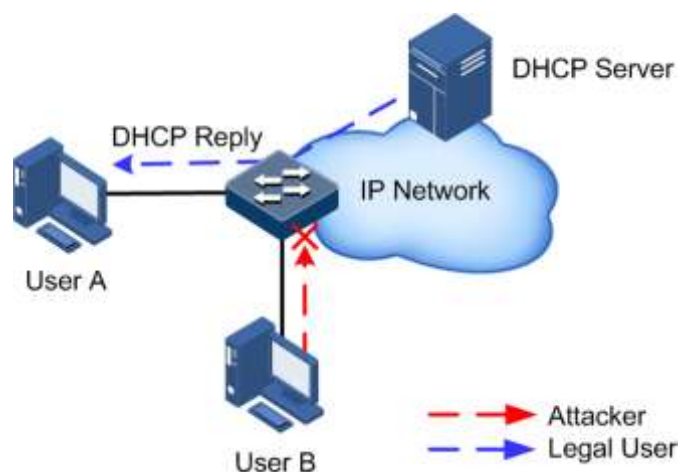


Figure 10-9 Principle of IP Source Guard

Before forwarding IP packets, the SNR-S212i-8POE compares the source IP address, source MAC address, interface number, and VLAN ID of the IP packets with binding table information. If the information matches, it indicates that it is a legal user and the packets are permitted to forward normally. Otherwise, it 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 makes the legitimate users cannot get network services normally.

With IP Source Guard binding, you can filter and control packets forwarded by the interface, prevent the illegal packets passing through the interface, thus to restrict the illegal use of network resources and improve the interface security.

Prerequisite

Enable DHCP Snooping before if there is a DHCP user.

10.7.3 Default configurations of IP Source Guard

Default configurations of IP Source Guard are as below.

Function	Default value
IP Source Guide static binding	Disable
IP Source Guide dynamic binding	Disable
Interface trust status	Untrusted

10.7.4 Configuring interface trust status of IP Source Guard

Configure interface trust status of IP Source Guard for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# inter face interface- type interface- number	Enter physical layer interface configuration mode.
3	NAG(confi g- port)# i p veri fy source trust	(Optional) configure the interface to a trusted interface. Use no ip verify source trust command to configure the interface to an untrusted interface. In this case, all packets, but for DHCP packets and IP packets that meet binding, are not be forwarded. When the interface is in trusted status, all packets are forwarded normally.

10.7.5 Configuring IP Source Guide binding

Configuring IP Source Guide static binding

Configure IP Source Guide static binding for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i p veri fy source	Enable IP Source Guide static binding.
3	NAG(confi g)# i p source bi ndi ng <i>i p-address [mac-address]</i> <i>[vl an vlan-id] port port-id</i>	Configure static binding.



Note

- The configured static binding does not take effect when global static binding is disabled. Only when global static binding is enabled can the static binding take effect.
- For an identical IP address, the manually configured static binding will cover the dynamic binding. However, it cannot cover the existing static binding. When the static binding is deleted, the system will recover the covered dynamic binding automatically.

Configuring IP Source Guide dynamic binding

Configure IP Source Guide dynamic binding for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i p veri fy source dhcp-snoopi ng	Enable IP Source Guide 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 SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#i p veri fy source dhcp- snoopi ng	Enable IP Source Guide dynamic binding.
3	NAG(confi g)#i p source bi ndi ng dhcp- snoopi ng stati c	Translate the dynamic binding to the static binding.
4	NAG(confi g)#i p source bi ndi ng auto- update	(Optional) enable auto-translation. After it is enabled, dynamic binding entries learned through DHCP Snooping are directly translated into static binding entries.

10.7.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show i p veri fy source	Show global binding status and interface trusted status.
2	NAG#show i p source bi ndi ng [port <i>port- id</i>]	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 10-10, to prevent IP address embezzlement, you need to configure IP Source Guard on the switch.

- The Switch permits all IP packets on Port 1 to pass.
- Port 2 permits IP packets with specified the IP address 10.10.10.1 and subnet mask 255.255.255.0 and the IP packets meeting DHCP Snooping learnt dynamic binding to pass.
- Other interfaces only permit the packets meeting DHCP Snooping learnt dynamic binding to pass.

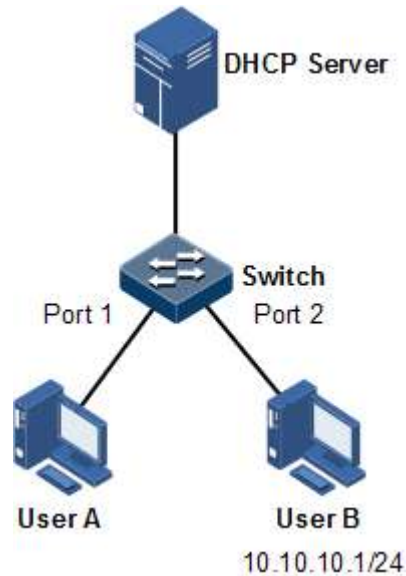


Figure 10-10 Configuring IP Source Guard

Configuration steps

Step 1 Set Port 1 to a trusted interface.

```

NAG#confi g
NAG(confi g)#i nterface port 1
NAG(confi g-port)#i p veri fy source trust
NAG(confi g-port)#exi t
  
```

Step 2 Configure the static binding.

```

NAG(confi g)#i p veri fy source
NAG(confi g)#i p source bi ndi ng 10. 10. 10. 1 port 2
  
```

Step 3 Enable IP Source Guard dynamic binding.

```

NAG(confi g)#i p veri fy source dhcp-snoopi ng
  
```

Checking results

Use the **show ip source binding** command to show configurations of the static binding table.

```

NAG#show i p source bi ndi ng
History Max Entry Num: 1
  
```

```

Current Entry Num: 1
Ip Address      Mac Address  VLAN  Port          Type      Inhw
-----
10.10.10.1     --          --   port2 static     yes

```

Use the **show ip verify source** command to show interface trusted status and configurations of IP Source Guard static/dynamic binding.

```

NAG#show ip verify source
Static Bind: Enable
Dhcp-Snooping Bind: Enable
Port          Trust
-----
port1         yes
port2         no
port3         no
.....

```

10.8 PPPoE+

10.8.1 Introduction

PPPoE Intermediate Agent (PPPoE+) is used to process authentication packets. PPPoE+ adds user information 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.

With PPPoE dial-up mode, you can access the network through various interfaces of the device only when one authentication is successfully. 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 C/S mode, as shown in Figure 10-11. The Switch acts as a relay agent. Users access the network through PPPoE authentication. If the PPPoE server needs to locate users, more information should be contained in the authentication packet.

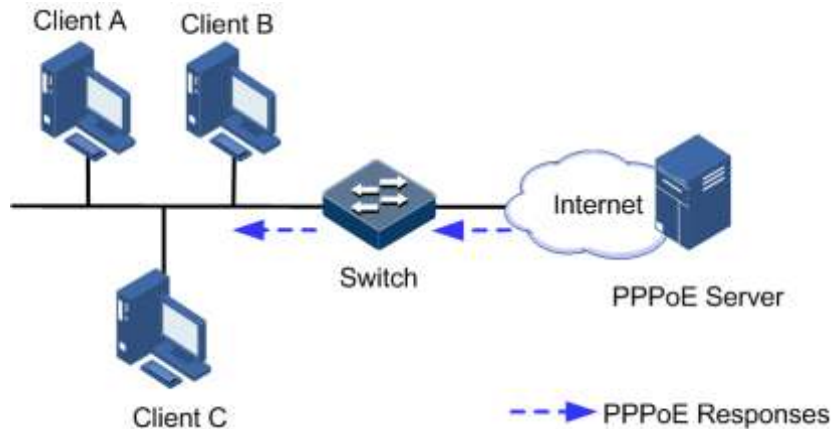


Figure 10-11 Accessing the network through PPPoE authentication

To access the network through PPPoE authentication, you need to pass through the following 2 stages: discovery stage (authentication stage) and session stage. PPPoE+ is used to process packets at the discovery stage. The following steps show the whole discovery stage.

- Step 1 To access the network through PPPoE authentication, the client sends a broadcast packet PPPoE Active Discovery Initiation (PADI). This packet is used to query the authentication server.
- Step 2 After receiving the PADI packet, the authentication server replies a unicast packet PPPoE Active Discovery Offer (PADO).
- Step 3 If multiple authentication servers reply PADO packets, the client selects one from them and then sends a unicast PPPoE Active Discovery Request (PADR) to the authentication server.
- Step 4 After receiving the PADR packet, if the authentication server believes that the user is legal, it sends a unicast packet PPPoE Active Discovery Session-confirmation (PADS) to the client.

PPPoE is used to add user identification information in to PADI and PADR. Therefore, the server can identify whether the user identification information is identical to the user account for assigning resources.

10.8.2 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 packet 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 I PPPoE+ are as below.

Function	Default value
Global PPPoE	Disable
Interface PPPoE	Disable
Padding mode of Circuit ID	Switch
Circuit ID information	Interface ID/VLAN ID/attached string
Attached string of Circuit ID	hostname
Padded MAC address of Remote ID	MAC address of the switch
Padding mode of Remote ID	Binary
Interface trusted status	Untrusted
Tag overriding	Disable



Note

By default, PPPoE packet is forwarded without being attached 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. An interface is either enabled with PPPoE+ or is 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 SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# pppoeagent enable	Enable global PPPoE+.
3	NAG(confi g)# i nterface port port-id	Enter physical layer interface configuration mode.
4	NAG(confi g-port)# pppoeagent enable	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 set 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 SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#i nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)#pppoeagent trust	Configure the PPPoE trusted interface. Use the no pppoeagent trust command to configure the interface as the untrusted 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 the PPPoE packet. 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 set to hostname by default.
- Customized mode: when customized Circuit ID is configured, the padding content is the Circuit IS string.

Configure Circuit ID for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# pppoeagent ci rcui t-i d mode { onu swi tch }	Configure the padding mode of the Circuit ID.
3	NAG(confi g)# I nterface port port-i d	Enter physical layer interface configuration mode.
4	NAG(confi g-port)# pppoeagent ci rcui t-i d string	(Optional) set the Circuit ID to the customized string.

In default mode, the Circuit ID contains an attached string. By default, the attached string is set to the hostname of the switch. You can set it to a customized string.

Configure the attached string of the Circuit ID for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# pppoeagent ci rcui t-i d attach-stri ng string	(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 SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# I nterface port port-i d	Enter physical layer interface configuration mode.
3	NAG(confi g-port)# pppoeagent remote-i d { cli ent-mac swi tch-mac }	(Optional) configure PPPoE+ Remote ID to be padded with the MAC address.
4	NAG(confi g-port)# pppoeagent remote-i d format { asci i bi nary }	(Optional) configure the padding modes of the PPPoE+ Remote ID.

Configuring Tag overriding

Tags of some fields may be forged by the client because of some reasons. The client overrides the original Tags. After Tag overriding is enabled, if the PPPoE packets contain Tags, these Tags are overridden. If not, add Tags to these PPPoE packets.

Configure Tag overriding for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#i nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g-port)#pppoeagent vendor-speci fi c-tag overwri te enable	Enable Tag overriding.

10.8.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show pppoeagent [port-list <i>port-list</i>]	Show PPPoE+ configurations.
2	NAG#show pppoeagent statist ic [port-list <i>port-list</i>]	Show PPPoE+ statistics.

10.8.7 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	NAG(confi g)#cl ear pppoeagent statist ic [port-list <i>port-list</i>]	Clear PPPoE+ statistics.

10.8.8 Example for configuring PPPoE+

Networking requirements

As shown in Figure 10-12, to prevent illegal access during PPPoE authentication and to control and monitor users, configure PPPoE+ on the Switch.

- Port 1 and Port 2 are connected to Client 1 and Client 2 respectively. Port 3 is connected to the PPPoE server.
- Enable global PPPoE+ and enable PPPoE+ on Port 1 and Port 2. Set Port 3 to the trusted interface.

- Set the attached string of the Circuit ID to NAG. Set the padding content of the Circuit ID on Port 1 to user01. Set the padding content of the Remote ID on Port 2 to the MAC address of the client. The padding contents are in ASCII mode.
- Enable Tag overriding on Port 1 and Port 2.

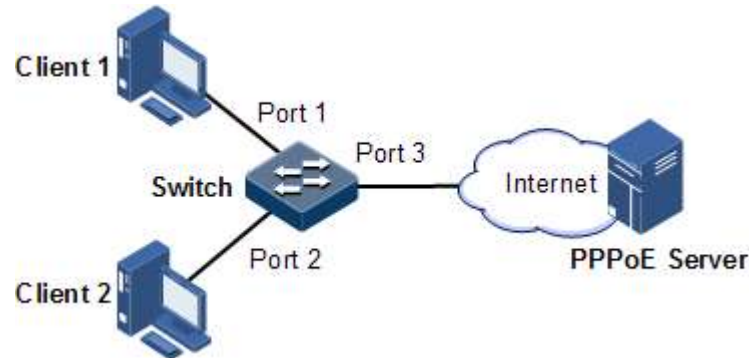


Figure 10-12 Configuring PPPoE+

Configuration steps

Step 1 Set Port 3 to the trusted interface.

```
NAG#confi g
NAG(confi g)#i nterface port 3
NAG(confi g-port)#pppoenagent trust
NAG(confi g-port)#exi t
```

Step 2 Configure packet information about Port 1 and Port 2.

```
NAG(confi g)#pppoeagent ci rcui t-i d attach-string NAG
NAG(confi g)#i nterface port 1
NAG(confi g-port)#pppoeagent ci rcui t-i d user01
NAG(confi g-port)#exi t
NAG(confi g)#i nterface port 2
NAG(confi g-port)#pppoeagent remote-i d client-mac
NAG(confi g-port)#pppoeagent remote-i d format asci i
NAG(confi g-port)#exi t
```

Step 3 Enable Tag overriding on Port 1 and Port 2.

```
NAG(confi g)#i nterface port 1
NAG(confi g-port)#pppoeagent vendor-speci fi c-tag overwri te enabl e
NAG(confi g-port)#exi t
NAG(confi g)#i nterface port 2
NAG(confi g-port)#pppoeagent vendor-speci fi c-tag overwri te enabl e
NAG(confi g-port)#exi t
```

Step 4 Enable global PPPoE+ and enable PPPoE+ on Port 1 and Port 2.

```
NAG(confi g)#pppoeagent enable
NAG(confi g)#interface port 1
NAG(confi g-port)#pppoeagent enable
NAG(confi g-port)#exit
NAG(confi g)#interface port 2
NAG(confi g-port)#pppoeagent enable
```

Checking results

Use the **show pppoeagent** command to show PPPoE+ configurations.

```
NAG#show pppoeagent port 1-2
NAG#show pppoeagent port-list 1-3
Global PPPoE+ status: enable
Attach-string: NAG
Circuit ID padding mode: switch
Port   State  Overwrite Remote-ID  Format-rules  Circuit-ID
-----
port1   enable enable   switch-mac  binary       user01
port2   enable enable   client-mac  ascii        %default%
port3   trust  disable  switch-mac  binary       %default%
```

**In switch mode, Circuit-ID's default string is: Port\VI an\Attach-string.
**In onu mode, Circuit-ID's default string is: 0 0/0/0:0.0 0/0/0/0/0/0/MAC
0/0/Port:eth/4096.CVLAN LN.
**Attach-string's default string is the hostname.

11 Reliability

This chapter describes basic principle and configuration of reliability and provides related configuration examples.

- Link aggregation
- Interface backup
- Failover

11.1 Link aggregation

11.1.1 Introduction

With link aggregation, multiple physical Ethernet interfaces are combined to form a Logical Aggregation Group (LAG). Multiple physical links in one LAG are taken as a logical link. The link aggregation helps share traffics among members in an LAG. Link aggregation not only effectively improves reliability of links between devices, but also helps gain higher bandwidth without upgrading hardware.

Every physical interface in the LAG is called the member interface, and the aggregated logical interface is called the trunk interface.

Link aggregation is the most widely used and most simple function in Ethernet reliability technology.

Advantage of link aggregation

As shown in Figure 11-1, Switch A and Switch B have two physical links between them. These two links are grouped together and form a logical link aggregation 1.



Figure 11-1 Link aggregation

Logical Link Aggregation 1 has the following advantages:

- Higher reliability: all the members in the LAG keep standby for others. If one link becomes Down, the others can carry the traffic of the Down one immediately.
- Higher bandwidth: you need not to upgrade the existing hardware to obtain a higher throughput bandwidth. By combining several physical links, the LAG can provide a higher bandwidth based on bandwidth summary of all the physical links.
- Load sharing: service flow is divided and lead to different member interface according to configured load sharing policy. This is a load sharing on the link level.
- Optimized network management: all the member interfaces in one logical group can be managed at the same time as a normal interface.
- Saving IP addresses: only one IP address is needed for the LAG, and member interfaces do not need IP addresses.

LACP protocol

Link Aggregation Control Protocol (LACP) is based on IEEE802.3ad recommendation. LACP exchanges information with peer through Link Aggregation Control Protocol Data Unit (LACPDU). After enabling LACP of an interface, it notifies the peer of its own LACP priority, system MAC, interface LACP priority, port ID and operation Key by sending LACPDU.

The peer receives LACPDU, compares information with that received by other interfaces, and chooses the interface in Selected status. The interfaces at both ends become consistent in Selected status.

Every member interface in a LAG has an operation Key which indicates the aggregation ability of this interface. The operation Key is created according to the interface configurations (LAG number, speed, duplex mode). Any change of the configurations will lead to recount of the operation Key. In a LAG, all the active interfaces must have the same operation Key.

Interface status

Member interfaces in a LAG have two kinds of statuses:

- Active status: send/receive LACP packets and forward user data. This kind of interfaces is called the working interface.
- Standby status: send/receive LACP packets, but does not forward user data. This kind of interfaces is called the backup interface.

The SNR-S212i-8POE supports up to 14 LAGs. Each LAG supports up to 8 member interfaces. By default, the number of supported active interfaces in a LAG ranges from 1 to 8.

Link aggregation method

There are several methods of link aggregation:

- Manual aggregation mode

This mode is to add several physical interfaces into a LAG, all the Up interfaces make up a logical interface. The link under one logical link can realize load sharing. This mode does not need LACP packet interaction.

- Static LACP aggregation mode

This mode is to negotiate aggregation parameters and select active interfaces by LACP packet. After manually adding several physical interfaces into a LAG, the local device notifies the

peer of its own LACP information. The interfaces at both ends elect the active interface, aggregate the link, etc.

- Dynamic LACP aggregation mode

In dynamic LACP aggregation mode, the SNR-S212i-8POE creates and deletes the LAG automatically, as well as adding and removing the member interface. Finally it implements link aggregation by using LACP packets. Only when interfaces have the same basic configuration, speed, and duplex mode can they be aggregated into a LAG. In a dynamic LACP LAG, the active interface with the minimum interface number is called the primary interface, and the others are member interfaces.

The main difference between manual aggregation and static/dynamic LACP aggregation is: manual aggregation mode has all the member interfaces in active status and sharing loading flow, while other two LACP aggregation modes have parts of member interfaces in standby status forming standby link.

The SNR-S212i-8POE supports manual aggregation, static LACP aggregation, and dynamic LACP aggregation modes.

Load sharing

Load sharing mechanism is used in link aggregation. It divides certain service traffic into different links, thus providing a higher performance ability and reliability.

- Load sharing algorithm: choose the output interface of a packet according to different algorithm, including MAC CRC hash mapping and direct mapping
- Load sharing mode: choose the output interface base on different load sharing mode or their combination. Make sure packets with same attribution sent out from the same interface. By this, the SNR-S212i-8POE can achieve a flexible load sharing. You can assign the load sharing based on port ID, ip address, mac in the packet or their combination. There are following modes:
 - SIP: choose the output interface based on the source IP address.
 - DIP: choose the output interface based on the destination IP address.
 - SMAC: choose the output interface based on the source MAC address.
 - DMAC: choose the output interface based on the destination MAC address.
 - SXORDIP: choose the output interface based on the source IP address XOR the destination IP address.
 - SXORDMAC: choose the output interface based on the source MAC address XOR the destination MAC address.

The SNR-S212i-8POE supports service load sharing based on load sharing mode.

11.1.2 Preparing for configurations

Scenario

To provide higher bandwidth and reliability for a link between two devices, configure link aggregation.

With link aggregation, multiple physical Ethernet interface are added into a LAG and are aggregated to a logical link. Link aggregation helps share uplink and downlink traffic among members in one LAG. Therefore, the link aggregation helps obtain higher bandwidth and

helps members in one LAG back up data for each other, which improves reliability of Ethernet connection.

Prerequisite

Before configuring link aggregation, you need to configure physical parameters on a port and make the physical layer **Up**.

11.1.3 Default configurations of link aggregation

Default configurations of link aggregation are as below.

Function	Default value
Link aggregation	Enable
Load balancing mode	Sxordmac
Aggregation group	Existing, in manual mode
LACP system priority	32768
LACP interface priority	32768
LACP interface mode	Active
LACP timeout mode	Slow
Minimum number of active interfaces	1
Maximum number of active interfaces	8
Interface dynamic LACP link aggregation	Disable

11.1.4 Configuring manual link aggregation

Configure manual link aggregation for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#l i nk-aggregati on enabl e</code>	Enable link aggregation.
3	<code>NAG(confi g)#l i nk-aggregati on l oadi ng-shari ng mode { di p dmac si p smac sxordi p sxordmac }</code>	(Optional) configure the load-sharing mode for link aggregation.
4	<code>NAG(confi g)#i nterface port- channel <i>port-channel-number</i></code>	Enter LAG configuration mode.
5	<code>NAG(confi g-aggregator)#mode manual NAG(confi g-aggregator)#exi t</code>	Configure manual link aggregation mode.
6	<code>NAG(confi g)#i nterface port <i>port-id</i></code>	Enter physical layer interface configuration mode.

Step	Command	Description
7	NAG(config-g-port)# channel group <i>port-channel-number</i>	Add interfaces to the LAG.



Note

In the same LAG, member interfaces that share loads must be identically configured. Otherwise, data cannot be forwarded properly. These configurations include STP, QoS, QinQ, VLAN, interface properties, and MAC address learning.

- STP: the STP enabling/disabling status on the interface, properties for links that are connected to the interface (such as point-to-point or non point-to-point), path cost on the interface, STP priority, limit on rate for sending packets, whether the loopback protection and the root protection is configured, and whether the interface is an edge interface
- QoS: traffic policing, 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 static MAC address entries are configured, whether enabling the MAC address learning function, whether a limit is configured for the maximum value of learned MAC address, and whether continue to forwarding packets after the MAC addresses exceed the threshold

11.1.5 Configuring static LACP link aggregation

Configure static LACP link aggregation for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(config)# l i nk-aggreati on enable	(Optional) enable link aggregation.
3	NAG(config)# l i nk-aggreati on loadi ng-shari ng mode { di p dmac si p smac sxordi p sxordmac }	(Optional) configure load sharing mode for the LAG.
4	NAG(config)# l acp system-pri ori ty system-pri ori ty	(Optional) configure system LACP priority. The higher priority end is active end. LACP chooses active and backup interfaces according to the active end configuration. The smaller the number is, the higher the priority is. The smaller system MAC address device will be chosen as active end if devices system LACP priorities are identical.

Step	Command	Description
5	NAG(config)#l acp timeout { fast slow } [port-list port-list]	(Optional) configure LACP timeout mode.
6	NAG(config)#i nterface port-channel port- channel -number	Enter LAG configuration mode.
7	NAG(config- aggregator)#mode l acp-stati c	Configure static LACP LAG.
8	NAG(config- aggregator)#{ max- acti ve mi n-acti ve } l i nks number NAG(config- aggregator)#exi t	(Optional) configure maximum or minimum number of active interfaces in the LACP LAG.
9	NAG(config)#i nterface port port-i d	Enter physical layer interface configuration mode.
10	NAG(config- port)#channel group port-channel -number	Add member interfaces into the LACP LAG.
11	NAG(config-port)#l acp port-pri ori ty port- pri ori ty	(Optional) configure interface LACP priority. The priority influences default interface selection for LACP. The smaller the value is, the higher the priority is.
12	NAG(config-port)#l acp mode { acti ve passi ve }	(Optional) configure LACP mode for member interface. By default is in active mode. LACP connection will fail when both ends of a link are in passive mode.



Note

The system chooses default interface in the order of neighbor discovery, interface maximum speed, interface highest LACP priority, and interface minimum ID. The interface is in active status by default, the interface with identical speed, identical peer and identical device operation key is also in active status; other interfaces are in standby status.

11.1.6 Configuring dynamic LACP link aggregation

Configure dynamic LACP link aggregation for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(config)#l i n k- aggre gati on enabl e	(Optional) enable link aggregation.
3	NAG(config)#l acp enabl e port-l i s t port-l i s t	Enable interface dynamic LACP link aggregation.

Step	Command	Description
4	<code>NAG(config)#link-aggregation load-sharing mode { dip dmac sip smac sxordi p sxordmac }</code>	(Optional) configure a load-sharing mode for link aggregation.
5	<code>NAG(config)#lACP system-priority system-priority</code>	(Optional) configure system LACP priority.
6	<code>NAG(config)#lACP timeout { fast slow } [port-list port-list]</code>	(Optional) configure LACP timeout mode.
7	<code>NAG(config)#interface port-channel port-channel-number</code>	Enter LAG configuration mode.
8	<code>NAG(config-aggregator)#{ max-active min-active } links number</code> <code>NAG(config-aggregator)#exit</code>	(Optional) configure the maximum or minimum number of active links in LACP LAG.
9	<code>NAG(config)#interface port port-id</code>	Enter physical layer interface configuration mode.
10	<code>NAG(config-port)#lACP port-priority port-priority</code>	(Optional) configure interface LACP priority.
11	<code>NAG(config-port)#lACP mode { active passive }</code>	(Optional) configure LACP mode for member interface. LACP connection will fail when both ends of a link are in passive mode.



Note

When dynamic LACP link aggregation is enabled on an interface, to perform a dynamic link aggregation, perform these operations:

- LACP chooses the empty manual LAG with the smaller LAG number. Set it to dynamic LACP link aggregation mode and add interfaces to the LAG.
- Prompt users when no LAG is available. Add interfaces to the manual LAG if a manual link aggregation is available. In addition, set the manual link aggregation mode to dynamic LACP link aggregation mode.
- If the interface, where LACP is enabled, is in Down status, prompt users with the successful configurations. When the interface is in Up status, LACP chooses a proper dynamic LAG to add interfaces.
- If the interface meets the election requirements on the active interface, the interface is set to the active interface of the LAG. Based on load-balancing and load-sharing algorithms, this interface and other active interfaces in the LAG share loads of the LAG.

11.1.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>NAG#show lACP internal [detail]</code>	Show local LACP information.

No.	Command	Description
2	NAG#show lacp nei ghbor [detail]	Show peer LACP information.
3	NAG#show lacp stati sti cs [port-list port-list]	Show interface LACP statistics.
4	NAG#show lacp sys-id	Show information about the system ID used by LACP.
5	NAG#show link-aggregati on	Show link aggregation information.

11.1.8 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	NAG(confi g)#cl ear lacp stati sti cs [port-list port-list]	Clear statistics of LACP packets on a specified interface.

11.1.9 Example for configuring manual link aggregation

Networking requirements

As shown in Figure 11-2, to improve link reliability between Switch A and Switch B, you need to configure manual link aggregation for the two devices. Add Port 1 and Port 2 into the LAG to build up a unique logical interface. The LAG conducts load sharing according to the source MAC address.

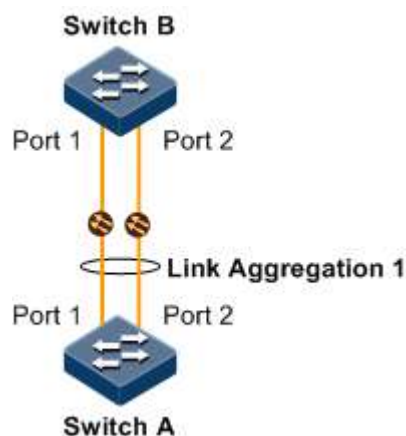


Figure 11-2 Configuring manual link aggregation

Configuration steps

Configurations of Switch A are the same with those of Switch B. Thus configurations of Switch A are described here.

Step 1 Create a manual LAG.

Configure Switch A.

```
NAG#hostname Swi tchA
Swi tchA#confi g
Swi tchA(confi g)#i nterface port-channel 1
Swi tchA(confi g-aggregator)#mode manual
Swi tchA(confi g-aggregator)#exi t
```

Step 2 Add interfaces into the LAG.

Configure Switch A.

```
Swi tchA(confi g)#i nterface port 1
Swi tchA(confi g-port)#channel group 1
Swi tchA(confi g-port)#exi t
Swi tchA(confi g)#i nterface port 2
Swi tchA(confi g-port)#channel group 1
Swi tchA(confi g-port)#exi t
```

Step 3 Configure the load sharing mode for aggregated links.

Configure Switch A.

```
Swi tchA(confi g)#l i nk-aggregati on load-shari ng mode sxordmac
```

Step 4 Enable link aggregation.

Configure Switch A.

```
Swi tchA(confi g)#l i nk-aggregati on enabl e
```

Checking results

Use the **show link-aggregation** command to show global configurations of manual link aggregation.

```
Swi tchA#show l i nk-aggregati on
Link aggregati on status: Enabl e
Load shari ng mode: SXORDMAC
Load shari ng ti cket generati on al gori thm: N/A
M - Manual   S - Stati c-Lacp   D - Dynami c-Lacp
```

GroupID	Mode	MinLinks	MaxLinks	UpLinks	Member Port List	Efficient Port List
1	M	1	8	2	port 1-2	port 1-2

11.1.10 Example for configuring static LACP link aggregation

Networking requirements

As shown in Figure 11-3, to improve link reliability between Switch A and Switch B, you can configure static LACP link aggregation between these 2 devices. Add Port 1 and Port 2 into one LAG, where Port 1 is used as the current link and Port 2 is the protection link.

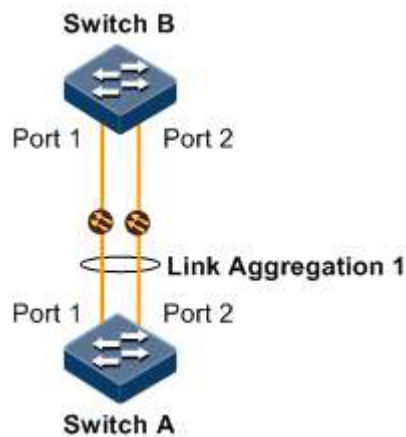


Figure 11-3 Configuring static LACP link aggregation

Configuration steps

Step 1 Configure the static LACP LAG on Switch A.

Configure Switch A.

```
NAG#hostname Swi tchA
Swi tchA#confi g
Swi tchA(confi g)#i nterface port-channel 1
Swi tchA(confi g-aggregator)#mode l acp-stati c
Swi tchA(confi g-aggregator)#max-acti ve l i nks 1
Swi tchA(confi g-aggregator)#exi t
```

Configure Switch B.

```
NAG#hostname Swi tchB
Swi tchB#confi g
Swi tchB(confi g)#i nterface port-channel 1
Swi tchB(confi g-aggregator)#mode l acp-stati c
```

```
SwitchB(config-aggregator)#exit
```

- Step 2 **Configure LACP system priority and LACP interface priority, and set Switch A as the active end.**

Configure Switch A.

```
SwitchA(config)#lacp system-priority 1000
SwitchA(config)#interface port 1
SwitchA(config-port)#lacp port-priority 1000
```

- Step 3 **Add interfaces into the LAG.**

Configure Switch A.

```
SwitchA(config-port)#channel group 1
SwitchA(config-port)#exit
SwitchA(config)#interface port 2
SwitchA(config-port)#channel group 1
SwitchA(config-port)#exit
```

Configure Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#channel group 1
SwitchB(config-port)#exit
SwitchB(config)#interface port 2
SwitchB(config-port)#channel group 1
SwitchB(config-port)#exit
```

- Step 4 **Enable link aggregation.**

Configure Switch A.

```
SwitchA(config)#link-aggregation enable
```

Configure Switch B.

```
SwitchB(config)#link-aggregation enable
```


Checking results

Use the **link-aggregation** command to show global configurations of static LACP link aggregation on Switch A.

```
SwitchA#show link-aggregation
Link aggregation status: Enable
Load sharing mode: SXORDMAC
Load sharing ticket generation algorithm: N/A
M - Manual   S - Static-Lacp   D - Dynamic-Lacp
GroupID  Mode  MinLinks  MaxLinks  UpLinks  Member Port List  Efficient Port List
-----
1         S     1         1         2        port 1-2         port 1
```

Use the **show lacp internal** command to show local system LACP interface state, flag, interface priority, administration key, operation key, and interface state machine state 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
-----
port1      active  SA      1000      1      1      0x45
port2      standby SA      32768     1      1      0x45
```

Use the **show lacp neighbor** command to show peer system LACP interface state, flag, interface priority, administration key, operation key, and interface state machine state on Switch A.

11.1.11 Example for configuring dynamic LACP link aggregation

Networking requirements

As shown in Figure 11-4, to improve link reliability between Switch A and Switch B, you can configure dynamic LACP link aggregation between these 2 devices to dynamically add Port 1, Port 2, and Port 3 on Switch A and Switch B into the LAG and form a single logical interface.

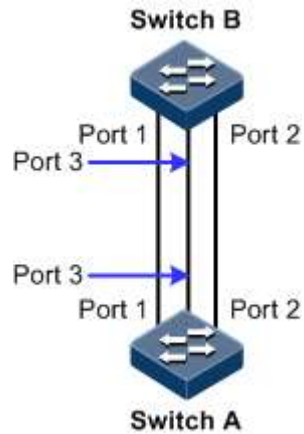


Figure 11-4 Configuring dynamic LACP link aggregation

Configuration steps

Configurations of Switch A are the same with those of Switch B. Thus configurations of Switch A are described here.

Step 1 Configure the dynamic LACP LAG to implement link aggregation.

```
NAG#hostname SwitchA
SwitchA#confi g
SwitchA(confi g)#l acp enable port-l i st 1-3
```

Step 2 Enable link aggregation.

```
SwitchA(confi g)#l i nk-aggregati on enable
```

Checking results

Use the **show link-aggregation** command to show global configurations of dynamic LACP link aggregation.

```
SwitchA#show l i nk-aggregati on
Link aggregation status: Enable
Load sharing mode: SXORDMAC
Load sharing ticket generation algorithm: N/A
M - Manual S - Static-Lacp D - Dynamic-Lacp
GroupID Mode Mi nLi nks MaxLi nks UpLi nks Member Port Li st Effi cient Port
Li st
-----
-----
1 D 1 8 3 port 1-3 port 1-3
```

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, but 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 Carrier-grade network core.

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 solution of STP. 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.

Principle

Interface backup is realized 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 Up interface fails, the Standby interface is switched to the Up status.

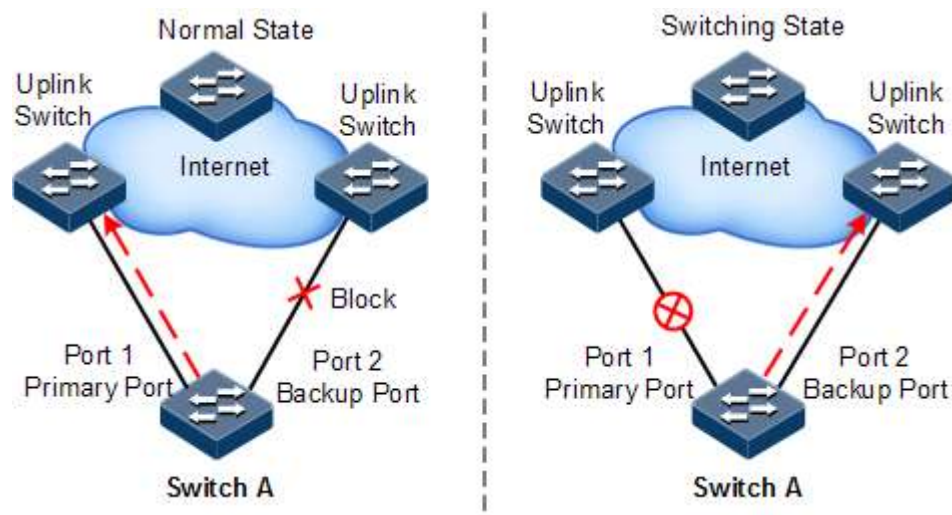


Figure 11-5 Principles of interface backup

As shown in Figure 11-5, Port 1 and Port 2 on Switch A are connected to their uplink devices respectively. The interface forwarding states are shown as below:

- Under normal conditions, Port 1 is the primary interface while Port 2 is the backup interface. Port 1 and the uplink device forward packets to each other while Port 2 and the uplink device do not forward packets to each other.
- When the link between Port 1 and its uplink device fails, the backup Port 2 and its uplink device forward packets to each other.
- When Port 1 restores normally and keeps Up for a period (restore-delay), Port 1 restores to forward packets and Port 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 11-6.

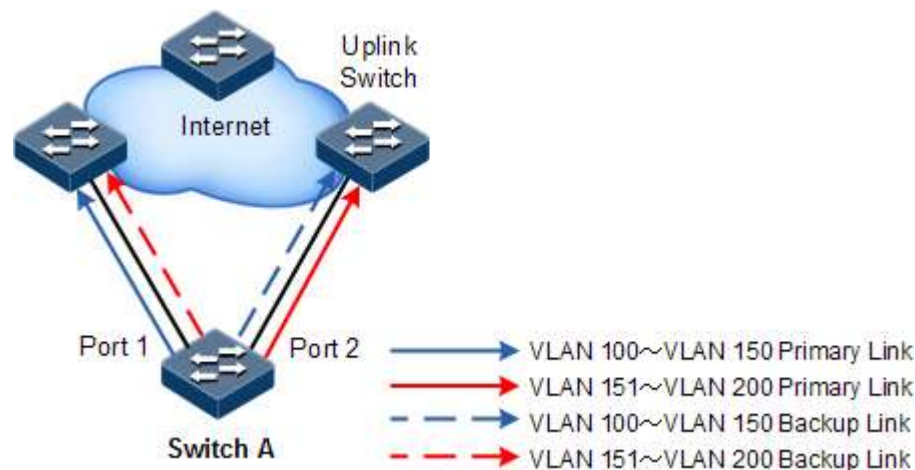


Figure 11-6 Networking with interface backup in different VLANs

In different VLANs, the forwarding status is shown as below:

- Under normal conditions, configure Switch A in VLANs 100–150.
 - In VLANs 100–150, Port 1 is the primary interface and Port 2 is the backup interface.
 - In VLANs 151–200, Port 2 is the primary interface and Port 1 is the backup interface.
 - Port 1 forwards traffic of VLANs 100–150, and Port 2 forwards traffic of VLANs 151–200.
- When Port 1 fails, Port 2 forwards traffic of VLANs 100–200.
- When Port 1 restores normally and keeps Up for a period (restore-delay), Port 1 forwards traffic of VLANs 100–150, and Port 2 forwards VLANs 151–200.

Interface backup is used share service load in different VLANs without depending on configurations of uplink switches, thus facilitating users' operation.

11.2.2 Preparing for configurations

Scenario

When STP is disabled, by configuring interface backup, you can realize redundancy backup and fast switching of primary/backup link, and load sharing 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	Interface connection mode (port-up)

11.2.4 Configuring basic functions of interface backup



Caution

Interface backup and STP, loopback detection, Ethernet ring, or G.8032 may interfere with each other. Configuring both of them on an interface is not recommended.

Configure basic functions of interface backup for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i nterface <i>i nterface-type pri mary-</i> <i>i nterface-number</i>	Enter physical layer interface configuration mode or LAG configuration mode.
3	NAG(confi g- port)# swi tchport backup <i>i nterface-type backup-</i> <i>i nterface-number</i> [v l a n l i s t <i>v l a n-l i s t</i>]	Configure the interface backup group. In the VLAN list, set the interface <i>backup-interface-number</i> to the backup interface and set the interface <i>primary-interface-number</i> to the primary interface. If no VLAN list is specified, the VLAN ranges from 1 to 4094.
	NAG(confi g- aggregator)# swi tchport backup <i>i nterface-type</i> <i>backup-i nterface-number</i> [v l a n l i s t <i>v l a n-l i s t</i>]	
4	NAG(confi g-port)# exi t	Return to global configuration mode.
	NAG(confi g- aggregator)# exi t	
5	NAG(confi g)# swi tchport backup restore-del ay <i>peri od</i>	(Optional) configure the restore-delay period.

Step	Command	Description
6	NAG(config)#swi tchport backup restore-mode { di sabl e nei ghbor- di scover port-up }	(Optional) configure restoration mode.



Note

- In an interface backup group, an interface is either a primary interface or a backup interface.
- In a VLAN, an interface or a LAG cannot be a member of two interface backup groups simultaneously.

11.2.5 (Optional) configuring FS on interfaces



Caution

- After FS is successfully configured, the primary/backup link will be switched; namely, 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 the primary interface is configured with multiple interface backup groups in different VLANs, you should input the backup interface number.

Configure FS on interfaces for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(config)#i nterface <i>interface-type primary- interface-number</i>	Enter physical layer interface configuration mode or LAG configuration mode.
3	NAG(config- port)#swi tchport backup [<i>interface-type backup- interface-number</i>] force- swi tch NAG(config- aggregator)#swi tchport backup [<i>interface-type backup-i nterface-number</i>] force-sw i tch	Configure FS on the interface. Use the no switchport backup [<i>interface-type backup-interface-number</i>] force-switch command to cancel FS. Then, selecting the current link according to link status are as below: <ul style="list-style-type: none"> • If the Up/Down statuses of the two interfaces are the same, the primary interface is of high priority. • If the Up/Down statuses of the two interfaces are different, the Up interface is of high priority.

11.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show swi tchport backup	Show related status information of interface backup.

11.2.7 Example for configuring interface backup

Networking requirements

As shown in Figure 11-7, the PC accesses the server through switches. To realize 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 share load. Configure Switch A as below:

- Switch A is in VLANs 100–150. Port 1 is the primary interface and Port 2 is the backup interface.
- Switch A is in VLANs 151–200. Port 2 is the primary interface and Port 1 is the backup interface.

When Port 1 or its link fails, the system switches to the backup Port 2 to resume the link.

Switch A should support interface backup while Switch B, Switch C, and Switch D do not need to support interface backup.

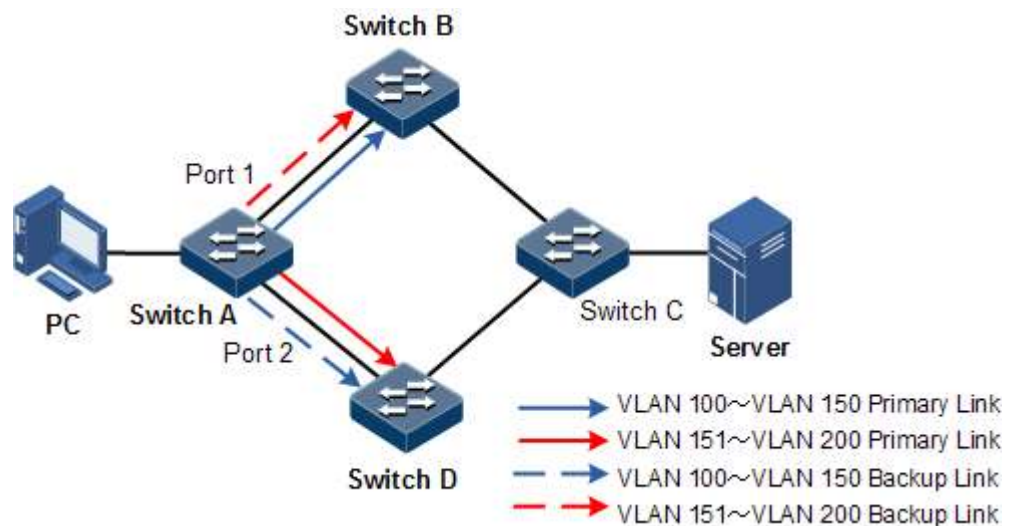


Figure 11-7 Configuring interface backup

Configuration steps

Step 1 Create VLANs 100–200 and add Port 1 and Port 2 to VLANs 100–200.

```
NAG#confi g
NAG(confi g)#create vl an 100-200 active
NAG(confi g)#i nterface port 1
NAG(confi g-port)#swi tchport mode trunk
```

```

NAG(confi g-port)#swi tchport trunk allowed vl an 100-200 confi rm
NAG(confi g-port)#exi t
NAG(confi g)#I nterface port 2
NAG(confi g-port)#swi tchport mode trunk
NAG(confi g-port)#swi tchport trunk allowed vl an 100-200 confi rm
NAG(confi g-port)#exi t

```

Step 2 Set Port 1 to the primary interface and set Port 2 to the backup interface in VLANs 100–150.

```

NAG(confi g)#I nterface port 1
NAG(confi g-port)#swi tchport backup port 2 vl an l i st 100-150
NAG(confi g-port)#exi t

```

Step 3 Set Port 2 to the primary interface and set Port 1 to the backup interface in VLANs 151–200.

```

NAG(confi g)#I nterface port 2
NAG(confi g-port)#swi tchport backup port 1 vl an l i st 151-200

```

Checking results

Use the **show switchport backup** command to show status of interface backup under normal or faulty conditions.

When both Port 1 and Port 2 are Up, Port 1 forwards traffic of VLANs 100–150, and Port 2 forwards traffic of VLANs 151–200.

```

NAG#show swi tchport backup
Restore del ay: 15s.
Restore mode: port-up.
Active Port(State)    Backup Port(State)    Vl an l i st
-----
port1(Up)             port2(Standby)       100-150
port2(Up)             port1(Standby)       151-200

```

Manually disconnect the link between Switch A and Switch B to emulate a fault. Then, Port 1 becomes Down, and Port 2 forwards traffic of VLANs 100–200.

```

NAG#show swi tchport backup
Restore del ay: 15s
Restore mode: port-up
Active Port(State)    Backup Port(State)    Vl an l i st
-----
port1(Down)          port2(Up)             100-150
port2(Up)            port1(Down)           151-200

```


When Port 1 resumes and keeps Up for 15s (restore-delay), it forwards traffic of VLANs 100–150 while Port 2 forwards traffic of VLANs 151–200.

11.3 Failover

11.3.1 Introduction

Failover 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 failover group. Therefore, faults of uplink devices can be informed to the downlink devices to trigger switching. Failover can be used to prevent traffic loss due to uplink failure.

Once all uplink interfaces fail, down link interfaces are in Down status. When at least one uplink interface recovers, downlink interface recovers to Up status. Therefore, faults of uplink devices can be informed to the downlink devices immediately. Uplink interfaces are not influenced when downlink interfaces fail.

11.3.2 Preparing for configurations

Scenario

When uplink fails, traffic cannot switch to the standby link if it cannot notify downlink devices in time, and then traffic will be broken.

Failover can be used to add downlink interfaces and uplink interfaces of the middle device to a failover group and monitor uplink interfaces. When all uplink interfaces fails, faults of uplink devices can be informed to the downlink devices to trigger switching.

Prerequisite

N/A

11.3.3 Default configurations of failover

Default configurations of failover are as below.

Function	Default value
Failover group	N/A

11.3.4 Configuring failover

Configure failover for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.

Step	Command	Description
2	<code>NAG(config)#link-state-tracking group group-number</code>	Create the failover group, and enable failover.
3	<code>NAG(config)#interface { port port-id port-channel port-channel-number }</code>	Enter physical layer interface configuration mode.
4	<code>NAG(config-port)#link-state-tracking group group-number { downstream upstream }</code>	Configure the failover group of the interface and interface type. One interface can only belong to one failover group and can be either the uplink interface or downlink interface.
	<code>NAG(config-aggregator)#link-state-tracking group group-number { downstream upstream }</code>	
5	<code>NAG(config-port)#link-state-tracking processing mode { shutdown trap-only }</code>	Configure the processing mode for the failover interface.
	<code>NAG(config-aggregator)#link-state-tracking processing mode { shutdown trap-only }</code>	



Note

- One failover group can contain several uplink interfaces. Failover will not be performed when at least one uplink interface is Up. Only when all uplink interfaces are Down, failover occurs.
- In global configuration mode, use the **no link-state-tracking group group-number** command to disable failover. The failover group will be deleted if there is no interface in it.
- Use the **no link-state-tracking group** command to delete an interface from the failover group in physical layer interface configuration mode. If there is no other interface, the failover group will be deleted when the interface is deleted.

11.3.5 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	<code>NAG#show link-state-tracking group group-number [detail]</code>	Show configurations and status of the failover group.

11.3.6 Example for configuring failover

Networking requirements

As shown in Figure 11-8, to improve network reliability, Link 1 and Link 2 of Switch B are connected to Switch A and Switch C respectively. Link 1 is the primary link and Link 2 is the standby link. Link 2 will not be used to forward data until Link 1 is fault.

Switch A and Switch C are connected to the uplink network in link aggregation mode. When all uplink interfaces of Switch A and Switch C fails, Switch B needs to sense fault in time switches traffic to the standby link. Therefore, you should deploy failover on Switch A and Switch C.

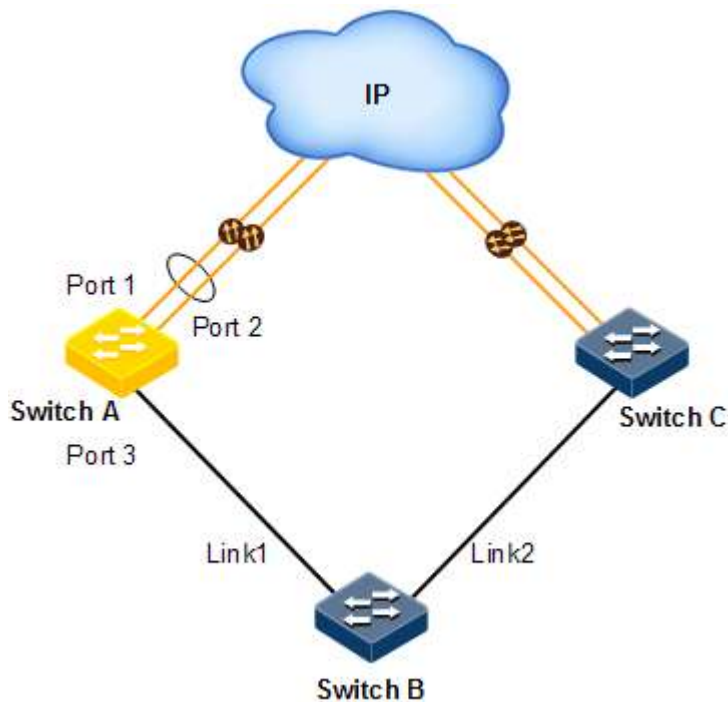


Figure 11-8 Configuring failover

Configuration steps

Step 1 Configure failover on Switch A.

Create LAG 1, and add uplink interfaces to it.

```
NAG#confi g
NAG(confi g)#I nterface port 1
NAG(confi g-port)#channel group 1
NAG(confi g-port)#exl t
NAG(confi g)#I nterface port 2
NAG(confi g-port)#channel group 1
NAG(confi g-port)#exl t
```

Create failover group 1. Add LAG interfaces to the failover group.

```
NAG(config)#link-state-tracking group 1
NAG(config)#interface port-channel 1
NAG(config-aggregator)#link-state-tracking group 1 upstream
NAG(config-aggregator)#exit
```

Add downlink interfaces to the failover group.

```
NAG(config)#interface port 3
NAG(config-g-port)#link-state-tracking group 1 downstream
```

Step 2 Configure failover on Switch C.

Configurations are identical to the ones on Switch A.

Checking results

Take configurations on Switch A for example.

Use the **show link-state-tracking group** command to show configurations of the failover group.

```
SwitchA#show link-state-tracking group 1
Link State Tracking Group: 1 (Enable)
Status: Normal
Upstream Interfaces:
  port-channel 1(Up)
Upstream Mep:
  --
Upstream aps-8031:
  --
Downstream Interfaces:
  Port3(Up)
```

After all uplinks of Switch A fails, use the **show link-state-tracking group** command again, and you can find that downlink Port 3 is disabled.

```
SwitchA#show link-state-tracking group 1
Link State Tracking Group: 1 (Enable)
Status: Failover
Upstream Interfaces:
  port-channel 1(Down)
Upstream Mep:
  --
Upstream aps-8031:
```

```
--  
Downstream Interfaces:  
port3 (Di sabl e)
```

12 System management

This chapter describes basic principle and configuration of system management and maintenance, and provides related configuration examples, including the following sections:

- SNMP
- KeepAlive
- RMON
- Cluster management
- LLDP
- Optical module DDM
- System log
- Alarm management
- Hardware environment monitoring
- CPU monitoring
- CPU protection
- Ping
- Traceroute

12.1 SNMP

12.1.1 Introduction

Simple Network Management Protocol (SNMP) is designed by the Internet Engineering Task Force (IETF) to resolve problems in managing network devices connected to the Internet. Through SNMP, a network management system 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.

Principle of SNMP

SNMP is separated into two parts: Agent and NMS. The Agent and NMS communicate by SNMP packets being sent through UDP.

Figure 12-1 shows the principle of SNMP.

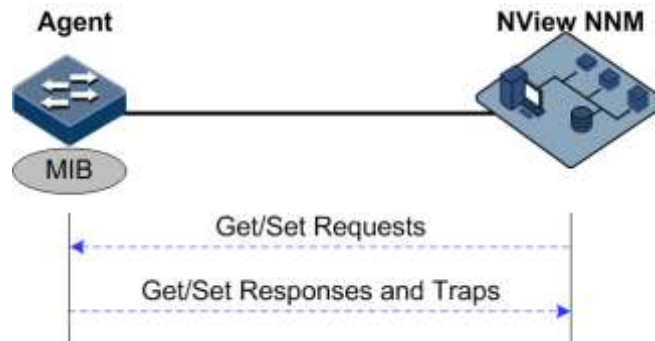


Figure 12-1 Principle of SNMP

NAG NView NNM system can provide friendly Human Machine Interface (HMI) to facilitate network management. The following functions can be realized through it:

- Send request packets to the managed device.
- Receive reply packets and Trap packets from the managed device, and show result.

The Agent is a program installed in the managed device, realizing the following functions:

- Receive/reply request packets from NView NNM system
- Read/write packets and generate response packets according to the packets type, then return the result to NView NNM system
- Define trigger condition according to protocol modules, enter/exit from system or reboot device when conditions are satisfied; reply module sends Trap packets to NView NNM system through agent to report current status of device.



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.

- SNMP v1 uses community name authentication mechanism. The community name, a string defined by an agent, acts like a secret. The network management system can visit the agent only by specifying its community name correctly. If the community name carried in a SNMP packet is not accepted by the SNR-S212i-8POE, the packet will be dropped.
- Compatible with SNMP v1, SNMP v2c also uses community name authentication mechanism. SNMP V2c supports more operation types, data types, and errored codes, and thus better identifying errors.
- SNMP v3 uses User-based Security Model (USM) and View-based Access Control Model (VACM) security models. You can configure whether USM authentication is enabled and whether encryption is enabled to provide higher security. USM authentication mechanism allows authenticated senders and prevents unauthenticated senders. Encryption is to encrypt packets transmitted between the network management system and agents, thus preventing interception.

The SNR-S212i-8POE supports v1, v2c, and v3 of SNMP.

MIB

Management Information Base (MIB) is the collection of all objects managed by 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 SNR-S212i-8POE.

MIB stores information in a tree structure, and its root is on the top, without name. Nodes of the tree are the managed objects, which take a uniquely path starting from root (OID) for identification. SNMP protocol packets can access network devices by checking the nodes in MIB tree directory.

The SNR-S212i-8POE supports standard MIB and NAG-customized MIB.

12.1.2 Preparing for configurations

Scenario

When you need to log in to the SNR-S212i-8POE through NMS, configure SNMP basic functions for the SNR-S212i-8POE in advance.

Prerequisite

Configure the routing protocol to the route between the SNR-S212i-8POE and NMS reachable.

12.1.3 Default configurations of SNMP

Default configurations of SNMP are as below.

Function	Default value												
SNMP view	system and internet views (default)												
SNMP community	public and private communities (default) <table border="1"> <thead> <tr> <th>Index</th> <th>CommunityName</th> <th>ViewName</th> <th>Permission</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>public</td> <td>internet</td> <td>ro</td> </tr> <tr> <td>2</td> <td>private</td> <td>internet</td> <td>rw</td> </tr> </tbody> </table>	Index	CommunityName	ViewName	Permission	1	public	internet	ro	2	private	internet	rw
Index	CommunityName	ViewName	Permission										
1	public	internet	ro										
2	private	internet	rw										
SNMP access group	initialnone and initial access groups (existing by default)												
SNMP user	none, md5nopriv, shapriv, md5priv, and shanopriv users (existing by default)												

Function	Default value			
Mapping relationship between SNMP user and access group	Index	GroupName	UserName	SecModel

	0	initialnone	none	usm
	1	initial	md5priv	usm
	2	initial	shapriv	usm
	3	initial	md5nopriv	usm
4	initial	shanopriv	usm	
Logo and the contact method of administrator	Contact			
Device physical location	Location			
Trap	Enable			
SNMP target host address	N/A			
SNMP engine ID	800022B603000E5E000000			

12.1.4 Configuring basic functions of SNMP v1/v2c

To protect itself and prevent its MIB from unauthorized access, SNMP Agent proposes the concept of community. The management station in the same community must use the community name in all Agent operating. Otherwise, their requests will not be accepted.

The community name uses different SNMP string to identify different groups. Different communities can have read-only or read-write access authority. Groups with read-only authority can only query the device information, while groups with read-write authority can configure the device and query the device information.

SNMP v1/v2c uses the community name authentication scheme, and the SNMP packets which are inconsistent to the community name will be discarded.

Configure basic functions of SNMP v1/v2c for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#snmp- server vi ew <i>vi ew-name</i> <i>oid-tree</i> [<i>mask</i>] { <i>excl uded</i> <i>incl uded</i> }	(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	NAG(confi g)#snmp- server communi ty <i>com-</i> <i>name</i> [<i>vi ew vi ew-</i> <i>name</i>] { <i>ro</i> <i>rw</i> }	Create community name and configure the corresponding view and authority. Use default view internet if vi ew <i>view-name</i> option is empty.

12.1.5 Configuring basic functions of SNMP v3

SNMP v3 uses USM mechanism. USM comes up with the concept of access group. One or more users correspond to one access group. Each access group sets the related read, write, and notification views. Users in an access group have access authorities of this view. The access group of users, who send Get and Set requests, must have authorities corresponding to the requests. Otherwise, the requests will not be accepted.

As shown in Figure 12-2, to access the switch through SNMP v3, you should perform the following configurations:

- Configure users.
- Configure the access group of users.
- Configure the view authority of the access group.
- Create views.

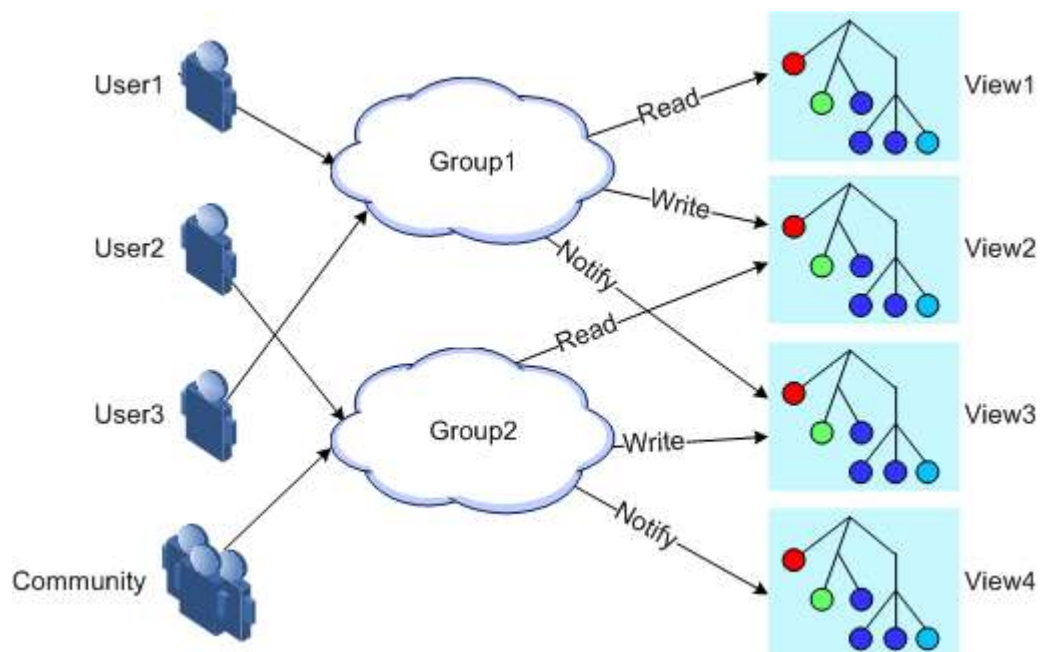


Figure 12-2 SNMP v3 authentication mechanism

Configure basic functions of SNMP v3 for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#snmp-server vi ew vi ew-name oid-tree [mask] { excl uded i ncl uded }</code>	(Optional) create SNMP view and configure MIB variable range.
3	<code>NAG(confi g)#snmp-server user user-name [remote engi ne-i d] authenti cati on { md5 sha } authpassword [pri vacy pri vacypassword]</code>	Create users and configure authentication modes.

Step	Command	Description
4	<code>NAG(config)#snmp-server user <i>user-name</i> [remote <i>engine-id</i>] authkey { md5 sha } keyword [privacy <i>privacypassword</i>]</code>	(Optional) modify the authentication key and the encryption key.
5	<code>NAG(config)#snmp-server access <i>group-name</i> [read <i>view-name</i>] [write <i>view-name</i>] [notify <i>view-name</i>] [context <i>context-name</i> { exact prefix }] usm { authnopriv authpriv noauthnopriv }</code>	Create and configure the SNMP v3 access group.
6	<code>NAG(config)#snmp-server group <i>group-name</i> user <i>user-name</i> usm</code>	Configure the mapping relationship between users and the access group.

12.1.6 Configuring IP authentication by SNMP server

Configure IP authentication by SNMP server for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(config)#snmp-server server-auth enable</code>	Enable SNMP server IP authentication.
3	<code>NAG(config)#snmp-server server-auth <i>ip-address</i></code>	Configure IP authentication address of the SNMP server.

12.1.7 Configuring other information of SNMP


Other information of SNMP includes:

- Logo and contact method of the administrator, which is used to identify and contact the administrator
- Physical location of the device: describes where the device is located

SNMP v1, v2c, and v3 support configuring this information.

Configure other information of SNMP for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.

Step	Command	Description
2	<code>NAG(config)#snmp-server contact <i>contact</i></code>	(Optional) configure the logo and contact method of the administrator.  Note For example, set the E-mail to the logo and contact method of the administrator.
3	<code>NAG(config)#snmp-server location <i>location</i></code>	(Optional) specify the physical location of the device.

12.1.8 Configuring Trap



Trap configurations on SNMP v1, v2c, and v3 are identical except for Trap target host configurations. Configure Trap as required.

Trap is unrequested information sent by the SNR-S212i-8POE 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. SNMP v1 and v2c need to configure the community name; SNMP v3 needs to configure the user name and SNMP view.
- Configure the routing protocol and ensure that the route between the SNR-S212i-8POE and NMS is reachable.

Configure Trap of SNMP for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(config)#I nterface I p <i>if-number</i></code>	Enter Layer 3 interface configuration mode.
3	<code>NAG(config-i p)#I p address <i>ip-address</i> [<i>ip-mask</i>] [<i>sub</i>] [<i>vlan-list</i>]</code>	Configure the IP address of the Layer 3 interface.
4	<code>NAG(config-i p)#exi t</code>	Exit from global configuration and enter privileged EXEC mode.
5	<code>NAG(config)#snmp-server host <i>ip-address</i> versi on 3 { <i>authnopri v</i> <i>authpri v</i> <i>noauthnopri v</i> } <i>user-name</i> [<i>udpport port-id</i>]</code>	(Optional) configure SNMP v3-based Trap target host.
6	<code>NAG(config)#snmp-server host <i>ip-address</i> versi on { 1 2c } <i>com-name</i> [<i>udpport udpport</i>]</code>	(Optional) configure SNMP v1-/SNMP v2c-based Trap target host.

Step	Command	Description
7	NAG(config)#snmp-server enable traps	Enable Trap.

12.1.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show snmp access	Show SNMP access group configurations.
2	NAG#show snmp community	Show SNMP community configurations.
3	NAG#show snmp config	Show SNMP basic configurations.
4	NAG#show snmp group	Show the mapping relationship between SNMP users and the access group.
5	NAG#show snmp host	Show Trap target host information.
6	NAG#show snmp statistics	Show SNMP statistics.
7	NAG#show snmp user	Show SNMP user information.
8	NAG#show snmp view	Show SNMP view information.
9	NAG#show snmp server-auth	Show SNMP server authentication configurations.

12.1.10 Example for configuring SNMP v1/v2c and Trap

Networking requirements

As shown in Figure 12-3, the route between the NView NNM system and Agent is reachable. The Nview NNM system can view MIBs in the view of the remote switch through SNMP v1/v2c. And the switch can automatically send Trap to Nview NNM in emergency.

By default, there is VLAN 1 in the SNR-S212i-8POE and all physical interfaces belong to VLAN 1.

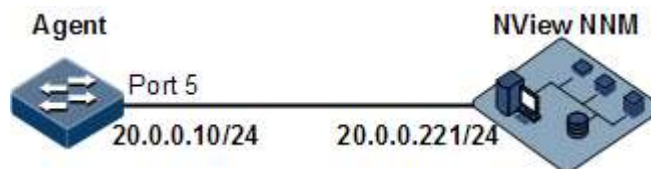


Figure 12-3 Configuring SNMP v1/v2c and Trap

Configuration steps

Step 1 Configure the IP address of the switch.

```
NAG#confi g
NAG(confi g)#I nterface I p 0
NAG(confi g-i p)#I p address 20. 0. 0. 10 255. 255. 255. 0 1
NAG(confi g-i p)#exl t
```

Step 2 Configure the SNMP v1/v2c view.

```
NAG(confi g)#snmp-server vi ew mi b2 1. 3. 6. 1. 2. 1 i ncl uded
```

Step 3 Configure the SNMP v1/v2c community.

```
NAG(confi g)#snmp-server communi ty NAG vi ew mi b2 ro
```

Step 4 Configure Trap.

```
NAG(confi g)#snmp-server enable traps
NAG(confi g)#snmp-server host 20.0.0.221 versi on 2c NAG
```

Checking results

Use the **show interface ip brief** command to show configurations of IP addresses.

```
NAG#show I p I nterface bri ef
I F      Address          NetMask          Source          Catagory
-----
0       20. 0. 0. 10      255. 255. 255. 0  assi gned      pri mary
```

Use the **show snmp view** command to show view configurations.

```
NAG#show snmp vi ew
I ndex:      0
Vi ew Name:  mi b2
O I D Tree:  1. 3. 6. 1. 2. 1
Mask:       --
Type:       i ncl ude
...
```

Use the **show snmp community** command to show community configurations.

```
NAG#show snmp community
Index   Community Name   View Name   Permission
-----
1       private          internet   rw
2       public           internet   ro
3       NAG              mi b2      ro
```

Use the **show snmp host** command to show configurations of the Trap target host.

```
NAG#show snmp host
Index:      0
IP family:  IPv4
IP address: 20.0.0.221
Port:       162
User Name:  NAG
SNMP Version: v2c
Security Level: noauthnopriv
TagList:    bridge config interface rmon snmp ospf
```

12.1.11 Example for configuring SNMP v3 and Trap

Networking requirements

As shown in Figure 12-4, the route between the NView NNM system and Agent is reachable. The Nview NNM system monitors the Agent through SNMP v3. The Agent can automatically send Trap to Nview NNM in emergency.

By default, there is VLAN 1 in the SNR-S212i-8POE and all physical interfaces belong to VLAN 1.

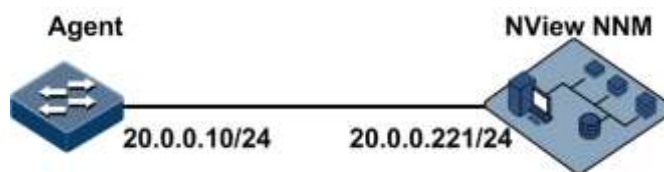


Figure 12-4 Configuring SNMP v3 and Trap

Configuration steps

Step 1 Configure the IP address of the switch.

```
NAG#confi g
NAG(confi g)#i nterface i p 0
NAG(confi g-i p)#i p address 20. 0. 0. 10 255. 255. 255. 0 1
NAG(confi g-i p)#exi t
```

Step 2 Configure SNMP v3 access.

Configure access view mib2, including all MIB variables under 1.3.6.x.1.

```
NAG(confi g)#snmp-server vi ew mi b2 1. 3. 6. 1. 2. 1 1. 1. 1. 1. 0. 1 i ncl uded
```

Create user gusterus1. Adopt md5 authentication algorithm. Set the password to NAG.

```
NAG(confi g)#snmp-server user gustomer1 authenti cati on md5 NAG
```

Create a guestgroup access group. Set the security mode to usm. Set the security level to authnopriv. Set the name of the read-only view to mib2.

```
NAG(confi g)#snmp-server access guestgroup read mi b2 usm authnopri v
```

Map user gustomer1 to the access group guestgroup.

```
NAG(confi g)#snmp-server group guestgroup user gustomer1 usm
```

Step 3 Configure Trap.

```
NAG(confi g)#snmp-server enable traps  
NAG(confi g)#snmp-server host 20.0.0.221 versi on 3 authnopri v gustomer1
```

Checking results

Use the **show snmp access** command to show configurations of the SNMP access group.

```
NAG#show snmp access  
...  
Index:          1  
Group:          guestgroup  
Security Model: usm  
Security Level: authnopri v  
Context Prefix: --  
Context Match: exact  
Read View:     mi b2  
Write View:    --  
Notify View:   i nternet  
...
```


Use the **show snmp group** command to show the mapping between users and the access group.

```
NAG#show snmp group
Index      GroupName      UserName      SecModel
-----
0          initial none      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.

```
NAG#show snmp host
Index:      0
IP family:  IPv4
IP address: 20.0.0.221
Port:       162
User Name:  guestuser1
SNMP Version: v3
Security Level: authpriv
TagList:    bridge config interface rmon snmp ospf
```

12.2 KeepAlive

12.2.1 Introduction

KeepAlive packet is a kind of KeepAlive mechanism running in High-Level Data Link Control (HDLC) link layer protocol. The SNR-S212i-8POE will send a KeepAlive packet to confirm whether the peer is online every several seconds to realize neighbour detection mechanism.

Trap is the unrequested information sent by the SNR-S212i-8POE actively to NMS, used to report some urgent and important events.

The SNR-S212i-8POE sends KeepAlive Trap packet actively to the NView NNM system. The KeepAlive Trap packet includes the basic information of SNR-S212i-8POE, such as the name, OID, MAC address, and IP address. The Nview NNM system synchronizes device information based on IP address to discover NEs in a short time. This helps improve working efficiency and reduce working load of the administrator.

12.2.2 Preparing for configurations

Scenario

The SNR-S212i-8POE sends KeepAlive Trap packet actively to the NView NNM system. Therefore, the Nview NNM system can discover NEs in a short time. This helps improve working efficiency and reduce working load of the administrator. You can enable or disable KeepAlive Trap and configure the period for sending KeepAlive Trap. When KeepAlive Trap is enabled, if configured with **snmp enable traps** and Layer 3 IP address, the SNR-S212i-8POE will send a KeepAlive Trap to all target hosts with Bridge Trap every KeepAlive Trap interval.

Prerequisite

- Configure basic functions of SNMP. SNMP v1 and v2c need to configure the community name; SNMP v3 needs to configure the user name and SNMP view.
- Configure the routing protocol to make the route between the SNR-S212i-8POE and NMS reachable.

12.2.3 Default configurations of KeepAlive

Default configurations of KeepAlive are as below.

Function	Default value
KeepAlive Trap	Disable
KeepAlive Trap period	300s

12.2.4 Configuring KeepAlive

Configure KeepAlive for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#snmp-server keepal i ve-trap enable	Enable KeepAlive Trap.
3	NAG(confi g)#snmp-server keepal i ve-trap i nterval <i>peri od</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, the real transmission period of KeepAlive Trap is timed as period+5s random transmission.

12.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show keepal i ve	Show KeepAlive configurations.

12.2.6 Example for configuring KeepAlive

Networking requirements

Figure 12-5 shows how to configure KeepAlive.

- IP address of the switch: 192.169.1.2
- IP address of the SNMP v2c Trap target host: 192.168.1.1
- Name of the read-write community: public
- SNMP version: SNMP v2c
- Period for sending KeepAlive Trap: 120s
- KeepAlive Trap: enabled

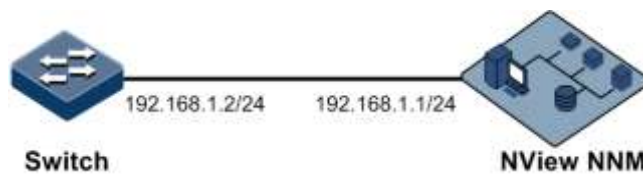


Figure 12-5 Configuring KeepAlive

Configuration steps

Step 1 Configure the management IP address of the switch.

```
NAG#confi g
NAG(confi g)#i nterface l p 0
NAG(confi g-i p)#i p address 192. 168. 1. 2 255. 255. 255. 0 1
NAG(confi g-i p)#exi t
```

Step 2 Configure the IP address of the SNMP Trap target host.

```
NAG(confi g)#snmp-server host 192. 168. 1. 1 versi on 2c publ ic
```

Step 3 Enable KeepAlive Trap.

```
NAG(confi g)#snmp-server keepal i ve-trap enabl e
NAG(confi g)#snmp-server keepal i ve-trap i nterval 120
```

Checking results

Use the **show keepalive** command to show KeepAlive configurations.

```
NAG#show keepal i ve
Keepal i ve Admi n State: Enabl e
Keepal i ve trap i nterval : 120s
Keepal i ve trap count: 1
```

12.3 RMON

12.3.1 Introduction

Remote Network Monitoring (RMON) is a standard stipulated by IETF (Internet Engineering Task Force) for network data monitoring through different network Agent and NMS.

RMON is achieved based on SNMP architecture, including the network management center 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 network segment and the whole network, while SNMP only can monitor the partial information of a single device and it is difficult for it to monitor one network segment.

RMON Agent is commonly referred to as the probe program; RMON Probe can take the communication subnet statistics and performance analysis. Whenever it finds network failure, RMON Probe can report network management center, and describes the capture information under unusual circumstances so that the network management center 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, network segment or device malfunction more quickly. This approach reduces the data flows between network management center 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 data collection methods:

- Distributed RMON: network management center obtains network management information and controls network resources directly from RMON Probe through dedicated RMON Probe collection data.
- Embedded RMON: embed RMON Agent directly to network devices (such as switches) to make them with RMON Probe function. Network management center will collect network management information through the basic operation of SNMP and the exchange data information of RMON Agent.

The SNR-S212i-8POE adopts embedded RMON, as shown in Figure 12-6. The SNR-S212i-8POE implements RMON Agent. Through this function, the management station can obtain the overall flow, error statistics, and performance statistics of this network segment connected to the managed network device interface to a monitor the network segment.

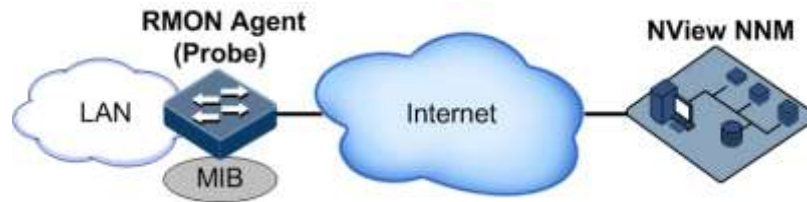


Figure 12-6 RMON

RMON MIBs are grouped into 9 groups according to functions. Currently, there are 4 groups achieved: statistics group, history group, alarm group, and event group.

- **Statistics group:** collect statistics on each interface, including number of received packets and packet size distribution statistics.
- **History group:** similar with the statistics group, but it only collect statistics in an assigned detection period.
- **Alarm group:** monitor an assigned MIB object, set the upper and lower thresholds in an assigned time interval, and trigger an event if the monitored object exceeds the threshold.
- **Event group:** cooperating with the alarm group, when alarm triggers an event, it records the event, such as sending Trap or writing it into the log, etc.

12.3.2 Preparing for configurations

Scenario

RMON helps monitor and account network traffics.

Compared with SNMP, RMON is a more high-efficient monitoring method. After you specifying the alarm threshold, the SNR-S212i-8POE actively sends alarms when the threshold is exceeded without obtaining variable information. This helps reduce traffic of Central Office (CO) and managed devices and facilitates network management.

Prerequisite

The route between the SNR-S212i-8POE and the NView NNM system is reachable.

12.3.3 Default configurations of RMON

Default configurations of RMON are as below.

Function	Default value
Statistics group	Enable
History group	Disable
Alarm group	N/A
Event group	N/A

12.3.4 Configuring RMON statistics

RMON statistics is used to take statistics on an interface, including the number of received packets, undersized/oversized packets, collision, CRC and errors, discarded packets, fragments, unicast packets, broadcast packets, and multicast packets, as well as received packet size.

Configure RMON statistics for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#rmon stati stics port-l ist port-l ist [owner owner-name]	Enable RMON statistics on an interface and configure related parameters.



Note

When using the **no rmon statistics port-list port-list** command to disable RMON statistics on an interface, you cannot continue to obtain the interface statistics, but the interface can still count data.

12.3.5 Configuring RMON historical statistics

Configure RMON historical statistics for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#rmon hi story port-l ist port-l ist [shorti nterval short-period] [longi nterval long-period] [buckets buckets-number] [owner owner-name]	Enable RMON historical statistics on an interface and configure related parameters.



Note

When you use the **no rmon historyport-list port-list** command to disable RMON historical statistics on an interface, the interface will not count data and clear all historical data collected previously.

12.3.6 Configuring RMON alarm group

You can monitor a MIB variable (mibvar) by setting a RMON alarm group instance (*alarm-id*). An alarm event is generated when the value of the monitored data exceeds the defined threshold. And then record the log or send Trap to the NView NNM system according to the definition of alarm events.

The monitored MIB variable must be real, and the data value type is correct.

- If the setting variable does not exist or value type variable is incorrect, the system returns an error.
- For the successfully-set alarm, if the variable cannot be collected later, close the alarm. Reset it if you need to monitor the variable again.

By default, the triggered event ID is 0, which indicates that no event is triggered. If the number is not set to 0 and there is no event configured in the event group, the event will not be successfully triggered when the monitored variable is abnormal. The event cannot be successfully triggered unless the event is established.

The alarm will be triggered as long as the upper or lower threshold of the event in the event table is matched. The alarm is not generated even when alarm conditions are matched if the event related to the upper/lower threshold (*rising-event-id* or *falling-event-id*) is not configured in the event table.

Configure RMON alarm group for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#rmon alarm <i>alarm-id</i> <i>mi bvar</i> [<i>interval period</i>] { <i>absolute</i> <i>delta</i> } <i>rising-threshold rising-value</i> [<i>rising-event-id</i>] <i>falling-threshold falling-value</i> [<i>falling-event-id</i>] [<i>owner owner-name</i>]	Add alarm instances to the RMON alarm group and configure related parameters.

12.3.7 Configuring RMON event group

Configure RMON event group for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#rmon event <i>event-id</i> [<i>log</i>] [<i>trap</i>] [<i>description string</i>] [<i>owner owner-name</i>]	Add events to the RMON event group and configure processing modes of events.

12.3.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show rmon	Show RMON configurations.
2	NAG#show rmon alarms	Show information about the RMON alarm group.
3	NAG#show rmon events	Show information about the RMON event group.

No.	Command	Description
4	NAG#show rmon statistics [port-list port-list]	Show information about the RMON statistics group.
5	NAG#show rmon history port-list port-list	Show information about the RMON history group.

12.3.9 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	NAG(config)#clear rmon	Clear all RMON configurations.

12.3.10 Example for configuring RMON alarm group

Networking requirements

As shown in Figure 12-7, the SNR-S212i-8POE is the Agent, connecting to terminal through Console interface, connecting to the remote NNM system through Internet. Enable RMON statistics and perform performance statistics on Port 1. When the number of packets received by Port 1 exceeds the threshold in a period, the SNR-S212i-8POE records logs and sends Trap to the NView NNM system.

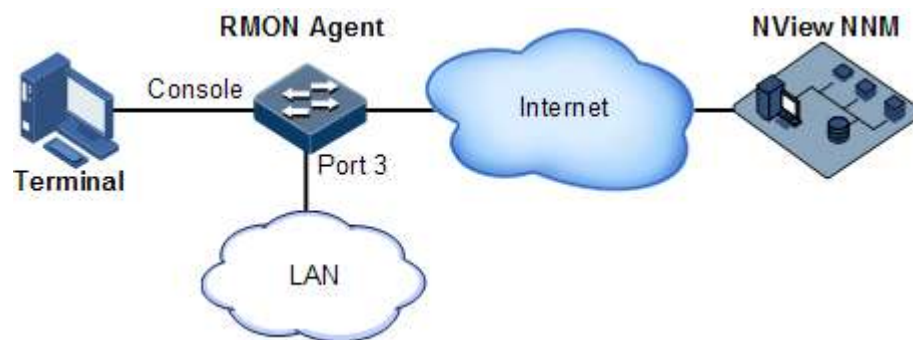


Figure 12-7 Configuring RMON alarm group

Configuration steps

- Step 1 Create event 1. Event 1 is used to record and send the log information which contains the string High-ifOutErrors. The owner of the log information is set to system.

```

NAG#confi g
NAG(config)#rmon event 1 log description High-ifOutErrors owner system
  
```


- Step 2 Create alarm 10. Alarm 10 is used to monitor the MIB variable (1.3.6.1.2.1.2.2.1.20.1) every 20 seconds. If the value of the variable is added by 15 or greater, a Trap is triggered. The owner of the Trap is also set to system.

```
NAG(confi g)#rmon alarm 10 1.3.6.1.2.1.2.2.1.20.1 interval 20 del ta ri si ng-  
threshold 15 1 fall i ng-threshol d 0 owner system
```

Checking results

Use the **show rmon alarms** command to show information about the alarm group.

```
NAG#show rmon alarms  
Alarm 10 is active, owned by system  
Moni tors 1.3.6.1.2.1.2.2.1.20.1 every 20 seconds  
Taki ng del ta samples, last value was 0  
Ri si ng threshol d is 15, assigned to event 1  
Fall i ng threshol d is 0, assigned to event 0  
On startup enable ri si ng and fall i ng alarm
```

Use the **show rmon events** command to show information about the event group on the SNR-S212i-8POE.

```
NAG#show rmon events  
Event 1 is active, owned by system  
Event descri pti on: Hi gh-i fOutErrors.  
Event generated at 0:0:0  
Regi ster log i nformation when event is fi red.
```

When an alarm event is triggered, you can view related records at the alarm management dialog box of the NView NNM system.

12.4 Cluster management

12.4.1 Introduction

Cluster management protocol is used to manage a set of switch devices to provide users a new management method.

You can set up a cluster through a master switch to achieve centralized management and configuration to multiple devices added to the cluster. The main switch is called commander device, and the other managed switches are member devices. The commander device has a public IP address, while the member device is not configured with the IP address; the management and maintenance of member devices are often achieved through command redirection.

The cluster management can reduce workload of engineering and maintenance, and also save public IP address resources. The administrator only needs to configure the public IP address on one device to achieve management and maintenance of all cluster devices without logging into each device for configuration.

When using cluster management, different manufacturers have different implementations on the cluster program, generally using proprietary protocols, cluster, which shows that the cluster management technology has its limitations.

Cluster roles

According to the different position and function of switches, the cluster has different roles. You can configure to specify the role of switch. The cluster role can be commander device, member device, and candidate device.

- **Commander:** also known as the management device, used to assign public IP addresses to provide management interfaces for all switches in the cluster. The commander device manages member devices by command redirection: the NMS system sends commands to the commander device for processing through the public network. The commander device will forward commands to member devices if it finds the commands should be executed on member devices. The commander device can discover neighbor information, collect the entire network topology, manage cluster, maintain cluster state, and support a variety of agent functions.
- **Member:** members in cluster, generally not configured with a public IP address. You manage member devices by command redirection through the commander device. The member device can discover neighbor information, accept commander device management, equipment, execute the commands from the commander device, and report fault/log. The member device can be managed through the NMS or Telnet mode directly on the commander device after activation.
- **Candidate:** it has not joined any clusters but still has cluster ability to become a cluster member switch. The difference from member device is the topology information of candidate device has already collected by commander device but not yet joined the cluster. When a candidate device is added to the cluster, it becomes a member device. When a member device is removed from the cluster, the device will recover to the candidate device again.

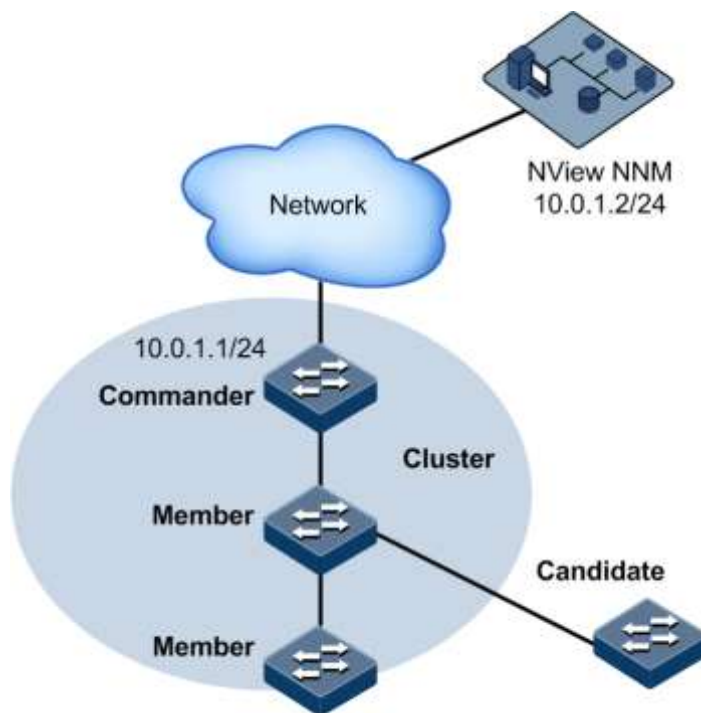


Figure 12-8 Cluster management

As shown in Figure 12-8, the switch configured with the IP address is the commander device, while the switch managed by the commander device redirection is a member device. The commander device and member devices can form a cluster. The device not joining the cluster but with cluster ability is the candidate device.

Principle of cluster

Cluster management mainly contains three protocols:

- Remote Neighbor Discover Protocol (RNDP) is responsible for the neighbor discovery and information gathering of devices.
- Remote Topology Discover Protocol (RTDP) is responsible for the entire network topology information collection and processing.
- Remote Cluster Management Protocol (RCMP) mainly configures to add, activate, and delete cluster members.

RTDP and RCMP protocols make communication in the cluster VLAN. So, if there are devices not supporting SNR cluster management between the two devices for cluster management, you need to configure the cluster VLAN to ensure normal communication of RCMP and RTDP protocols.

Each cluster must be specified with a commander device. After the commander device is specified, it can discover and determine candidate devices through neighbour discovery and topology gathering protocol. You can add candidate device to the cluster by configuring them.

The candidate device will become a member device after be added to the cluster. If you wish to manage the SNR-S212i-8POE through cluster management, you must activate it, or configure auto-activation on it.

12.4.2 Preparing for configurations

Scenario

There are a large number of switches needed to be managed in Layer 2 network, but the number of usable IP addresses is limited. Cluster management can use one IP address to manage multiple devices in one cluster.

Prerequisite

Ensure that the link between commander device and member device is reachable.

12.4.3 Default configurations of cluster management

Default configurations of cluster management are as below.

Function	Default value
Device cluster role	Candidate
Global RNDP status of cluster member	Disable
Interface RNDP of cluster member	Enable
RTDP collection of cluster member	Disable
Maximum RTDP collection range of cluster member	16 hops
Cluster management VLAN	VLAN 4093
Cluster management of the commander device	Disable
Maximum number of members managed by the commander device in the cluster	128
Auto-activation of candidate device	Disable
MAC address of the commander device for auto-activation of candidate devices	0000.0000.0000

12.4.4 Configuring RNDP

Configure RNDP for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# rndp enabl e	Enable global RNDP.
3	NAG(confi g)# i nterface port port-i d	Enter physical layer interface configuration mode.
4	NAG(confi g-port)# rndp enabl e	Enable interface RNDP.

12.4.5 Configuring RTDP

Configuring basic functions of RTDP

Configure basic functions of RTDP for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# rtdp enabl e	Enable global RTDP function.
3	NAG(confi g)# rtdp max-hop max-hop	(Optional) configuration the maximum RTDP collection range for cluster member.

(Optional) configuring cluster VLAN



Caution

When configuring cluster VLAN, if the SNR-S212i-8POE is a commander device or member device, due to the cluster device has already confirmed cluster VLAN, then cluster VLAN configuration will lead to conflict and failure, exit cluster and configure successfully.

Configure cluster VLAN for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# cl uster vl an vlan-id port-list port-list	Configure cluster VLAN and interface list. The VLAN used by cluster protocol packet communication has limited the range of cluster management.

12.4.6 Configuring cluster management on commander devices

Enabling cluster management



Caution

This configuration only applies to the command device.

If the SNR-S212i-8POE is a cluster member device, delete it from member devices if you wish to use it as the commander device. At this time, the SNR-S212i-8POE has become the commander device, but the SNR-S212i-8POE still cannot manage other devices because there is already a commander device on the network.

Enable cluster management for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# cl uster r	Configure the SNR-S212i-8POE as the commander device and enable cluster management.
3	NAG(confi g-cl uster)# max-member <i>max-number</i>	(Optional) configure the maximum number of members managed by the commander device in the cluster.

Adding and activating candidate devices automatically

On the commander device, to facilitate adding and activating cluster members, you can use the same user name and password to add and activate all the candidate devices, or you can perform adding and activation operations on all candidate devices configured by this command. In addition, you can add or activate candidate devices one by one by following CLI.

Add and activate candidate devices automatically for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# cl uster	Enter cluster configuration mode.
3	NAG(confi g-cl uster)# member auto-build [active <i>user-name password</i> [all]]	Add and activate candidate devices automatically.

Adding and activating candidate device manually

To add and activate candidate device on commander device, you need to add cluster management device to cluster and activate it. After adding member device to the cluster, commander device cannot manage member device through cluster management without activation.

Add and activate candidate devices manually for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# cl uster	Enable cluster management function and enter cluster configuration mode.
3	NAG(confi g-cl uster)# member <i>mac-address</i> [active <i>user-name password</i>]	Configure to add candidate device to cluster and activate it. Use the no member { all <i>mac-address</i> } command to delete all or specified cluster members. Use the member { all <i>mac-address</i> } suspend to suspend all or specified cluster members.

Accessing member devices remotely

Configure accessing member devices remotely for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# cl uster	Enter cluster configuration mode.
3	NAG(confi g-cl uster)# rcommand { <i>hostname</i> [<i>mac-address</i>] <i>mac-address</i> }	Log in to the cluster member device. You can conduct remote management to the activated member devices on the commander device.

12.4.7 (Optional) configuring auto-activation for candidate device

You must set MAC address of the commander device after setting auto-activation on candidate device. And then the candidate device can be activated automatically by its commander device if the commander device is configured to add and activate all candidate members to cluster automatically when connecting the SNR-S212i-8POE to network.

Configure auto-activation for candidate device for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# cl uster-autoacti ve	Enable auto-activation.
3	NAG(confi g)# cl uster-autoacti ve commander-mac <i>mac-address</i>	Specify the MAC address of the commander device.

12.4.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG# show rndp	Show RNDP configurations.
2	NAG# show rndp nei ghbor	Show information about the RNDP neighbor.
3	NAG# show cl uster { candi date member [<i>mac-address</i>] }	Show configurations on candidate and member devices.
4	NAG# show rtdp	Show RTDP configurations.
5	NAG# show cl uster vl an	Show cluster VLAN configurations.
6	NAG# show rtdp devi ce-l i st [<i>mac-address</i> <i>hostname</i>] [detai led]	Show RTDP discovery device list.

No.	Command	Description
7	NAG#show cluster	Show cluster information.

12.4.9 Example for providing remote access through cluster management

Networking requirements

A lot of devices in Layer 2 network need to be managed, but current public IP address resources are limited. To manage multiple devices through a device, you can configure cluster management.

Cluster management uses one IP address to manage multiple devices in a cluster. Cluster management can be used to manage all member devices in cluster through commander device and log in to member devices remotely for configuration and maintenance.

As shown in Figure 12-9, Switch A can log in to Switch B and Switch C for remote management and maintenance. The following table list configurations on Switch A, Switch B, and Switch C.

Device	MAC address	Role
Switch A	000E.5E03.5318	Commander device
Switch B	000E.5EBD.5951	Member device
Switch C	000E.5E03.023C	Member device

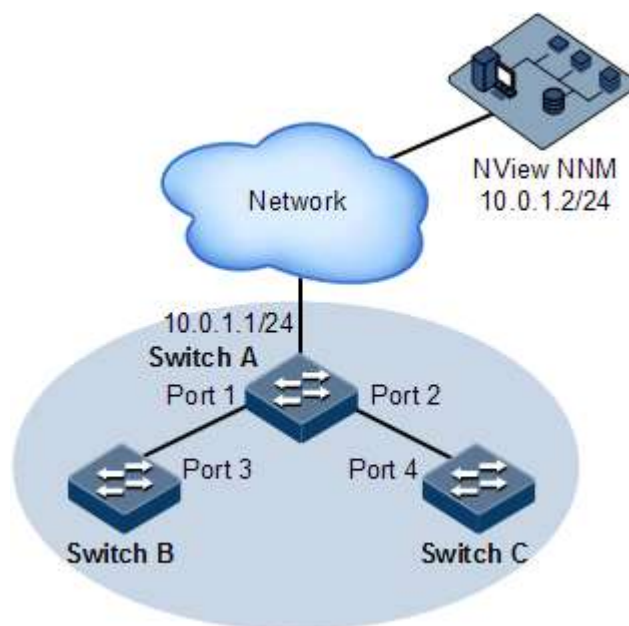


Figure 12-9 Providing remote access through cluster management

Configuration steps

Step 1 Enable global RNDP and enable RNDP on interfaces. Enable RTDP on Switch A.

Configure Switch A.

```
NAG#hostname Swi tchA
Swi tchA#confi g
Swi tchA(confi g)#rndp enable
Swi tchA(confi g)#rt dp enable
Swi tchA(confi g)#i nterface port 1
Swi tchA(confi g-port)#rndp enable
Swi tchA(confi g-port)#exi t
Swi tchA(confi g)#i nterface port 2
Swi tchA(confi g-port)#rndp enable
Swi tchA(confi g-port)#exi t
```

Configure Switch B.

```
NAG#hostname Swi tchB
Swi tchB#confi g
Swi tchB(confi g)#rndp enable
Swi tchB(confi g)#i nterface port 3
Swi tchB(confi g-port)#rndp enable
Swi tchB(confi g-port)#exi t
```

Configure Switch C.

```
NAG#hostname Swi tchC
Swi tchC#confi g
Swi tchC(confi g)#rndp enable
Swi tchC(confi g)#i nterface port 4
Swi tchC(confi g-port)#rndp enable
Swi tchC(confi g-port)#exi t
```

Step 2 Enable cluster management on Switch A and automatically activate all candidate devices.

```
Swi tchA(confi g)#cl uster
Swi tchA(confi g-cl uster)#member auto-bui ld acti ve NAG NAG al l
Swi tchA(confi g-cl uster)#exi t
```

Step 3 Enable auto-activation on Switch B and Switch C.

Configure Switch B.

```

SwitchB(config)#cluster-autoactive
SwitchB(config)#cluster-autoactive commander-mac 000e.5e03.5318

```

Configure Switch C.

```

SwitchC(config)#cluster-autoactive
SwitchC(config)#cluster-autoactive commander-mac 000e.5e03.5318

```

Step 4 Log in to Switch B through Switch A.

```

SwitchA#confi g
SwitchA(config)#cluster
SwitchA(config-cluster)#rcommand SwitchB
Logi n: NAG
Password:
SwitchB>

```

Step 5 Log in to Switch C through Switch A. Steps are identical to the ones used for logging in to Switch B.

Checking results

Use the **show cluster** command to show cluster information on Switch A.

```

SwitchA#show cluster
Identity: Commander
Current member number: 2
Max member number: 128

```

Use the **show cluster** command to show information about the cluster member.

```

SwitchA#show cluster member
MAC Address      ActiveOperati onState  ActiveManageState  Hostname
-----
000E.5EBD.5951  Up                    Active              SwitchB
000E.5E03.023C  Up                    Active              SwitchC

```

Use the **show cluster** to show cluster information on Switch B.

```

SwitchB#show cluster
Identity: Member
Autoactive: ON

```

```
Autoactive commander mac: 000e.5e03.5318
```

Use the **show cluster** command to show cluster information on Switch C. Configurations are identical to the ones on Switch B.

12.5 LLDP

12.5.1 Introduction

With the enlargement of network scale and increase of network devices, the network topology becomes more and more complex and network management becomes very important. A lot of network management software adopts "auto-detection" function to trace changes of network topology, but most of the software can only analyze to the 3rd layer and cannot ensure that the interfaces connect to other devices.

Link Layer Discovery Protocol (LLDP) is based on IEEE 802.1ab standard. Network management system can fast grip the Layer 2 network topology and changes.

LLDP organizes the local device information in different Type Length Value (TLV) and encapsulates in Link Layer Discovery Protocol Data Unit (LLDPDU) to transmit to straight-connected neighbour. It also saves the information from neighbour as standard Management Information Base (MIB) for network management system querying and judging link communication.

Basic concepts

LLDP packet is to encapsulate LLDPDU Ethernet packet in data unit and transmitted by multicast.

LLDPDU is data unit of LLDP. The device encapsulates local information in TLV before forming LLDPDU, then several TLV fit together in one LLDPDU and encapsulated in Ethernet data for transmission.

As shown in Figure 12-11, LLDPDU is made by several TLV, including 4 mandatory TLV and several optional TLV.

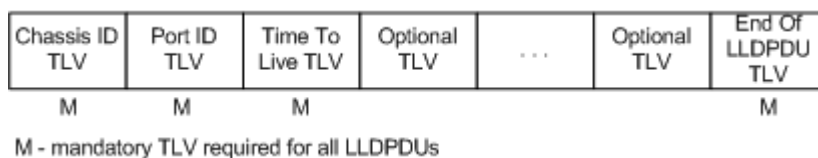


Figure 12-10 LLDPDU structure

TLV: unit combining LLDPDU, which refers to the unit describing the object type, length and information.

As shown in Figure 12-11, each TLV denotes piece of information at local, such as device ID, interface number, etc. related Chassis ID TLV, Port ID TLV fixed TLV.

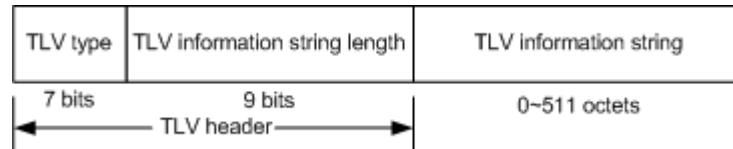


Figure 12-11 Basic TLV structure

Table 12-1 lists TLV type. At present only types 0–8 are used.

Table 12-1 TLV types

TLV type	Description	Optional/Required
0	End Of LLDPDU	Required
1	Chassis ID	Required
2	Port ID	Required
3	Time To Live	Required
4	Port Description	Optional
5	System Name	Optional
6	System Description	Optional
7	System Capabilities	Optional
8	Management Address	Optional

Principle of LLDP

LLDP is a kind of point-to-point one-way issuance protocol, which sends link status of the local device to peer end by sending LLDPDU (or sending LLDPDU when link status changes) periodically from the local device to the peer end.

The procedure of packet exchange is as below:

- When the local device transmits packet, it obtains system information required by TLV from NView NNM (Network Node Management), obtains configurations from LLDP MIB, generates TLV, makes LLDPDU, encapsulates information to LLDP packets, and send LLDP packets to the peer end.
- The peer end receives LLDPDU and analyzes TLV information. If there is any change, the information will be updated in neighbor MIB table of LLDP and the NView NNM system will be notified.

The aging time of Time To Live (TTL) in local device information in the neighbour node can be adjusted by modifying the parameter values of aging coefficient, sends LLDP packets to neighbour node, after receiving LLDP packets, neighbour node will adjust the aging time of its neighbour nodes (sending side) information. Aging time formula, $TTL = \text{Min} \{65535, (\text{interval} \times \text{hold-multiplier})\}$:

- Interval: indicate the period for sending LLDP packets from the neighbor node.
- Hold-multiplier: the aging coefficient of device information in neighbor node.

12.5.2 Preparing for configurations

Scenario

When you obtain connection information between devices through NView NNM system for topology discovery, the SNR-S212i-8POE needs to enable LLDP, notify their information to the neighbours mutually, and store neighbour information to facilitate the NView NNM system queries.

Prerequisite

N/A

12.5.3 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

12.5.4 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 SNR-S212i-8POE 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 SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.

Step	Command	Description
2	NAG(config)#lldp enable	Enable global LLDP.

12.5.5 Enabling interface LLDP

Enable interface LLDP for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode or aggregation group configuration mode.
3	NAG(config-port)#lldp enable NAG(config-aggregator)#lldp enable	Enable LLDP on an interface.

12.5.6 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 SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(config)#lldp message-transmission interval <i>period</i>	(Optional) configure the period timer of the LLDP packet.
3	NAG(config)#lldp message-transmission delay <i>period</i>	(Optional) configure the delay timer of the LLDP packet.
4	NAG(config)#lldp message-transmission hold-multiplier <i>hold-multiplier</i>	(Optional) configure the aging coefficient of the LLDP packet.
5	NAG(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.

12.5.7 Configuring LLDP alarm

When the network changes, you need to enable LLDP alarm notification function to send topology update alarm to the NView NNM system immediately.

Configure LLDP alarm for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# snmp-server ll dp-trap enable	Enable LLDP alarm.
3	NAG(confi g)# ll dp trap-interval <i>period</i>	(Optional) configure the period timer of LLDP alarm Trap.



Note

After enabled with LLDP alarm, the SNR-S212i-8POE will send Traps after detecting aged neighbours, newly-added neighbours, and changed neighbour information.

12.5.8 Configuring destination MAC address of LLDP packets

Configure the destination MAC address of LLDP packets for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# i nterface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode or aggregation group configuration mode.
3	NAG(confi g-port)# ll dp dest-address <i>mac-address</i> NAG(confi g-aggregato r)# ll dp dest-address <i>mac-address</i>	Configure the destination MAC address of the LLDP packets.

12.5.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG# show ll dp local confi g	Show LLDP local configurations.
2	NAG# show ll dp local system-data [<i>interface-type interface-number</i>]	Show information about the LLDP local system.
3	NAG# show ll dp remote [<i>interface-type interface-number</i>] [detail]	Show information about the LLDP neighbor.

No.	Command	Description
4	NAG#show ll dp statisti c [interface-type interface-number]	Show statistics of LLDP packets.

12.5.10 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	NAG(confi g)#cl ear ll dp gl obal statisti c	Clear global LLDP statistics.
2	NAG(confi g)#cl ear ll dp statisti c interface-type interface-number	Clear LLDP statistics.
3	NAG(confi g)#cl ear ll dp remote-table [interface-type interface-number]	Clear LLDP neighbor information.

12.5.11 Example for configuring basic functions of LLDP

Networking requirements

As shown in Figure 12-12, Switches are connected to the NView NNM system. Enable LLDP on links between Switch A and Switch B. And then you can query the Layer 2 link changes through the NView NNM system. If the neighbour is aged, the neighbour is added, or the neighbour information changes, Switch A and Switch B sends LLDP alarm to the NView NNM system.

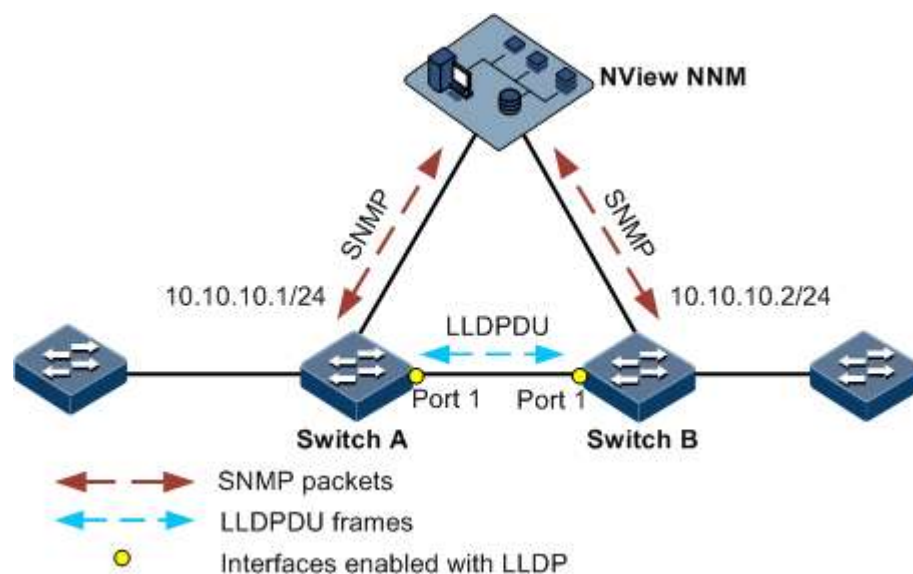


Figure 12-12 Configuring basic functions of LLDP

Configuration steps

Step 1 Enable LLDP globally and enable LLDP alarm.

Configure Switch A.

```
NAG#hostname Swi tchA
Swi tchA#confi g
Swi tchA(confi g)#l l dp enabl e
Swi tchA(confi g)#snmp-server l l dp-trap enabl e
```

Configure Switch B.

```
NAG#hostname Swi tchB
Swi tchB#confi g
Swi tchB(confi g)#l l dp enabl e
Swi tchB(confi g)#snmp-server l l dp-trap enabl e
```

Step 2 Configure management IP addresses.

Configure Switch A.

```
Swi tchA(confi g)#create vl an 1024 acti ve
Swi tchA(confi g)#i nterface port 1
Swi tchA(confi g-port)#swi tchport access vl an 1024
Swi tchA(confi g-port)#exi t
Swi tchA(confi g)#i nterface i p 1
Swi tchA(confi g-i p)#i p address 10. 10. 10. 1 1024
Swi tchA(confi g-i p)#exi t
```

Configure Switch B.

```
Swi tchB(confi g)#create vl an 1024 acti ve
Swi tchB(confi g)#i nterface port 1
Swi tchB(confi g-port)#swi tchport access vl an 1024
Swi tchB(confi g)#i nterface i p 1
Swi tchB(confi g-i p)#i p address 10. 10. 10. 2 1024
Swi tchB(confi g-i p)#exi t
```

Step 3 Configure LLDP properties.

Configure Switch A.

```
Swi tchA(confi g)#l l dp message-transmi ssi on i nterval 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 LLDP configurations.

```
SwitchA#show lldp local config
System configuration:
-----
LLDP enable status: enable (default is disabled)
LLDP enable ports: 1-34
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)

The destination mac address of LLDPDU: (default is 0180.c200.000e)
-----
port1      : destination-mac: 0180.C200.000E
port2      : destination-mac: 0180.C200.000E
port3      : destination-mac: 0180.C200.000E
.....
```

```
SwitchB#show lldp local config
System configuration:
-----
LLDP enable status: enable (default is disabled)
LLDP enable ports: 1-34
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)
```

Use the **show lldp remote** command to show information about the LLDP neighbour.

```

Swi tchA#show ll dp remote
Port  Chassi sl d          PortI d          SysName  MgtAddress  Expi redTi me
-----
port1  000E. 5E02. B010      port 1          Swi tchB  10. 10. 10. 2  106
.....
Swi tchB#show ll dp remote
Port  Chassi sl d          PortI d          SysName  MgtAddress  Expi redTi me
-----
port1  000E. 5E12. F120      port 1          Swi tchA  10. 10. 10. 1  106
.....

```

12.6 Optical module DDM

12.6.1 Introduction

Digital Diagnostic Monitoring (DDM) on the SNR-S212i-8POE supports diagnosing the Small Form-factor Pluggable (SFP) module.

SFP DDM provides a method for monitoring performance. By analyzing monitored data provides by the SFP module, the administrator can predict the lifetime for the SFP module, isolate system faults, as well as verify the compatibility of the SFP module.

The SFP module offers 5 performance parameters:

- Module temperature
- Internal Power Feeding Voltage (PFV)
- Launched bias current
- Launched optical power
- Received optical power

When SFP performance parameters exceed thresholds or when SFP state changes, related Trap is generated.

12.6.2 Preparing for configurations

Scenario

SFP DDM provides a method for monitoring performance parameters of the SFP module. By analyzing monitored data, you can predict the lifetime of the SFP module, isolate system faults, as well as verify the compatibility of the SFP module.

Prerequisite

N/A

12.6.3 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	Enable
Global optical DDM Trap	Disable
Interface optical DDM Trap	Enable
Interface optical DDM password check	Disable

12.6.4 Enabling optical module DDM

Enable optical module DDM for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# transcei ve r ddm enable	Enable SFP DDM globally.
3	NAG(confi g)# i nterface port port-id	Enter physical layer interface configuration mode.
4	NAG(confi g- port)# transcei ver ddm enable	Enable interface optical module DDM. Only when global optical DDM is enabled, the optical module, where interface optical module DDM is enabled, can the SNR-S212i-8POE perform DDM.

12.6.5 Enabling optical module DDM Trap

Enable optical module DDM Trap for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# snmp- server trap transcei ver enable	Enable optical module DDM Trap globally.
3	NAG(confi g)# i nterface port port-id	Enter physical layer interface configuration mode.
4	NAG(confi g- port)# transcei ver trap enable	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 SNR-S212i-8POE send Traps.

12.6.6 Enabling optical DDM module password check

Enable optical module DDM password check for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# confi g	Enter global configuration mode.
2	NAG(confi g)# I nterface port <i>port-id</i>	Enter physical layer interface configuration mode.
3	NAG(confi g- port)# transcei ver check-password enabl e	Enable interface optical module DDM password check.

12.6.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG# show transcei ver	Show global optical module DDM and interface optical module DDM configurations.
2	NAG# show transcei ver ddm port-list <i>port-list</i> [detail]	Show optical module DDM performance parameters.
3	NAG# show transcei ver port- list <i>port-list</i> history [15m 24h]	Show historical information about optical module DDM.
4	NAG# show transcei ver information port-list <i>port-</i> <i>list</i>	Show basic information about the optical module.
5	NAG# show transcei ver threshol d-vi ol ations port- list <i>port-list</i>	Show the information when the optical module parameters exceed the thresholds.

12.7 System log

12.7.1 Introduction

The system log refers that the SNR-S212i-8POE records the system information and debugging information in a log and sends the log to the specified destination. When the SNR-S212i-8POE fails to work, you can check and locate the fault easily.

The system information and some scheduling output will be sent to the system log to deal with. According to the configuration, the system will send the log to various destinations. The destinations that receive the system log are divided into:

- Console: send the log message to the local console through Console interface.

- Host: send the log message to the host.
- Monitor: send the log message to the monitor, such as Telnet terminal.
- File: send the log message to the Flash of the device.
- Buffer: send the log message to the buffer.

According to the severity level, the log is identified by 8 severity levels, as listed in Table 12-2.

Table 12-2 Log levels

Severity	Level	Description
Emergency	0	The system cannot be used.
Alert	1	Need to deal immediately.
Critical	2	Serious status
Error	3	Errored status
Warning	4	Warning status
Notice	5	Normal but important status
Informational	6	Informational event
Debug	7	Debugging information



Note

The severity of output information can be manually set. 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, that is, the severity ranges from emergencies to errors, can be sent.

12.7.2 Preparing for configurations

Scenario

The SNR-S212i-8POE generates critical information, debugging information, or error information of the system to system logs and outputs the system logs to log files or transmit them to the host, Console interface, or monitor for viewing and locating faults.

Prerequisite

N/A

12.7.3 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	Disable, the fixed level is warning (4).
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.

12.7.4 Configuring basic information of system log

Configure basic information of system log for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#l oggi ng on</code>	(Optional) enable system log.
3	<code>NAG(confi g)#l oggi ng time-stamp { debug log } { dateti me none upti me }</code>	<p>(Optional) configure timestamp for system log.</p> <p>The optional parameter debug is used to assign debug level (7) system log timestamp; by default, this system log does not have timestamp</p> <p>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.</p>
4	<code>NAG(confi g)#l oggi ng rate-limi t log-num</code>	(Optional) configure transmitting rate of system log.
5	<code>NAG(confi g)#l oggi ng sequence-number</code>	<p>(Optional) configure sequency of system log.</p> <p>The sequence number only applies to Console, monitor, log file, and log buffer, but not log host and history list.</p>

Step	Command	Description
6	NAG(config)#logging discriminator discriminator-number { facility mnemonics msg-body } { { drops includes } key none }	(Optional) create and configure system log filter. The filter can filter output log from Console, monitor, log file and log buffer.
7	NAG(config)#logging debug [high normal low none]	(Optional) configure sending Debug-level logs.

12.7.5 Configuring system log output

Configure system log output for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#config	Enter global configuration mode.
2	NAG(config)#logging console [log-level alerts critical debugging emergencies errors informational notifications warnings discriminator discriminator-number]	(Optional) output system logs to the Console.
3	NAG(config)#logging host ip-address [log-level alerts critical debugging emergencies errors informational notifications warnings discriminator discriminator-number]	(Optional) output system logs to the log host. Up to 10 log hosts are supported.
	NAG(config)#logging [host ip-address] facility { alert audit auth clock cron daemon ftp kern local 0 local 1 local 2 local 3 local 4 local 5 local 6 local 7 lpr mail news ntp security syslog user uucp }	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 SNR-S212i-8POE.
4	NAG(config)#logging monitor [log-level alerts critical debugging emergencies errors informational notifications warnings discriminator discriminator-number]	(Optional) output system logs to the monitor.

Step	Command	Description
5	NAG(config)#logging file [discriminator discriminator-number]	(Optional) output system logs to the Flash of the SNR-S212i-8POE. Only warning-level logs are available.
6	NAG(config)#logging buffered [log-level alerts critical debugging emergencies errors informational notifications warnings discriminator discriminator-number]	(Optional) output system logs to the buffer.
	NAG(config)#logging buffered size size	(Optional) configure the system log buffer size.
7	NAG(config)#logging history	(Optional) output system logs to the log history list. The level of the output logs is the one of the translated Trap.
	NAG(config)#logging history size size	(Optional) configure the log history list size.
	NAG(config)#logging trap [log-level alerts critical debugging emergencies errors informational notifications warnings discriminator discriminator-number]	(Optional) enable translating specified logs in the history list to Traps. Configurations may fail if the system logs are not output to the log history list.

12.7.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show logging	Show configurations of system log.
2	NAG#show logging buffer	Show information about the system log buffer.
3	NAG#show logging discriminator	Show filter information.
4	NAG#show logging file	Show contents of system log.
5	NAG#show logging history	Show information about the system log history list.

12.7.7 Maintenance

Maintain the SNR-S212i-8POE as below.

No.	Command	Description
1	NAG(confi g)#cl ear l oggi ng bu ffer	Clear log information in the buffer.
2	NAG(confi g)#cl ear l oggi ng statl stl cs	Clear log statistics.

12.7.8 Example for outputting system logs to log host

Networking requirements

As shown in Figure 12-13, configure system log to output system logs of the switch to the log host, facilitating view logs at any time.

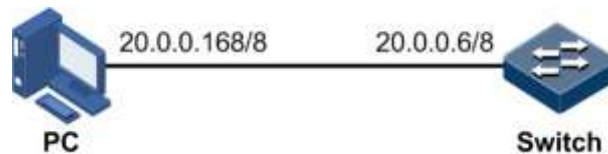


Figure 12-13 Outputting system logs to log hosts

Configuration steps

Step 1 Configure the IP address of the switch.

```
NAG#confi g
NAG(confi g)#i nterface i p 0
NAG(confi g-i p)#i p address 20. 0. 0. 6 255. 0. 0. 0 1
NAG(confi g-i p)#exi t
```

Step 2 Output system logs to the log host.

```
NAG(confi g)#l oggi ng on
NAG(confi g)#l oggi ng ti me-stamp l og dateti me
NAG(confi g)#l oggi ng rate-l i mi t 2
NAG(confi g)#l oggi ng host 20. 0. 0. 168 warni ngs
```

Checking results

Use the **show logging** command to show configurations of system log.

```

NAG#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    disable  informational (6)    0           0             0
console   enable   informational (6)    203         4             0
trap      disable  warnings(4)         0           0             0
file      disable  warnings(4)         0           0             0
monitor   disable  informational (6)    0           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    1    0    0

```

12.8 Alarm management

12.8.1 Introduction

Alarm means when a fault is generated on the SNR-S212i-8POE 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 network management system through SNMP. The information sent to the NMS is called Trap information.

Alarm classification

There are three kinds of alarm information according to properties of an alarm:

- **Fault alarm:** refers to alarms for some hardware fault or some abnormal important functions, such as port Down alarm;
- **Recovery alarm:** refers to alarms that are generated when device failure or abnormal function returns to normal, such as port Up alarm;

- Event alarm: refers 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.

The alarm information can be divided into five types according to functions:

- Communication alarm: refers 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: refers to alarms caused by service quality degradation, including congestion, performance decline, high resource utilization rate, and the bandwidth reducing.
- Processing errored alarm: refers to alarms caused by software or processing errors, including software errors, memory overflow, version mismatching, and the abnormal program aborts.
- Environmental alarm: refers to alarms caused by equipment location-related problems, including the environment temperature, humidity, ventilation and other abnormal working conditions.
- Device alarm: refers to alarms caused by failure of physical resources, including power, fan, processor, clock, input/output ports 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 SNR-S212i-8POE, including CLI terminal and NMS.

Log output of alarm information starts with the symbol "#", and the output format is:

```
#Index TimeStamp HostName ModuleName/Severity/name: Arise From Description
```

Table 12-3 lists alarm fields.

Table 12-3 Alarm fields

Field	Description
Index	Alarm index
TimeStamp	Time when an alarm is generated
HostName	Name of the host where the alarm occurs

Field	Description
ModuleName	Name for a module where alarms are generated
Severity	Alarm level
Name	Alarm name
Arise From Description	Descriptions about an alarm

Alarm levels

The alarm level is used to identify the severity degree of an alarm. The level is defined in Table 12-4.

Table 12-4 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 inhibition

The SNR-S212i-8POE only records root-cause alarms but incidental alarms when enabling alarm inhibition. For example, the generation of alarm A will inevitably produce alarm B, then alarm B is inhibited and does not appear in alarm buffer and record the log information

when enabling alarm inhibition. By enabling alarm inhibition, the SNR-S212i-8POE can effectively reduce the number of alarms.

All root-cause alarms and incidental alarms will be recorded on the SNR-S212i-8POE when alarm inhibition 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 set 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, or 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, etc;
- 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 SNR-S212i-8POE.

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. Not report if there is alarm information.

Currently, the device is only in support of reverse mode configuration of the interface. There are three reverse modes to be set; the specific definitions are as below:

- Non-reverse mode

Device alarm is reported normally.

- Manual reverse mode

Set the alarm reverse mode of an interface as manual reverse mode, then no matter what the current alarm state is, the reported alarm state of the interface will be changed opposite to the actual alarm state immediately, that is to say, not report when there are alarms, report when there are not alarms actually. The interface will maintain the opposite alarm state regardless of the alarm state changes before the alarm reverse state being restored to non-reverse mode.

- Auto-reverse mode

Set the alarm reverse mode as auto-reverse mode. If the interface has not actual reverse alarm currently, the setting will return fail; if the interface has actual reverse alarm, the setting 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 state of interface

alarm reverse will ends automatically and changes to non-reverse alarm mode so that the alarm state can be reported normally in next alarm.

- Alarm delay

Alarm delay refers that the SNR-S212i-8POE will record alarms and report them to NMS after a delay but not immediately when alarms generate. Delay for recording and reporting alarms are identical.

By default, the device alarm is reported once generating (0s), which is instant reporting; clear alarm once it ends (0s), which is instant clearing.

- Alarm storage mode

Alarm storage mode refers to how to record new generated alarms when the alarm buffer is full. There are two ways:

- **stop**: stop mode, when the alarm buffer is full, new generated alarms will be discarded without recording.
- **loop**: wrapping mode, when the alarm buffer is full, the new generated alarms will replace old alarm information and take rolling records.

Use configured storage mode to deal with new generated alarm information when the alarm information 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 SNR-S212i-8POE. If the SNR-S212i-8POE is configured with NView NNM system, the administrator can monitor alarms on the NView NNM system.

12.8.2 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 network management system, alarm information can be reported directly to the network management system, providing possible alarm causes and treatment recommendations to help users deal with fault.

Alarm management makes it easy for the user to take alarm suppression, alarm auto-reporting, alarm monitoring, alarm reverse, alarm delay, alarm memory mode, alarm clear and alarm view directly on the device.

Prerequisite

N/A

12.8.3 Default configurations of alarm management

Default configurations of alarm management are as below.

Function	Default value
Alarm inhibition	Enable
Alarm monitoring	Enable
Alarm auto-reporting	Enable
Alarm reverse mode	Auto-reverse
Alarm delay	0s
Alarm storage mode	stop
Output alarms to system logs	Disable

12.8.4 Configuring basic functions of alarm management

Configure basic information of alarm management for the SNR-S212i-8POE as below.

All following steps are optional and no sequence between them.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#al arm i nhi bl t enabl e</code>	Enable alarm inhibition.
3	<code>NAG(confi g)#al arm auto-report { module_name [group_name] port-list port-list [module_name [group_name]] } enabl e</code>	Enable alarm auto-reporting.
4	<code>NAG(confi g)#al arm moni tor { module_name port-list port-list [portlib portbackup hw_moni tor] } enabl e</code>	Enable alarm monitoring.
5	<code>NAG(confi g)#al arm i nverse port-list port-list { auto manual none }</code>	Configure alarm reverse modes.
6	<code>NAG(confi g)#al arm { acti ve clear } del ay del ay</code>	Configure alarm delay.
7	<code>NAG(confi g)#al arm acti ve storage- mode { loop stop }</code>	Configure alarm storage modes.
8	<code>NAG(confi g)#al arm cl ear i ndex i ndex</code>	Clear specified current alarms.
	<code>NAG(confi g)#al arm cl ear modul e_name</code>	Clear current alarms on specified modules.
	<code>NAG(confi g)#al arm cl ear port-list port-list</code>	Clear current alarms on specified interfaces.

Step	Command	Description
9	NAG(config)#alarm syslog enable	Output alarms to system logs.
10	NAG(config)#exit NAG#show alarm active [module_name severity severity]	Show current alarms.
	NAG#show alarm cleared [module_name severity severity]	Show historical alarms.



Note

You can enable/disable alarm monitoring, alarm auto-reporting, alarm clearing on modules that support alarm management.

12.8.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show alarm management [module_name]	Show parameters of current alarms, including status of alarm inhibition, alarm reverse mode, alarm delay, and alarm storage mode, maximum alarm buffer size, and alarm log size.
2	NAG#show alarm log	Show alarm statistics in the system log.
3	NAG#show alarm management statistics	Show alarm management module statistics.

12.9 Hardware environment monitoring

12.9.1 Introduction

Hardware environment monitoring mainly refers to monitor the running environment of the SNR-S212i-8POE. The monitoring alarm events include:

- Power supply state alarm
- Overtemperature 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 network management center;

- Output to the relay fault indication LED.

You can take appropriate measures to prevent failure when alarm events happen.

Alarm events

- Power supply monitoring alarms

Power supply state change refers that unplugged power supply is plugged into the device and vice versa. The SNR-S212i-8POE supports dual power supplies. Therefore, power supply state change alarms are divided into the single power supply state change alarm and device dying gasp alarm.

- Single power supply state change alarm: notify uses that power supply 1/power supply 2 changes. The SNR-S212i-8POE 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 SNR-S212i-8POE supports recording the hardware environment monitoring alarm table, Trap, Syslog, and relay outputting modes.

- 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 SNR-S212i-8POE 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 SNR-S212i-8POE 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.

Both the two alarm events support recording the hardware environment alarm table, Trap, Syslog and relay outputting modes.

- Flash monitoring alarm

The SNR-S212i-8POE supports monitoring the Flash. When the Flash is over written or the times of writing exceed the upper limit, the SNR-S212i-8POE supports generate a Trap, reports the event to the NMS, and logs the event.

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 automatically recorded in the hardware environment monitoring current alarm table and hardware environment monitoring historical alarm table without manual configurations.

- Trap output

Alarms are output to network management center in Trap mode.

Trap output has global switch and all monitored alarm events still have their own Trap alarm output switches. When enabling the global switch and monitored alarm events switches simultaneously, the alarm will generate Trap output.

Table 12-5 describes Trap information.

Table 12-5 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) • 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 12-6 describes Syslog information.

Table 12-6 Syslog information

Field	Description
Facility	The module name generating alarm, the hardware environment monitoring module is fixed as alarm.
Severity	Level, see Table 12-2 for the same system log defined levels.
Mnemonics	Alarm event type, see Table 12-5 for the detailed type description.

Field	Description
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 indicate 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 SNR-S212i-8POE, 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.

12.9.2 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. When you need 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 network management center IP address for the device.
- In relay output mode: relay alarm output switch is enabled for every alarm.

12.9.3 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.

Function	Default value
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	100°C
Low temperature alarm threshold	-40°C

12.9.4 Enabling global hardware environment monitoring

Enable global hardware environment monitoring for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#l oggi ng al arm	(Optional) enable global hardware environment monitoring alarm Syslog output.
3	NAG(confi g)#snmp- server al arm-trap enabl e	(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.

12.9.5 Configuring power supply monitoring alarm

Configure power supply monitoring alarm for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#al arm power-suppl y { notl fies syst og rel ay }	Enable power supply monitoring alarm output and configure power supply monitoring alarm output modes.

12.9.6 Configuring temperature monitoring alarm

Configure temperature monitoring alarm for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#al arm temperature { hi gh <i>hi gh-val ue</i> lo w <i>lo w-val ue</i> noti fi es sysl og rel ay }	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).


12.9.7 Configuring interface status monitoring alarm

Configure interface status monitoring for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#al arm port { li nk-down li nk-faul t} { noti fi es rel ay sysl og } port-li st <i>port-li st</i>	Enable interface status alarm output and configure interface state alarm output modes.

12.9.8 Clearing all hardware environment monitoring alarms manually

Clear all hardware environment monitoring alarms manually for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG#confi g	Enter global configuration mode.
2	NAG(confi g)#c lear al arm	Clear alarms manually. <div style="margin-top: 10px;">  <p>Note</p> <p>Use this command to clear all alarms in current alarm list and generate an all-alarm alarm in history alarm list.</p> <p>If enabling global sending Trap, the all-alarm alarm will be output in Trap mode; if enabling global Syslog, the all-alarm alarm will be output in Syslog mode.</p> </div>

12.9.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show alarm	Show global hardware environment monitoring alarm configurations.
2	NAG#show alarm port-list <i>port-list</i>	Show interface state alarms.
3	NAG#show alarm current	Show current alarms of hardware environment monitoring.
4	NAG#show alarm history	Show historic alarms of hardware environment monitoring.
5	NAG#show environment [power temperature]	Show current environment information.

12.10 CPU monitoring

12.10.1 Introduction

The SNR-S212i-8POE supports CPU monitoring. It can monitor state, CPU utilization, and stack usage in real time. It helps to locate faults.

CPU monitoring can provide the following functions:

- Show CPU utilization

It can be used to show CPU unitization in each period (5s, 1 minute, 10 minutes, and 2 hours). Total CPU unitization in each period can be shown dynamically or statically.

It can be used to view the operating status of all tasks and the detailed running status of assigned tasks.

It can be used to view history CPU utilization in each period.

It can be used to view death task information.

- CPU unitization threshold alarm

If system CPU utilization changes below lower threshold or above upper threshold in a specified sampling period, an alarm will be generated and a Trap message will be sent. The Trap message provides serial number and CPU utilization of 5 tasks whose CPU unitization is the highest in the latest period (5s, 1 minute, 10 minutes).

12.10.2 Preparing for configurations

Scenario

CPU monitoring can monitor state, CPU utilization, and stack usage in real time, provide CPU utilization threshold alarm, detect and eliminate hidden dangers, or help the administrator with fault location.

Prerequisite

When the CPU monitoring alarm needs to be output in Trap mode, configure Trap output target host address, which is IP address of NView NNM system.

12.10.3 Default configurations of CPU monitoring

Default configurations of CPU monitoring are as below.

Function	Default value
CPU utilization rate alarm Trap output	Disable
Upper threshold of CPU utilization alarm	99%
Lower threshold of CPU utilization alarm	1%
Sampling period of CPU utilization	60s

12.10.4 Showing CPU monitoring information

Show CPU monitoring information for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#show cpu-utilization [dynamic history { 10min 1min 2hour 5sec }]</code>	Show CPU utilization.
2	<code>NAG#show process [dead sorted { normal -priority process-name } taskname]</code>	Show states of all tasks.
3	<code>NAG#show process cpu [sorted [10min 1min 5sec invoked]]</code>	Show CPU utilization of all tasks.

12.10.5 Configuring CPU monitoring alarm

Configure CPU monitoring alarm for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.

Step	Command	Description
2	NAG(config)#snmp-server trap enable cpu-threshold	Enable CPU threshold alarm Trap.
3	NAG(config)#cpu rising- threshold threshold-value	(Optional) configure CPU alarm rising threshold.
4	NAG(config)#cpu falling- threshold value	(Optional) configure CPU alarm falling threshold.
5	NAG(config)#cpu interval value	(Optional) configure the period for CPU alarms.

12.10.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG#show cpu- utilization	Show CPU utilization and related configurations.

12.11 CPU protection

12.11.1 Introduction

When the SNR-S212i-8POE works in a complex network, it may be attacked by multiple packets, such as ARP packet, BPDU packet, and ICMP packet. If the SNR-S212i-8POE receives multiple attack packets in a short period, the CPU will run in a fully-loaded state. This may cause that some functions of the device work improperly.

CPU protection is used to defend attack packets. It monitors Rx and Tx statistics of some packet in real time. In a period, if the number of some received packet exceeds the threshold on an interface, the interface will discard these packets without transmitting them to the CPU to protect CPU. However, in a period, if the number of some received packet does not reach the configured threshold on an interface, the interface does not discard received packets.

At present, CPU protection is used to prevent attacks from ARP packet, BPDU packets, and ICMP packets.

12.11.2 Preparing for configurations

Scenario

In the complex network, the SNR-S212i-8POE may be attacked by multiple packets. By being enabled with CPU protection, the device can effectively prevent attack from these packets, monitoring Tx/Rx packet statistics in real time, and protect CPU.

Prerequisite

N/A

12.11.3 Default configurations of CPU protection

Default configurations of CPU protection are as below.

Function	Default value
CPU protection	Disable
Sample interval for packets	<ul style="list-style-type: none"> • BPDU packet: 1s • ARP packet: 5s • ICMP packet: 5s
Threshold for discarding packets	<ul style="list-style-type: none"> • BPDU packet: 200 • ARP packet: 200 • ICMP packet: 300
Threshold for normally receiving packets	<ul style="list-style-type: none"> • BPDU packet: 50 • ARP packet: 40 • ICMP packet: 100

12.11.4 Configuring CPU protection on interfaces

**Caution**

For a packet, the threshold for normally receiving the packet should be smaller than the one for discarding the packet.

Configure CPU protection on interfaces for the SNR-S212i-8POE as below.

Step	Command	Description
1	<code>NAG#confi g</code>	Enter global configuration mode.
2	<code>NAG(confi g)#flood-protect { all arp bpdu icmp } enable port-list port-list</code>	Enable CPU protection for some packet on a specified interface.
3	<code>NAG(confi g)#flood-protect { all arp bpdu icmp } interval period</code>	(Optional) configure the sampling interval for some packets. The unit is set to second.
4	<code>NAG(confi g)#flood-protect { all arp bpdu icmp } high threshold</code>	(Optional) configure the threshold for discarding some packets in the sampling interval.
5	<code>NAG(confi g)#flood-protect { all arp bpdu icmp } low threshold</code>	(Optional) configure the threshold for normally receiving some packets in the sampling interval.

12.11.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	NAG# <code>show flood-protect</code>	Show CPU protection configurations.
2	NAG# <code>show flood-protect port-list port-list</code>	Show CPU protection state on a specified interface.

12.11.6 Example for configuring CPU protection

Networking requirements

As shown in Figure 12-14, to protect uplink interfaces from ARP attacks from the user network, you need to enable CPU protection for ARP packets on these interfaces. Detailed requirements are as below:

- Period for sampling ARP packets: 10s
- Threshold for discarding ARP packets: 500
- Threshold for normally receiving ARP packets: 50

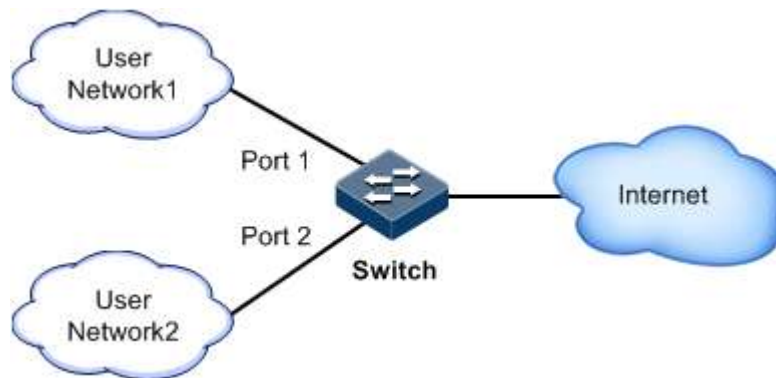


Figure 12-14 Configuring CPU protection

Configuration steps

Step 1 Enable CPU protection for ARP packet on Port 1 and Port 2.

```

NAG#confi g
NAG(confi g)#flood-protect arp enable port-list 1-2
  
```

Step 2 Configure the sampling period, threshold for discarding packets, and threshold for normally receiving packets for ARP packets.

```

NAG(confi g)#flood-protect arp interval 10
NAG(confi g)#flood-protect arp high 500
NAG(confi g)#flood-protect arp low 50

```

Checking results

Use the **show flood-protect [port-list port-list]** command to show CPU protection on Port 1.

```

NAG#show flood-protect port-list 1
port1:
Packet Type      isEnabled      Attacked Status      Attacked Count
-----
bpdud            disabled      not-attacking        1
arp              enabled       not-attacking        0
icmp             disabled      not-attacking        2

```

12.12 Ping

12.12.1 Introduction

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 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 the route between source and destination addresses are unreachable.

Figure 12-15 shows the principle of Ping.

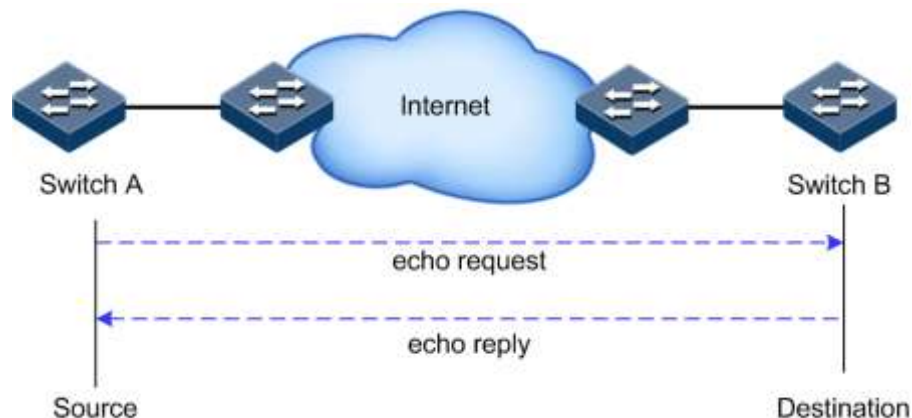


Figure 12-15 Principle of Ping

12.12.2 Configuring Ping

Configure Ping for the SNR-S212i-8POE as below.

Step	Command	Description
1	NAG# <code>ping ip-address</code> [<code>count count</code>] [<code>size size</code>] [<code>wai ttl me period</code>]	(Optional) test the connectivity of the IPv4 network by the ping command.



Note

The SNR-S212i-8POE cannot perform other operations in the process of Ping. It can perform other operations only when Ping is finished or break off Ping by pressing **Ctrl+C**.

12.13 Traceroute

12.13.1 Introduction

Just as Ping, Traceroute is a commonly used maintenance method in network management. **Traceroute** is often used to test the network nodes of packets from sender to destination, detect whether the network connection is reachable, and analyze network fault

The following shows how Traceroute works:

- First, send a piece of TTL1 sniffer packet (where the UDP port number of the packet is unavailable to any application programs in destination side).
- TTL deducts 1 when reaching the first hop. Because the TTL value is 0, in the first hop the device returns an ICMP timeout packet, indicating that this packet cannot be sent.
- The sending host adds 1 to TTL and resends this packet.
- Because the TTL value is reduced to 0 in the second hop, the device will return an ICMP timeout packet, indicating that this packet cannot be sent.

The above steps continue until the packet reaches the destination host, which will not return ICMP timeout packets. Because the port number of destination host is not be used, the destination host will send the port unreachable packet and finish the test. Thus, the sending host can record the source address of each ICMP TTL timeout packet and analyze the path to the destination according to the response packet. The Traceroute function principles are shown in Figure 12-16.

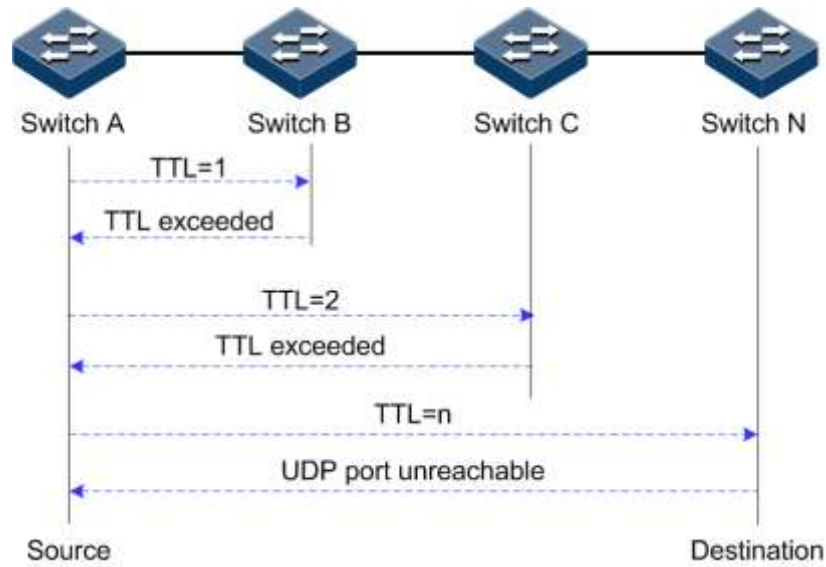


Figure 12-16 Principles of Traceroute

12.13.2 Configuring Traceroute

Before using Traceroute, you should configure the IP address and default gateway of the SNR-S212i-8POE.

Configure Traceroute for the SNR-S212i-8POE as below.

Step	Command	Description
1	<pre>NAG#traceroute ip-address [firstttl first-ttl] [maxttl max-ttl] [port port-id] [waittime second] [count times]</pre>	(Optional) test the connectivity of the IPv4 network and view nodes passed by the packet by the traceroute command.

13 Appendix

This chapter describes terms and abbreviations involved in this guide, including the following sections:

- Terms
- Acronyms and abbreviations

13.1 Terms

A

Access
Control List
(ACL)

A series of orderable rules composed by permit | deny sentences. The device decides the packets to be received/discarded based on these rules.

Automatic
Laser
Shutdown
(ALS)

A technology that is used for automatically turning the output power of laser and optical amplifier off to avoid personal injury.

Auto-
negotiation

The auto negotiation procedure is: the port at one site adapts its bit rate and duplex mode to the highest level that the opposite site device both support according to the bit rate and duplex mode adopted by the remote site device, that is, the connected devices on both site adopt the fastest transmission mode they both support after the auto negotiation process.

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, APS can make the working channel switched to the protection channel quickly to recover communication in a very short period.

C

Challenge-
Handshake
Authentication
Protocol
(CHAP)

A protocol of PPP. It is a 3-times handshake authentication protocol which is used to transmit the user name only on the network.

D

- Dynamic ARP Inspection (DAI)** A security feature that can be used to verify the ARP datagram on the network. With DIA, the administrator can intercept, record, and discard ARP packets with invalid MAC address/IP address to prevent common ARP attacks.
- Dynamic Host Configuration Protocol (DHCP)** A technology used for assigning IP address dynamically. It can automatically assign IP addresses for all clients in the network to reduce workload of the administrator. In addition, it can realize centralized management of IP addresses.

E

- Ear hanging** A component installed on both sides of the chassis, used for install the chassis to the rack.
- Ethernet in the First Mile (EFM)** Complied with IEEE 802.3ah protocol, Ethernet in the First Mile (EFM) is a link-level Ethernet OAM technology. It provides the link connectivity detection function, link fault monitor function, and remote fault notification function, etc for a link between two directly connected devices. EFM is used for Ethernet link on edges of the network accessed by users.
- Ethernet Ring Protection Switching (ERPS)** An APS (Automatic Protection Switching) protocol based on ITU-T G.8032 Recommendation to provide backup link protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer.

F

- Failover** Provide a port association solution, extending link backup range. Transport fault of upper layer device quickly to downstream device by monitoring upstream link and synchronize downstream link, then trigger switching between master and standby device and avoid traffic loss.
- Full-duplex** Communication link can transmit and receive data at the same time from both directions.

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 service transmitted in multiple high-speed logistic transmission channels.

H

- Half-duplex** Refers to two-way electronic communication that takes place unidirectionally at a time. Communication between people is half-duplex when one person listens while the other speaks.

I

Institute of Electrical and Electronics Engineers (IEEE)	An international Institute of electrical and Electronics Engineers. It is one of the largest technical organizations. It has more than 360,000 members in 175 countries (up to 2005).
Internet Assigned Numbers Authority (IANA)	It is used to assign and maintain the unique code and value in Internet technology standard (protocol), such as the IP address or multicast address.
Internet Engineering Task Force (IETF)	It is established in 1985. It is the most authoritative technology and standard organization, which develops and formulate specifications related to the Internet.
L	
Label	A group of signals that are used to identify the cable, chassis, or warning.
Link aggregation	A computer networking term which describes using multiple network cables/ports in parallel to increase the link speed beyond the limits of any one single cable or port, and to increase the redundancy for higher availability.
Link Aggregation Control Protocol (LACP)	A protocol used for realizing link dynamic aggregation. LACP communicates with the peer by exchanging LACPDU.
M	
Multi-mode Fiber	Multi-mode can be transmitted in one fiber.
N	
Network Time Protocol (NTP)	A time synchronization protocol defined by RFC1305. It is used to synchronize time between distributed timer server and clients. NTP is used to perform clock synchronization on all devices in the network that support clock. Therefore, devices can provide different applications based on some time. In addition, NTP can ensure very high accuracy (about 10ms).
O	
Open Shortest Path First (OSPF)	An internal gateway dynamic routing protocol, which is used to decide the route in an Autonomous System (AS).

Optical Distribution 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 used for fiber splicing, optical connector installation, fiber adjustment, additional pigtail storage, and fiber protection.

P

Password Authentication Protocol (PAP) A password authentication protocol of Point to Point Protocol. It is a twice handshake protocol used for transmitting the user name and password in a plain text.

Point-to-point Protocol over Ethernet (PPPoE) With PPPoE, the remote 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.

Protection ground wire Cable to connect device to ground, usually it is co-axial cable in yellow and green

Q

QinQ QinQ is (also called Stacked VLAN or Double VLAN) extended from 802.1Q, defined by IEEE 802.1ad recommendation. Basic QinQ is a simple Layer 2 VPN tunnel technology, encapsulating outer VLAN Tag for client private packets at carrier access end, the packets take double VLAN Tag passing through trunk network (public network). In public network, packets only transmit according to outer VLAN Tag, the private VLAN Tag are transmitted as data in packets.

Quality of Service (QoS) A commonly-used performance indicator of a telecommunication system or channel. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio. It functions to measure the quality of the transmission system and the effectiveness of the services, as well as the capability of a service provider to meet the demands of users.

R

Rapid Spanning Tree Protocol (RSTP) RSTP is an extension of Spanning Tree Protocol, which realizes quick convergency of network topology.

Remote Authentication Dial In User Service (RADIUS)	A protocol used to authenticate and account users on the network.
S	
Simple Network Management Protocol (SNMP)	A network management protocol defined by Internet Engineering Task Force (IETF) used to manage devices in the Internet. SNMP can make the network management system to remotely manage all network devices that support SNMP, including monitoring network status, modifying network device configurations, and receiving network event alarms. At present, SNMP is the most widely-used network management protocol in the TCP/IP network.
Simple Network Time Protocol (SNTP)	SNTP is used for synchronizing time of devices on the network.
Single-mode fiber	Only a single mode can be transmitted in one fiber.
Spanning Tree Protocol (STP)	STP can be used to eliminate network loops and back up link data. It blocks loops in logic to prevent broadcast storms. When the unblocked link fails, the blocked link is re-activated to act as the protection link.
V	
Virtual Local Area Network (VLAN)	VLAN is a protocol proposed to solve broadcast and security issues for Ethernet. It divides devices in a LAN into different segment logically rather than physically, thus implementing virtual work groups which are based on Layer 2 isolation and do not affect each other.
VLAN Mapping	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. During packets are sent to the peer private network from the Carrier 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.

13.2 Acronyms and abbreviations

A	
AAA	Authentication, Authorization and Accounting
ABR	Area Border Router
AC	Alternating Current

ACL	Access Control List
ANSI	American National Standards Institute
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
AS	Autonomous System
ASCII	American Standard Code for Information Interchange
ASE	Autonomous System External
ATM	Asynchronous Transfer Mode
AWG	American Wire Gauge
B	
BC	Boundary Clock
BDR	Backup Designated Router
BITS	Building Integrated Timing Supply System
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BTS	Base Transceiver Station
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
RCMP	Cluster Management Protocol
RED	Random Early Detection
RH	Relative Humidity
RIP	Routing Information Protocol
RMON	Remote Network Monitoring
RNDP	NAG Neighbor Discover Protocol
NOS	Network Operating System
RPL	Ring Protection Link
RRPS	Redundant Ring Protection Switching
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource Reservation Protocol
RTDP	NAG 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

