

RT Series Layer 3 Industrial Switch

Command Line Interface

Manual

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Contents

Command Line Interface	1
Manual	1
1. Introduction to the CLI command line	9
1.1 Accessing the switch using the CLI	9
1.1.1 Users access CLI through Console port	9
1.1.2 Users access CLI through TELNET	10
1.2 Introduction to the CLI	11
1.2.1 The role of CLI model	11
1.2.2 Identification of CLI mode	11
1.2.3 Classification of CLI patterns	12
1.3 Introduction to command syntax	13
1.3.1 Command composition	13
1.3.2 Parameter type	13
1.3.3 Command syntax rules	14
1.3.4 Command abbreviation	15
1.3.5 Grammar help	15
1.3.6 Command line error message	15
1.4 Command line shortcuts	16
1.4.1 Line edit shortcut key	16
1.4.2 Display command shortcut key	16
1.5 Command History	17
2.0 System management configuration	18
2.1 System security configuration	18
2.1.1 Multi-user management control	18
2.1.2 TACACS+ authentication authorisation	19
2.1.3 Anonymous user password control	20
2.1.4 Enable password control	22
2.1.5 TELNET service control	22
2.1.6 SNMP service control	23
2.1.7 HTTP service control	23
2.1.8 SSH service control	24
2.2 System maintenance and debugging	24
2.2.1 Configure the host name of the system	24
2.2.2 Configuring the system clock	24
2.2.3 Configure terminal timeout attributes	25
2.2.4 System reset	25
2.2.5 View system information	25
2.2.6 Network connectivity debugging	26
2.2.7 Detecting line distance	26
2.2.8 Traceroute debugging	26
2.2.9 Telnet client	27
2.2.10 UDL D configuration	27
2.3 Configuration file management	28
2.3.1 View configuration information	28
2.3.2 Save configuration	29
2.3.3 Delete configuration file	29
2.3.4 Download configuration files	29
2.4 Software version upgrade	31
2.4.1 Software version upgrade commands	31
2.4.2 Software upgrade process	32
3 PORT CONFIGURATION	34
3.1 Common configuration for ports	34
3.1.1 Port rate configuration	34

3.1.2	Display port information.....	34
3.2	Configuring Port Mirroring.....	35
3.2.1	Configuring the Port to listen to (MIRROR) and listening on a port.....	35
3.2.2	Display the configuration of MIRROR.....	35
3.3	Configuring STORM-CONTROL.....	36
3.3.1	Default configuration.....	36
3.3.2	Broadcast suppression configuration.....	36
3.3.3	Multicast suppression configuration.....	36
3.3.4	DLF suppression configuration.....	36
3.3.5	Inhibition rate configuration.....	37
3.3.6	Display STORM-CONTROL configuration.....	37
3.4	Configuring STORM-CONSTRAIN.....	37
3.5	Configuring FLOW-CONTROL.....	39
3.5.1.	Default configuration.....	39
3.5.2.	Set port receive and send side flow control.....	39
3.5.3.	Closed port flow control.....	39
3.5.4	Display flow control information.....	39
3.6	Configuring port bandwidth.....	40
3.6.1	Default configuration.....	40
3.6.2	Set port send or receive bandwidth control.....	40
3.6.3	Cancellation of port transmit or receive bandwidth control.....	40
3.6.4	Bandwidth control of display port configuration.....	40
3.7	Configuring Trunks.....	40
3.7.1	LACP protocol configuration.....	41
3.7.2	Configuration of a TRUNK group.....	42
3.7.3	TRUNK group member port configuration.....	42
3.7.4	TRUNK load balancing policy configuration.....	43
3.7.5	Display of TRUNK.....	43
3.8	Configure super large frame.....	43
3.8.1	Oversize introduction.....	43
3.8.2	Oversize configuration.....	43
3.9	Configuring redundant ports.....	44
3.9.1	Configuration of redundant ports.....	44
3.9.2	Display of redundant ports.....	44
3.10	Configuring LLDP.....	45
3.10.1	LLDP configuration.....	45
3.10.2	LLDP display.....	46
4	Port based MAC security.....	47
4.1	Brief introduction.....	47
4.2	MAC binding configuration.....	47
4.3	MAC filter configuration.....	48
4.4	Port learning constraint configuration.....	49
5.	Port IP and MAC binding.....	50
5.1	Brief introduction.....	50
5.2	IP and MAC binding configurations.....	50
5.3	Configuration example.....	51
5.4	Configuration misarrangement.....	52
6.	VLAN CONFIGURATION.....	53
6.1	VLAN introduction.....	53
6.1.1	The benefits of VLAN.....	53
6.1.2	VLAN ID.....	54
6.1.3	VLAN port member type.....	55
6.1.4	Default VLAN of port.....	55
6.1.5	Port VLAN mode.....	55
6.1.6	VLAN relay.....	55

6.1.7	Data flow is forwarded in VLAN.....	56
6.2	VLAN configuration	57
6.2.1	Creating and deleting VLAN	57
6.2.2	Configuring port VLAN mode.....	57
6.2.3	VLAN configuration of ACCESS mode.....	58
6.2.4	VLAN configuration of TRUNK mode	59
6.2.5	HYBRID mode VLAN configuration	59
6.2.6	View VLAN information	60
6.3	VLAN configuration example	61
6.3.1	VLAN based on PORT	61
6.3.2	VLAN based on 802.1Q.....	62
6.4	MAC, IP subnet, protocol VLAN	63
6.5	Voice VLAN	64
6.6	VLAN mapping	65
6.7	QinQ.....	66
7.	QoS CONFIGURATION.....	68
7.1	QoS Introduction.....	68
7.1.1	QoS based on COS.....	69
7.1.2	QoS based on DSCP	69
7.1.3	Policy based QOS	69
7.2	QoS Configuration	70
7.2.1	Default configuration for QoS	70
7.2.2	Configuration scheduling mode.....	70
7.2.3	Configuring queue weights	71
7.2.4	Configure the mapping relationship between DSCP and QoSProfile.....	71
7.2.5	Configuring port QoS	71
7.2.6	Configuring the port user priority (COS value)	73
7.3	Example of basic QoS configuration	73
7.4	Policy QoS configuration example	73
8.	MSTP CONFIGURATION	75
8.1	MSTP introduction.....	75
8.1.1	Overview.....	75
8.1.2	Multiple Spanning Tree Domains	75
8.1.3	IST, CIST, and CST	76
8.1.4	Intra Domain Operation	76
8.1.5	Inter-domain operation.....	77
8.1.6	Hop count.....	77
8.1.7	Boundary port	77
8.1.8	MSTP 802.1d and STP interoperability	78
8.1.9	Port role.....	78
8.1.10	A brief introduction to 802.1D spanning tree.....	79
8.2	MSTP configuration.....	81
8.2.1	Default configuration	81
8.2.2	General configuration	81
8.2.3	Domain configuration	83
8.2.4	Instance configuration.....	83
8.2.5	port configuration.....	83
8.2.6	PORTFAST related configuration.....	85
8.2.7	Root Guard configuration	86
8.3	MSTP configuration example	87
9.	EAPS configuration	88
9.1	EAPS brief introduction.....	88
9.2	Basic concepts of EAPS.....	88
9.3	EAPS protocol introduction.....	88
9.3.1.	Link-Down alarm.....	89

9.3.2.	Loop inspection.....	89
9.3.3.	Ring restoration.....	89
9.3.4.	Extreme compatible with EAPS	90
9.3.5.	Multi EAPS Domain	90
9.4	EAPS configuration	90
9.5	Restrictive conditions.....	90
9.6	A brief introduction to the EAPS command	90
9.6.1	EAPS configuration command.....	91
9.7	Single - loop configuration example	92
9.8	Example of cross ring data forwarding configuration.....	95
10	ERPS configuration	98
10.1.	ERPS overview	98
10.2.	Introduction of ERPS Technology	98
10.2.1	ERPS ring	98
10.2.2	ERPS node	98
10.2.3	Link and channel.....	99
10.2.4	ERPS VLAN	99
10.3.	ERPS Working principle	99
10.3.1.	Normal state	99
10.3.2.	Link failures	100
10.3.3.	Link recovery	100
10.4.	Technical features of ERPS.....	101
10.4.1.	ERPS load balancing.....	101
10.4.2.	Good safety	101
10.4.3.	Multi-loop intersecting is supported	102
10.5.	ERPS protocol commands	102
10.6.	Typical use of ERPS	104
10.6.1.	Example of single ring.....	104
10.6.2.	Multi ring example.....	106
10.6.3.	Multi instance load balancing example.....	111
11.	AAA configuration	117
11.1	802.1x introduction	117
11.1.1	802.1x device composition	118
11.1.2	Brief introduction of protocol package	119
11.1.3	Protocol flow interaction.....	120
11.1.4	802.1x port state.....	121
11.2	RADIUS introduction	122
11.2.1	Brief introduction of protocol package	122
11.2.2	Protocol flow interaction.....	123
11.2.3	User authentication method	124
11.3	Configuring 802.1x	125
11.3.1	802.1x default configuration	125
11.3.2	Start and close 802.1x	126
11.3.3	Configuring 802.1x port status.....	126
11.3.4	Configuring 802.1x port authentication	126
11.3.5	Configuring 802.1x port guest VLAN	126
11.3.6	Configuration re authentication mechanism	127
11.3.7	Maximum number of configuration port access host.....	127
11.3.8	Configure interval times and resend times	127
11.3.9	Configuration port is the transport port.....	128
11.3.10	Configuring the 802.1x client version number	128
11.3.11	Configure whether to check the client version number.....	128
11.3.12	Configuration authentication method.....	128
11.3.13	Configure whether to check the client's timing packet	128
11.3.14	Display 802.1x information	129

11.4	Configuration RADIUS	129
11.4.1	RADIUS Default configuration	129
11.4.2	Configuring the IP address of the authentication server	129
11.4.3	Configuring shared keys	129
11.4.4	Start and close billing	130
11.4.5	Configuring RADIUS ports and attribute information	130
11.4.6	Configuring RADIUS roaming function.....	130
11.4.7	Display RADIUS information	130
11.5	Configuration example.....	131
12.	GMRP Configuration	132
12.1	GMRP introduction.....	132
12.2	GMRP Configuration.....	132
12.2.1	Open GMRP settings.....	132
12.2.2	View GMRP information	133
12.3	Examples of typical GMRP configurations.....	133
13.	SNOOPING configuration	134
13.1	IGMP SNOOPING introduction	134
13.1.1	IGMP SNOOPING processing	134
13.1.2	Second layer dynamic multicast	135
13.1.3	Join a group.....	135
13.1.4	Leave a group.....	137
13.2	IGMP SNOOPING configuration	137
13.2.1	IGMP SNOOPING default configuration	137
13.2.2	Open and close IGMP SNOOPING	137
13.2.3	Configuration survival time	138
13.2.4	Configuration fast-leave.....	138
13.2.5	MROUTER configuration.....	139
13.2.6	Display information	139
13.3	The IGMP SNOOPING configuration example	139
14.	MVR configuration	141
14.1	MVR profile.....	141
14.2	MVR configuration.....	141
14.3	MVR configuration example	142
15.	DHCP SNOOPING configuration	143
15.1	DHCP SNOOPING introduction	143
15.1.1	DHCP SNOOPING processing.....	143
15.1.2	DHCP SNOOPING binding table.....	144
15.1.3	DHCP SNOOPING specifies the physical port of the linked server.....	144
15.1.4	DHCP SNOOPING binding list is uploaded and downloaded	144
15.2	DHCP SNOOPING configuration	145
15.2.1	DHCP SNOOPING default configuration	145
15.2.2	Global open and close DHCP SNOOPING	145
15.2.3	The interface opens and closes DHCP SNOOPING.....	145
15.2.4	DHCP SNOOPING binding list is uploaded and downloaded	145
15.2.5	Display information	146
15.3	DHCP SNOOPING configuration example	146
15.3.1	DHCP SNOOPING configuration	146
15.4	DHCP SNOOPING configuration error.....	148
16.	MLD SNOOPING configuration	149
16.1	MLD SNOOPING introduction	149
16.1.1	MLD SNOOPING processing	149
16.1.2	Second layer dynamic multicast	150
16.1.3	Join a group.....	150
16.1.4	Leave a group.....	152
16.2	MLD SNOOPING configuration	152

16.2.1	MLD SNOOPING default configuration	152
16.2.2	Open and close MLD SNOOPING	152
16.2.3	Configuration survival time	153
16.2.4	Configuration of fast-leave	153
16.2.5	MROUTER configuration.....	153
16.2.6	Display information	153
16.3	MLD SNOOPING configuration example.....	154
17.	ACL configuration	155
17.1	Introduction of ACL resource library.....	155
17.2	ACL filtering introduction	156
17.3	ACL repository configuration	157
17.4	ACL based on time interval	159
17.5	ACL filter configuration	161
17.6	ACL configuration example.....	161
17.7	ACL configuration debugging	163
18.	TCP/IP basic configuration	164
18.1	Configuring the VLAN interface	164
18.2	Configuring ARP	165
18.2.1	Configuring static ARP	166
18.2.2	View ARP information.....	167
18.3	Configuring static routing	167
18.4	TCP/IP basic configuration example.....	170
18.4.1	Three layer interface	170
18.4.2	Static routing.....	170
18.4.3	ARP.....	171
19.	SNMP configuration	172
19.1	SNMP introduction	172
19.2	SNMP configuration	172
19.3	SNMP configuration example.....	175
20.	RMON configuration	176
20.1	RMON introduction	176
20.2	RMON configuration	176
20.3	RMON configuration example.....	178
21.	Cluster configuration	179
21.1	Introduction of cluster management	179
21.1.1	Cluster definition	179
21.1.2	Cluster role.....	180
21.1.3	NDP profile.....	180
21.1.4	NTDP profile.....	181
21.1.5	Cluster management maintenance	181
21.1.6	Managing VLAN	183
21.2	Brief introduction of cluster configuration	183
21.3	Configuration management equipment.....	184
21.3.1	Enable system and port NDP capabilities	184
21.3.2	Configuring NDP parameters.....	185
21.3.3	Enable system and interface NTDP capabilities	185
21.3.4	Configuring NTDP parameters	185
21.3.5	Configure manual collection of NTDP information.....	186
21.3.6	Enable cluster function	186
21.3.7	Build clusters	186
21.3.8	Configure the cluster's internal members to interact.....	188
21.3.9	Configuring cluster member management.....	188
21.4	Configuration member device.....	189
21.4.1	Enable system and port NDP capabilities	189
21.4.2	Enable system and port NTDP capabilities.....	189

21.4.3	Configure manual collection of NTDP information.....	189
21.4.4	Enable cluster function	189
21.5	Configuring access cluster members.....	189
21.6	Cluster management display and maintenance	190
21.7	Example of cluster management typical configuration.....	190
22.	System log configuration	193
22.1	System log introduction	193
22.1.1	Format of log information.....	193
22.1.2	Log storage	194
22.1.3	Log display	195
22.1.4	22.1.4 Debugging tools.....	195
22.2	System log configuration	195
22.2.1	Configuring terminal real time display switch.....	195
22.2.2	View log information	196
22.2.3	Configure debugging switch	196
22.2.4	View debugging information	198
22.3	SYSLOG configuration	198
22.3.1	SYSLOG introduction	198
22.3.2	SYSLOG configuration	199
22.3.3	SYSLOG configuration example.....	199
23.	Port loop.....	201
23.1	Profile.....	201
23.2	Protocol principle.....	201
23.2.1	Detection process.....	201
23.2.2	Recovery mode	201
23.2.3	Protocol security	201
23.3	Configuration introduction.....	201
23.3.1	Global configuration	202
23.3.2	Interface configuration.....	202
23.3.3	Display configuration.....	202
24.	SNTP configuration.....	203
24.1	SNTP introduction	203
24.2	SNTP configuration	203
24.2.1	Default SNTP settings.....	203
24.2.2	Configuring SNTP Server address.....	203
24.2.3	Configure the SNTP sync clock interval.....	204
24.2.4	Configuring the local time zone.....	204
24.3	SNTP information display.....	204
25.	OAM configuration.....	209
25.1	OAM introduction.....	209
25.1.1	Link performance monitoring	209
25.1.2	Remote fault detection	209
25.1.3	Distal loopback	210
25.2	OAM configuration.....	210
25.3	Typical configuration examples of OAM	212
26.	CFM configuration	213
26.1	CFM profile	213
26.1.1	Basic concepts of CFM.....	213
26.1.2	Various functions of CFM.....	216
26.2	Brief introduction of CFM configuration tasks.....	217
26.3	CFM base configuration.....	218
26.3.1	Enable CFM function.....	218
26.3.2	Configuration service instance.....	218
26.3.3	Configuration maintenance endpoint	218
26.3.4	Configuration maintenance intermediate point.....	219

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

26.4	Configure various functions of CFM	220
26.4.1	Configuration continuity detection function	220
26.4.2	Configuration loopback function	220
26.4.3	Configuring link tracking function	221
26.3	CFM display and maintenance.....	221
26.4	Typical configuration examples	222
27.	IPv6 basic configuration	226
27.1	IPv6 profile	226
27.1.1	The characteristics of IPv6 protocol	226
27.1.2	IPv6 address introduction.....	227
27.1.3	IPv6 neighbour discovery protocol	230
27.1.4	IPv6 PMTU discovery	232
27.1.5	Protocol specification.....	232
27.2	IPv6 basic configuration task profile	233
27.3	Configure IPv6 basic functionality	233
27.3.1	Configuring IPv6 unicast address	233
27.4	Configuring IPv6 neighbour discovery protocol.....	233
27.4.1	Configuring the parameters of the RA message.....	233
27.4.2	Setting number to neighbour requests.....	236
27.5	IPv6 static routing configuration.....	236
27.6	IPv6 display and maintenance.....	237

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

1. Introduction to the CLI command line

This chapter gives a detailed description of the CLI command line interface. The main contents are as follows:

- Access switch CLI
- CLI mode introduction
- Introduction to command syntax
- Command line shortcuts
- Command History

1.1 Accessing the switch using the CLI

The CLI command line interface of the switch provides the interface for the user to manage the switch. The user can access the CLI command line interface of the switch through the Console port and the Telnet two terminals. The following are introduced separately.

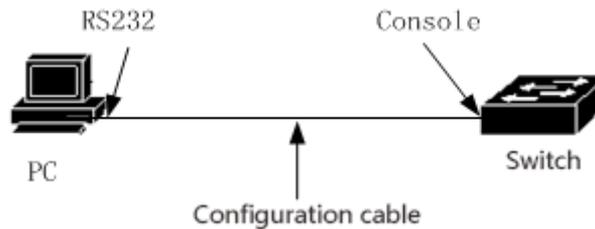
The main contents include:

- Users access CLI through Console port
- Users access CLI through TELNET

1.1.1 Users access CLI through Console port

The operating procedure is as follows:

First step: Connect the serial port of the PC with the Console port of the switch using the Configuration cable as seen in the following diagram:

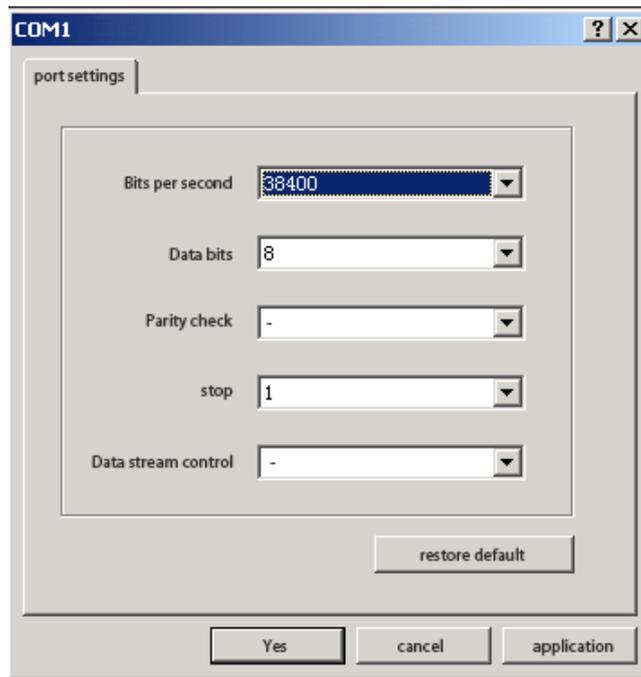


Second step: Start the terminal emulation program on the PC (such as the super terminal of Windows) Configure the communication parameters of the terminal emulation program.

The communication parameters of the terminal are configured as follows:

- Baud rate: 38400
- Data bits: 8
- Parity check: None
- Stop bit: 1
- Data stream control: None

For example the communication parameters configuration of the super terminal is shown below :



Third step: Power up the switch. After the Switch has started the CLI prompt will be displayed on the terminal (the default is Switch >) Users can enter commands at this prompt. This allows the user to access the CLI of the switch.

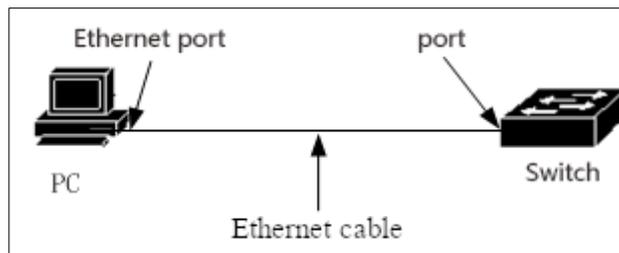
1.1.2 Users access CLI through TELNET

The user can access the switch through any port of the switch by using TELNET.

The IP address of the port of the switch defaults to 192.168.16.1

The steps to access the switch through the port are as follows :

First step: Connect Ethernet port and switch port of PC using an Ethernet cable as seen in the following diagram:



Second step: Set the IP address of the Ethernet port of the PC. The IP address must be in the 192.168.16.0/24 segment (e.g. IP address 192.168.16.100)

To confirm the connectivity between PC and switch use a Command Prompt window and Ping 192.168.16.1

Third step: If the PC is connected to the switch, then the command “Telnet 192.168.16.1” will access to the switch’s Telnet terminal interface.

Fourth step: If the system does not have a password, the Telnet interface goes directly to the CLI, and the CLI prompt appears (default is **Switch** >). If the system has a password set, then you need to enter the password on the Telnet interface to enter the CLI.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Please check the following before connecting

- The IP address of the switch port is based on the VLAN three layer interface, before accessing the switch you must set the IP address of a VLAN interface. The default IP address of VLAN1 is 192.168.16.1
The IP address of the VLAN interface can be configured through the Console port.
- The user accesses the switch through the port. You can connect a PC and ports directly through an Ethernet cable. You can also connect through a network.

1.2 Introduction to the CLI

The main contents include:

- The role of CLI model
- Identification of CLI mode
- Classification of CLI patterns

1.2.1 The role of CLI model

There are two main functions of CLI:

Classification of users to prevent unauthorised users from using CLI.

Users can be divided into two levels, Common users and Privileged users.

Common users can only see some of the running state of the switch and only use display commands.

Privileged users cannot only view the running state of the switch but also maintain and configure the switch to change the behaviour of the switch.

- **Convenient way for users to configure the switch**

The switches have a lot of configuration options and if you put all the configuration in one mode it's very difficult to configure the switch. To this end the establishment of multiple modes on the CLI with similar commands placed in a mode making the CLI as user-friendly as possible. For example by putting the commands associated with VLAN in the VLAN configuration mode. Put the interface related commands in the interface configuration mode.

1.2.2 Identification of CLI mode

The CLI prompt is the identity of the CLI mode. When the user is using the CLI by looking at the CLI prompt you will know which area of the CLI you're currently in.

The CLI prompt consists of two parts.

1. The first part identifies the host
2. The second pattern part identifies the CLI area

The host part of the CLI prompt uses the hostname of the system and the hostname of the system is configurable, the default hostname is **Switch**

The pattern part of the CLI prompt is not configurable each CLI area has its own corresponding pattern string, some pattern strings are constant and some strings are variable.

For example:

CLI prompt **Switch#** shows that the user is connected to a switch with the default name and the # shows that the user is in Privileged mode.

The CLI prompt **(config-ge1/1)#** shows that the user is in interface configuration mode and is configuring the ge1/1 port

The CLI prompt **Switch(config-vlan2)#** shows that the user is in interface configuration mod and can configure the VLAN2 interface.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

1.2.3 Classification of CLI patterns

The CLI model is divided into four categories: general mode, privileged mode, global configuration mode and configuration sub pattern while the configuration sub model is composed of many CLI modes.

Ordinary users can only access common patterns, and privileged users can access all of the CLI patterns.

Console and Telnet terminals first enter the common mode and can then enter the enable command in the common mode and if they can successfully verify the password, they are then granted access to the privileged mode.

On the Telnet terminal ordinary users can only stay in the ordinary mode and cannot enter privileged mode.

Privileged users can enter the configure terminal in privileged mode and can access the global configuration mode. In the global configuration mode you can enter the relevant commands and enter each configuration sub mode.

The following table lists the main CLI modes of switches :

Mode	Description	Prompt	Entry mode command	Exit mode command
Common mode	Provides a display command to view the status information of the switch.	Switch>	Terminal first entry mode.	On the Console terminal there is no exit mode command and exit or quit command is used to exit the Telnet terminal on the Telnet terminal.
Privileged mode	In addition to providing the display command to view the status information of the switch, it also provides commands such as debugging, version update and configuration maintenance.	Switch#	Enter the enable command in the normal mode.	Returns to normal mode using the disable command. On the Console terminal use exit or quit command to retreat to the normal mode and use the exit or quit command to exit the Telnet terminal on the Telnet terminal.
Global configuration mode	Provides generic commands that cannot be implemented in configuration sub patterns, such as configuring static routing commands.	Switch(config)#	Enter the configure terminal command in privileged mode.	Use exit, quit or end commands to exit to privileged mode.
Interface configuration	Provides commands for configuring ports and	port: Switch(config-	Input in global configuration	Use the exit or quit command to exit to the

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

mode	VLAN interfaces.	ge1/1)# VLANInterface: Switch(config- vlan1)#	modeinterface e <if-name>	global configuration mode and exit with the end command to the privileged mode.
VLAN configuration mode	Provides commands for configuring VLAN. For example, commands for creating and deleting VLAN.	Switch(config- vlan)#	In the global configuration mode, enter the VLAN database command.	Use the exit or quit command to exit to the global configuration mode and exit with the end command to the privileged mode.
MSTP configuration mode	Provides commands for configuring MSTP. For example, commands for creating and deleting instances of MSTP.	Switch(config- mst)#	In the global configuration mode, enter the spanning-tree MST configuration command.	Use the exit or quit command to exit to the global configuration mode and exit with the end command to the privileged mode.
Terminal configuration mode	Provides commands for configuring Console and Telnet terminals, such as configuring timeout time for a terminal.	Switch(config- line)#	In the global configuration mode, enter the line vty command.	Use the exit or quit command to exit to the global configuration mode and exit with the end command to the privileged mode.

1.3 Introduction to command syntax

The main contents include:

- Command composition
- Parameter type
- Command syntax rules
- Command abbreviation
- Grammar help
- Command line error message

1.3.1 Command composition

The CLI command consists of two parts, the keyword and the parameter. The first word must be a keyword, the latter word can be a keyword or a parameter and the keywords and parameters can appear alternately. A command must have a keyword, but it can have no parameters. For example the command write is only one keyword without a parameter, the command show version has two key words without a parameter, the command VLAN <vlan-id> has a key and an instance <instance-id> VLAN <vlan-id> command parameters and has two keywords and two keyword parameters and parameters appearing alternately.

1.3.2 Parameter type

CLI order parameters are divided into two types, mandatory and optional parameters.

Mandatory parameters are those that are required in the input command and must be entered.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

For example the command **VLAN <vlan-id>** the <vlan-id> parameter is a required parameter.

Optional parameters are those that are not required.

For example the command **show interface [if-name]** the [if-name] parameter is optional and only needed to show a specific interface.

1.3.3 Command syntax rules

When describing commands with text, the following rules must be satisfied:

1) Keywords are directly represented by words.

Such as command **show version**

2) Parameters must be enclosed with <>

Such as command **VLAN <vlan-id>**

3) If it's an optional parameter the parameters must be enclosed with [...]

Such as command **show VLAN [<vlan-id>]**

For this situation the parameter <> can be omitted and changed:

Command **show vlan [vlan-id]**

That is the parameter vlan-id is optional and can be input or not.

If this is a required parameter, the parameters cannot have []

4) If you have multiple keywords or parameters, you must choose one. You can enclose a number of keywords or parameters with {} between multiple keywords or parameters with | separated | required before and after a space.

If multiple keywords required command:

spanning-tree mst link-type {point-to-point | shared}

Between point-to-point and shared, you have to choose one.

A number of parameters required command:

no arp {<ip-address> | <ip-prefix>}

Keywords and parameters mixed with the necessary command:

Show spanning-tree mst {none|instance <0-15>}ng

5) If multiple keywords or parameters are selected one. Enclose a number of keywords or parameters with [...] Between multiple keywords or parameters with | separated, | required before and after a space.

The following commands:

debug ip tcp [recv | send]

Keywords recv and send can choose one, You can't choose either.

show ip route [<ip-address> | <ip-prefix>]

show interface [<if-name> | switchport]

6) If you have a keyword or parameter or a set of keywords or parameters, you can repeat the input, and add the symbol "*" after the keyword or parameter".

For example, the ping command:

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k <count> <ip-address>* | -w <timeout>]*
-j <count> <ip-address>* --- Multiple IP addresses can be repeatedly entered
The entire option can also be repeated.

7) Parameters are represented by descriptors of one or more words. If it is more than one word, each word is separated by sign "-", and each word is lowercase.
Correct parameter representation: <vlan-id>, <if-name>, <router-id>, <count> etc.
Wrong parameter representation: <1-255>, <A.B.C.D>, <WORD>, <IFNAME> etc.

1.3.4 Command abbreviation

When the user enters the command on the CLI interface the keyword of the command can be abbreviated. CLI supports the prefix matching function of the command. As long as the input word matches the keyword prefix the CLI can parse the input word into the matched keyword. In this way it is very convenient for users to use CLI and the user can type a command with very few characters for example such as the **show version** command, which can be shortened to **sh ver**

1.3.5 Grammar help

The CLI command line interface is set with syntax help to support each level command and parameters:

- 1) Direct input in a CLI mode use the ? character. On the terminal the first keyword and its description of all commands under this mode are listed, for example **Switch(config)#?** Will show all the commands available for the privileged mode user.
- 2) Enter the preceding part of a command, then enter a space and then enter the ? Character. On the terminal all the keywords or parameters of the next level are listed and their descriptions are given. for example **Switch#show ?**
- 3) Enter an incomplete keyword and enter it with the ? Character then all keywords and their descriptions that match the input prefix are listed on the terminal, for example **Switch#show ver?**
- 4) Enter the preceding part of a command, then enter a space and then enter the Tab key then the terminal will list all the keywords at the next level.
- 5) The input is not a complete keyword directly enter the Tab key, if there is only one keyword and the input prefix matching it will be filled, if there are multiple keyword matching with the input prefix, all matching keyword lists in the terminal will be shown.

1.3.6 Command line error message

If the command entered by the user does not pass the syntax check, the error message will be displayed on the terminal. The common error information is shown in the following table.

Error message	Possible Reason
Invalid input or Unrecognized command	No matching keywords found. Parameter input incorrect. Too many keywords or parameters are entered.
Incomplete command	Command input is incomplete, and the keyword or parameter is not entered.
Ambiguous command	The keyword input is incomplete, and multiple keywords match the input prefix.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

1.4 Command line shortcuts

The main contents include:

- Line edit shortcut key
- Display command shortcut key

1.4.1 Line edit shortcut key

The CLI command line interface supports the line editing shortcut function, and the line edit shortcut can facilitate the input and editing of the CLI command. When the user enters or edits commands, you can use the line edit shortcut to accelerate the command input. The following table lists all the line edit shortcuts and functions to implement:

Shortcut key	Function
Ctrl+p Or up arrow	The last command
Ctrl+n Or down arrow	Next command
Ctrl+u	Delete entire rows
Ctrl+a	The cursor back to the
Ctrl+f Or to key	The cursor moves to the right
Ctrl+b Or left key	Move the cursor to the left
Ctrl+d	Delete the character at the cursor
Ctrl+h	Delete the previous character of the cursor
Ctrl+k	Delete all characters at the cursor and cursor
Ctrl+w	Delete all characters before cursor
Ctrl+e	Move the cursor to the end of the line
Ctrl+c	Interrupt, do not execute command line. If CLI is in the global configuration mode or the configuration sub mode, CLI will retreat to privileged mode; if CLI is in normal mode or privileged mode, the CLI schema remains unchanged, but CLI starts another new line.
Ctrl+z	Same function as Ctrl+c.
Tab	Enter this keyword when you enter an incomplete keyword, and if there is a keyword that matches the entered prefix, the keyword is padded; if more than one keyword matches the entered prefix, all matching keywords are listed; If there is no keyword match, this key is invalid.

Be careful: some Console On the terminal ↑、↓、→、← These keys are unavailable

1.4.2 Display command shortcut key

The commands that start with the show keyword are all display commands. Some display commands cannot be displayed in one screen because of the display of a lot of contents, and the terminal provides the function of screen display. After displaying a screen, the terminal waits for user input to determine the subsequent processing. The following table lists the shortcut keys for displaying commands and their functions.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Shortcut key	Function
Space	Display next screen
Enter	Show next line
Ctrl+c	Break the execution of the command and exit to the CLI mode.
Other keys	Same function as Ctrl+c.

1.5 Command History

The CLI command line interface supports the history function of commands. It can remember up to 20 historical commands that the user has recently used and save the commands that the user recently typed.

You can use `show history` to display commands that have been entered. You can also use the keystrokes `Ctrl+p` `Ctrl+n` or `↑` `↓` keys to select historic commands. The history command function makes it easy for users to re-enter commands.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

2.0 System management configuration

Before configuring the switch, you need to master the switches basic configuration of the system management and maintenance.. This chapter describes the basic configuration of these system management and maintenance, including the following:

- System security configuration
- System maintenance and debugging
- Configuration file management
- Software version upgrade

2.1 System security configuration

In order to prevent illegal users from invading switches, the system provides several security measures for system management, mainly including :

- Multi-user management control
- TACACS+ authentication authorization
- Anonymous user password control
- Enable password control
- TELNET service control
- SNMP service control
- HTTP service control
- SSH service control

2.1.1 Multi-user management control

Multi-user management not only ensures the security of the switch system, but also provides the ability for multiple users to manage and maintain the switch simultaneously.

Multi-user management is used by giving each user a unique username, password and authority to ensure the safety of the system. The user first needs to authenticate their username and password in the access switch which will then verify the username and password. The user can then access the switch after verification, but the user's permission limits the scope of that user's access to the switch.

Multi-user management divides user's rights into two levels: ordinary users and privileged users. Ordinary users can only stay in the ordinary mode of the CLI command line interface and can only use the display command to query the information of the switch. Privileged users can access all the modes of the CLI command line interface and all commands provided by CLI can be used to query the information of the switches and to maintain and manage the switches.

The multi-user management function is only applied to the Telnet terminal and the Console terminal is not controlled. When you use Console terminal to access the switch you don't need to verify the username and password, and the user can access the CLI directly. Using the Telnet terminal to access the switch need to verify the username and password, only when the username and password are verified can they access the CLI.

The user management function is not enabled by default. At this point, the login Telnet terminal does not need to verify the username and password. When a username is added to the command, the multi-user management function is enabled. At this point, the Telnet terminal needs to verify the username and password. When commands are used to delete all users, the multi-user management function is closed and the system returns to the default state.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

The commands associated with multi-user management are as follows :

Command	Description	CLI mode
username <user-name> password <key> {normal privilege}	Add a user, if the specified user already exists then modify the password and permissions of the user. The first parameter is the user name, the second parameter is the password, the option represents the authority, normal represents the ordinary user, and the privilege represents the privileged user.	Global configuration mode
no username [user-name]	Delete one or all of the users. If you don't input a parameter, it means deleting all users, if the input parameter represents the user who deletes a specified user name.	Global configuration mode
show running-config	Viewing the current configuration of the system, you can see the configuration of multi user management.	Privileged mode

2.1.2 TACACS+ authentication authorisation

TACACS+ authentication and authorisation provides more strict user management rights, not only to verify the legitimacy of users, but also to authorise the command. After opening the TACACS+ authentication, the user first needs to verify the username and password through the TACACS+ server when accessing the switch. Only when the user name and password are correct and consistent can they pass the verification. The user can access the switch after verification.

TACACS+ also divides the user's permissions into two levels: ordinary users and privileged users. Ordinary users can only stay in the ordinary mode of the CLI command line interface, and privileged users can access all the patterns of the CLI command line interface. On the basis of permission level, it also sets the command execution authority, and the user enters a command (except enable, end and exit), which must be verified on the TACACS+ server, and the verification failure will not be executed.

The TACACS+ authentication and authorization function is only applied to Telnet and SSH terminals and does not control the Console terminal. The user name and password need to be verified when accessing the switch through the Telnet or SSH terminal. Only the user name and password are verified before they can access the CLI. When SSH is accessed, only privileged users can pass it. TACACS+ authentication is also applied to WEB login, but only verify password privilege permissions, do not command authorization.

By default, the switch TACACS+ is not enabled, the Telnet, SSH or WEB lands using the multi user management function. The TACACS+, user management function can continue to configure,

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

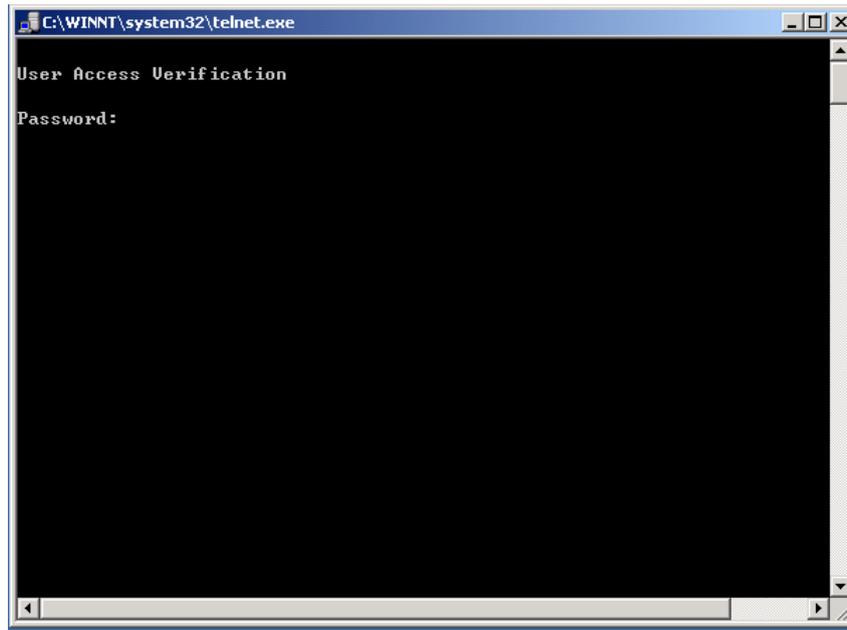
but not the actual use. The TACACS+ authentication authorization related commands are as follows:

Command	Description	CLI mode
tacacsplus enable	Open the TACACS+ function	Global configuration mode
tacacsplus disable	Close TACACS+ function	Global configuration mode
tacacsplus host A.B.C.D	Configuring the master server address, it is recommended to use Cisco's ACS	Global configuration mode
tacacsplus key WORD	Configure the shared key that encrypts the data and must be consistent with the configuration on the server	Global configuration mode
tacacsplus auth-type (PAP CHAP)	Select authentication methods, including PAP and CHAP. Among them, PAP is the default mode, the field encapsulates the password, and CHAP encapsulates the password MD5 check code.	Global configuration mode
show tacacsplus	View TACACS+ configuration information	Global configuration mode
no tacacsplus host	Clear master server address	Global configuration mode
no tacacsplus key	Clearing shared keys	Global configuration mode

2.1.3 Anonymous user password control

When multi-user management is not enabled, the user login Telnet terminal does not need to check the user name and password, a user can directly access the Telnet CLI. In order to improve the security of the system, the switch adds an anonymous user (admin) password to control the Telnet and Web access. When the switch is set the 'anonymous' user password and user management is not enabled to undertake an anonymous user password check user login Telnet terminal and Web, but only to enter the correct password to be able to access CLI and Web page. If the system uses multi-user management, 'anonymous' user password will not be effective, the user access to the Telnet terminal and Web does not undertake an anonymous user password check but do more user management user name and password check.

There is no anonymous user password in the switch. In this case, the user does not need to verify the anonymous user password when accessing the Telnet terminal and the Web. The figure below is the user login Telnet terminal interface, enter anonymous user password at this interface.



The diagram below is the dialog box for the user to log in to Web. In this dialog box, the anonymous user admin and password are entered.



The associated commands for anonymous user passwords are listed below :

Command	Description	CLI mode
password <key>	Setting anonymous user password.	Global configuration mode
no password	Clear anonymous user password.	Global configuration mode
show running-config	Viewing the current configuration of the system, you can see the configuration of the anonymous user password.	Privileged mode

Caution: For the security of the system, the administrator needs to set the anonymous user password of the system.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

2.1.4 Enable password control

The Enable password is used to control the switch from normal mode to privileged mode. Before Enable password authentication the user can only view the information of the switch. After the Enable password is verified, it is possible for the user to configure and maintain the switch.

Enable password does not depend on the user, any user login to the Console terminal or Telnet terminal, if you want to enter the privileged mode the switch must verify the Enable password, if the authentication is not successful, you can only stay in normal mode.

In the normal mode, enter the Enable command, the terminal will prompt the user to enter the password, then the user can enter the Enable password, if the password verification is successful, they will gain access to the privileged mode, otherwise they stay in the normal mode. For ordinary users whether or not the password is valid they enter the privilege mode.

Enable password defaults to empty, in this case, in the normal mode, enter the Enable command, the terminal does not prompt the password, enter the privileged mode directly.

The related commands of the Enable password are listed below :

Command	Description	CLI mode
enable password <key>	Set the enable password of the system.	Global configuration mode
no enable password	Clear the enable password of the system, enable password is empty	Global configuration mode
show running-config	View the current configuration of the system, you can see the configuration of the enable password.	Privileged mode
enable	The interactive command verifies the enable password of the system. After the verification is successful, the terminal enters the privileged mode.	Normal mode

Note: for the security of the system, the administrator needs to set the Enable password of the system.

2.1.5 TELNET service control

In some cases, administrators do not need to access the switch using remote management, they only need access through the Console terminal to the switch. If so, in order to improve the security of the system and to prevent illegal users from remote login Telnet terminal, the administrator can shut down the Telnet service. By default Telnet service is open.

The related commands of Telnet service control are as follows :

Command	Description	CLI mode
security-manage telnet enable	Open Telnet service.	Global configuration mode
security-manage telnet disable	Closing Telnet services.	Global configuration mode
security-manage telnet number <1-100>	The number parameter ranges from 1 to 100, and defaults to 5.	Global configuration mode
security-manage telnet access-group <1-99>	Specify an ACL group and open the source IP address control. If the specified ACL group does not exist or is not a	Global configuration mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

	standard ACL group, then the source IP address is not controlled.	
no security-manage telnet access-group	Close source IP address control.	Global configuration mode
show security-manage	You can see the configuration of the service control.	Privileged mode

2.1.6 SNMP service control

The SNMP service control can open / close the SNMP service, and also control the IP address of the access switch by ACL.

The related commands of SNMP service control are as follows :

Command	Description	CLI mode
security-manage snmp enable	Open SNMP service.	Global configuration mode
security-manage snmp disable	Closing SNMP services.	Global configuration mode
Security-manage snmp access-group <1-99>	Specify an ACL group and open the source IP address control. If the specified ACL group does not exist or is not a standard ACL group, then the source IP address is not controlled.	Global configuration mode
no security-manage snmp access-group	Close source IP address control.	Global configuration mode
show security-manage	You can see the configuration of the service control.	Privileged mode

2.1.7 HTTP service control

The HTTP service control can open / close the HTTP service, and also control the IP address of access to the switch using ACL.

The HTTP commands are as follows :

Command	Description	CLI mode
security-manage http enable	Open HTTP service.	Global configuration mode
security-manage http disable	Closing HTTP services.	Global configuration mode
security-manage http access-group <1-99>	Specify an ACL group and open the source IP address control. If the specified ACL group does not exist or is not a standard ACL group, then the source IP address is not controlled.	Global configuration mode
no security-manage http access-group	Close source IP address control.	Global configuration mode
show security-manage	You can see the configuration of the service control.	Privileged mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

2.1.8 SSH service control

The traditional network service program, such as: FTP, PoP and Telnet are not safe by nature because they use plain text passwords and data transfer on the network. For people who have an ulterior motive this is very easy to intercept these passwords and data. Moreover, the security verification of these service programs is also vulnerable, that is very easy to "man" (man-in-the-middle) in this way the attack. The so-called "middleman" attack, is the "middleman" to impersonate the real server to receive the data you send to the server, and then pretend to be you pass the data to the real server. When the data transfer between the server and you is done by the middleman, there will be a serious problem. By using SSH, you can encrypt all the data transmitted, so that "middleman" this attack cannot be possible, but also to prevent DNS spoofing and IP spoofing. With the use of SSH, there is an additional benefit is that the transmission of data is compressed, so you can speed up the transmission speed. SSH has a lot of features, it can replace Telnet, but also for FTP, PoP, and even for PPP to provide a secure "channel".

2.2 System maintenance and debugging

The basic functions of system maintenance and debugging include the following contents:

- Configure the host name of the system
- Configuring the system clock
- Configure terminal timeout attributes
- System reset
- View system information
- Network connectivity debugging
- Detecting line distance
- Traceroute debugging
- Telnet client
- UDLD configuration

2.2.1 Configure the host name of the system

The host name of the system is used to identify the switch which allows the user to distinguish between different switches because the host name of the system is part of the CLI prompt of the terminal. The host name of the system defaults to Switch.

The commands of the host name of the system are as follows:

Command	Description	CLI mode
hostname <name>	Set the host name of the system.	Global configuration mode
no hostname	Clear the host name of the system, that is, the hostname returns to the default value Switch.	Global configuration mode
show running-config	Viewing the current configuration of the system, you can see the configuration of the host name of the system.	Privileged mode

2.2.2 Configuring the system clock

The switch provides the function of a real time clock, the current clock can be set by the command and the current clock can also be viewed. The system clock is powered by internal power, so that the real time clock can be operated continuously when the system is powered off, and the system does not need to reset the clock after restarting.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

The switch has been set up in the factory clock, the user does not need to set again, if the user found that the time is not allowed, the user can reset the clock.

The related commands of the system clock are as follows:

Command	Description	CLI mode
set date-time <year> <month> <day> <hour> <minute> <second>	Set the current clock of the system, you need to input parameters of year, month, day, hour, minute and second.	Privileged mode
show date-time	The current clock of the display system.	Normal mode, Privileged mode

2.2.3 Configure terminal timeout attributes

For the security of the terminal, when the terminal has no key input for more than a certain period of time then the terminal will start the exit processing. Console terminal and Telnet terminal exit processing is not the same, for the Console terminal when the terminal timeout the CLI mode turns back to normal mode, for the Telnet terminal when the terminal timeout then the Telnet connection is interrupted and then exited.

The terminal timeout time is 10 minutes by default, and the user can also disable the terminal timeout.

The related commands for terminal timeout are listed below:

Command	Description	CLI mode
exec-timeout <minutes> [seconds]	Set terminal timeout time if the parameters are 0 indicating that the terminal will never timeout.	Terminal configuration mode
no exec-timeout	Set the terminal timeout time back to the default, that is, 10 minutes.	Terminal configuration mode
show running-config	View the current configuration of the system, you can see the terminal timeout configuration.	Privileged mode

2.2.4 System reset

The system provides a reset method:

- Reset switch

The related commands of system reset are as follows:

Command	Description	CLI mode
reset	Reset switch.	Privileged mode

2.2.5 View system information

The system provides rich display commands to see the system running status and system information, this is a list of a few commonly used system maintenance display commands:

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Command	Description	CLI mode
show version	Display system version number and compile time of executable file connection.	Normal mode, Privilege mode
show snmp system information	Display the basic information of the system, including how long the system started after the operation.	Normal mode, Privilege mode
show history	Displays the list of recently entered commands on the CLI command line.	Normal mode, Privilege mode

2.2.6 Network connectivity debugging

In order to debug the connectivity of the switch with another device in the network, you may need to ping the switch on the switch and ping the IP address of the peer. If the switch receives a ping reply from the other party, then it indicates that the two ends are connected.

The switch not only implements the ping command, but also supports many options on the ping command. The user can use these options to make more precise and complex debugging.

The ping command follows the table:

Command	Description	CLI mode
ping <ip-address> [-n <count> -l <size> -r <count> -s <count> -j <count> <ip-address>* -k <count> <ip-address>* -w <timeout>]*	It can be used without any options, or with one or more options. If you do not have any options, it is the simplest ping command. When the command is executed, you can type the execution of the Ctrl+c interrupt command.	Privileged mode

2.2.7 Detecting line distance

Command	Description	CLI mode
show cable-diag interface IFNAME	Detection of electrical cable distance	Privileged mode

2.2.8 Traceroute debugging

In order to debug the intermediate devices that the switch communicates with another device in the network, it may be necessary to implement the trace-route command on the switch. When using the trace-route command on the switch specify the IP address of the other party. When the command is executed, the path through to the remote end will be displayed.

The switch not only implements the trace-route command, but also supports many options on the trace-route command, which allows users to make more precise and complex debugging by using these options. The trace-route command follows the table below:

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Command	Description	CLI mode
<pre>trace-route <ip-address> [-h <maximum-hops> -j <count> <ip-address>* -w <timeout>]*</pre>	<p>You can use one or more options when you're using it without any options. If you don't have any options, it's the simplest trace-route command.</p> <p>When the command is executed, you can type the execution of the Ctrl+c interrupt command.</p>	Privileged mode

2.2.9 Telnet client

The switch provides Telnet client functions, and users can access other devices remotely through the Telnet client.

Command	Description	CLI mode
telnet <ip-address>	The parameter is the IP address of the target device	Privileged mode

2.2.10 UDLD configuration

UDLD (Uni Directional Link Detection) : Is a two-layer protocol that monitors the physical configuration of an Ethernet link using fiber or twisted pair connections.

When a uni-directional link (only one direction is transmitted, for example, it can send you data, (Receive), but if you send me the data, I cannot receive that data).

UDLD can detect this situation, close the corresponding interface and send a warning message.

Uni-directional links can cause a lot of problems, especially when using spanning tree, which may cause loops.

Note: UDLD requires both ends of the link to be supported for normal operation.

UDLD supports two modes of operation.

1. Common (normal) mode (default)
2. Radical (aggressive) mode.

General (normal) mode: in this mode, UDLD can detect uni-directional links and label ports as undetermined states to generate system logs. In other words, normal mode will shut down a port only if it can explicitly determine that the associated link is faulty for an extended period of time.

Aggressive mode: In this mode, UDLD can be detected by a unidirectional link. And will try to rebuild the link if after continuous transmission for 8 seconds of sending UDLD messages, if there is no UDLD echo response then this port will be placed in the errdisable (error-disabled) state.

(This can be caused by a faulty NIC, cable or misconfiguration etc)

Command	Description	CLI mode
udld enable	Global enable UDLD function	Global configuration mode
udld message time <time>	UDLD message transmission interval	Global configuration mode
udld port	Port enable UDLD	Interface configuration mode
udld aggressive	Enable port radical mode, default normal mode	Interface configuration mode
show udld <ifname>	View the port UDLD information	Privileged mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

2.3 Configuration file management

The configuration is divided into the current configuration and the initial configuration. The current configuration refers to the configuration of the system runtime and initial configuration refers to the default configuration of the switch.

The switch has onboard system memory and FLASH. FLASH stores the initial configuration and a copy of the current configuration. System memory stores the current configuration. When the user executes the relevant commands to modify the current configuration of the system only the configuration in system memory is changed, the user will need to enter the Save command to store the current configuration into FLASH for use the next time the switch powers up or is reset. When the system is started for the first time the system the current configuration information of the system is the same as the initial configuration.

The current configuration and the initial configuration use the same format and in the command-line text format is very intuitive and easy for users to read. The format of the configuration file has the following features:

- The configuration file is a text file.
- All the commands are saved.
- Only save non default configurations and do not save the default configuration.
- The commands are organized in the CLI mode, and the commands in the same CLI mode are organized together to form a segment separated by a "!". For commands within the global configuration mode, organize commands with the same function or function to be separated by "!".
 - For a command that configures a sub-pattern, there is a space before the command, and no commands are required for commands in the global configuration mode.
 - With "end" as the end of the configuration.

Configuration file management mainly includes the following:

- View configuration information
- Save configuration
- Delete configuration file
- Download configuration files

2.3.1 View configuration information

View configuration information including viewing the current configuration and initial configuration of the system. The initial configuration is actually in the FLASH configuration file, when the FLASH does not exist in the configuration file, the system starts using the default configuration, this time if you view the initial configuration of the system, the system will prompt the configuration file does not exist.

The commands for viewing configuration information are shown in the following table:

Command	Description	CLI mode
show running-config	See the current configuration of the system.	Privileged mode
show startup-config	See the initial configuration of the system.	Privileged mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

2.3.2 Save configuration

When the user changes the current configuration of the system, these configuration changes need to be saved to the configuration file in FLASH so that the correct configuration is used after the restart, otherwise on restart this configuration information is lost. Save configuration command saves the current configuration FLASH.

Save the configuration command as follows:

Note: You need to use this command to save the configuration after configuring the switch.

Command	Description	CLI mode
write	Save current configuration.	Privileged mode

Otherwise, the configuration will be lost after a system reboot.

2.3.3 Delete configuration file

When the user wants to return to the initial configuration of the system, the current configuration stored in FLASH must be deleted. After which the switch needs to be restarted for the initial configuration to be active.

Users must be cautious when deleting configuration files, otherwise the configuration will be lost. The commands for deleting configuration files are as follows,

Command	Description	CLI mode
delete startup-config	Delete the configuration file of the system.	Privileged mode

2.3.4 Download configuration files

It is possible to download the configuration into a file on a PC and upload an existing configuration file to the switch. After uploading a configuration file the switch must be restarted for the new configuration to be in effect.

The web browser interface uses the same configuration files.

The commands downloaded from the configuration file are as follows:

Command	Description	CLI mode
upload configure <ip-address> <file-name>	Upload the configuration file to the PC machine, the first parameter is the IP address of the PC machine, and the second parameter is the file name of the configuration file stored on the PC machine.	Privileged mode
download configure <ip-address> <file-name>	The configuration file is downloaded to the PC, the first parameter is the PC's IP address, the second parameter is the configuration file stored on the PC file name.	Privileged mode

The configuration file is downloaded and used to the TFTP protocol. The TFTP client software is run on the switch and the TFTP server software must be run on the PC server. The operating steps downloaded from the configuration file are as follows:

First step: Build network environment.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Second step: Start the TFTP server software on the PC, and set the directory stored in the configuration file.

Third step: Save configuration on switch.

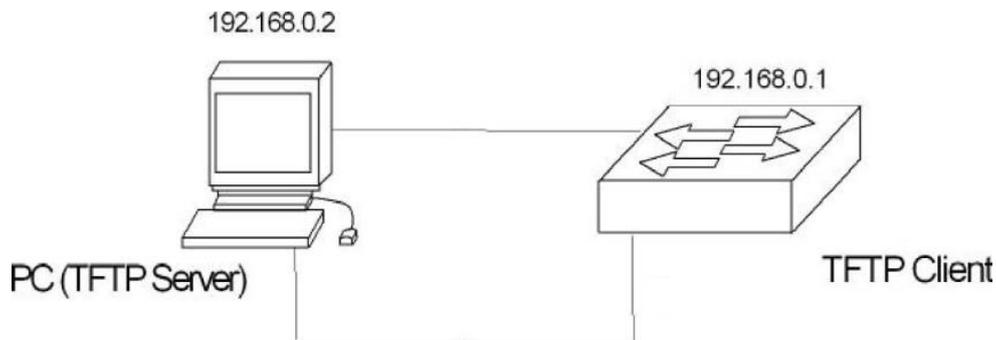
Fourth step: The configuration file upload command is executed on the switch, and the configuration files are backed up to the PC.

Fifth step: When the switch needs the configuration file on the PC machine, the configuration file download command is executed on the switch, and the configuration file on the PC machine is downloaded to the switch.

Sixth step: To make the configuration effective, the switch must be restarted.

Example: A switch that has been configured with VLAN and interface addresses, which needs to be downloaded on the configuration file.

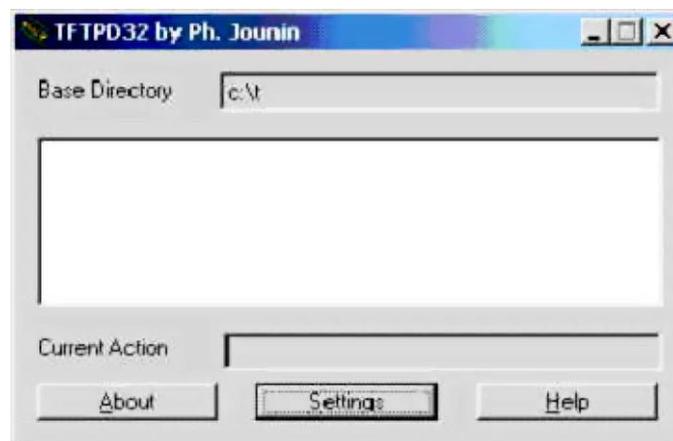
First step: Build the following network environment.



The configuration port of the switch is connected to a configuration terminal through the cable and connected with a PC through the network cable. Install TFTP Server in PC, configure Ethernet port IP address of PC, assume the IP address of PC is 192. 168.0.2. Then, configure the IP address of the switch, where the IP address of the switch is assumed to be 192.168. 0.1 to ensure the connectivity between the PC and the switch.

Second step: Start TFTP Server, configure TFTP Server parameters.

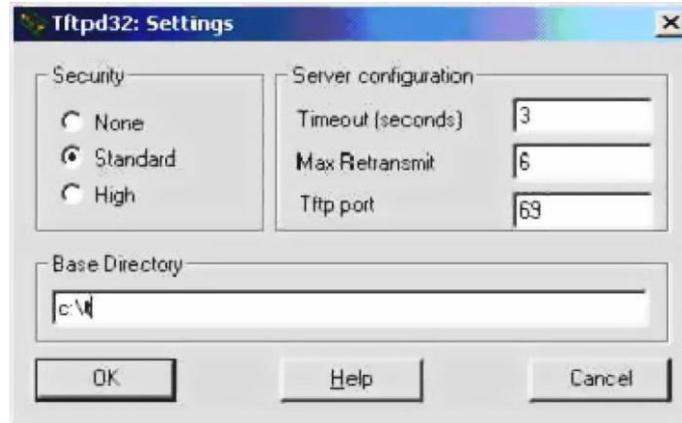
Run TFTP Server, the window interface as below :



Then, set the directory of the backup configuration file. The specific operation is, click the

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

[Settings] button, set the interface, the following chart:



Enter the file path in "Base Directory". Click the [OK] button to confirm.

Third step: Execute the write command on the switch and save the current configuration to the configuration file.

Fourth step: To back up a file to a PC, run the Switch # upload configuration 192.168.0.2 beifen.cfg.

Fifth step: If necessary, download the backup file to the switch and execute the command Switch#download configuration 192.168.0.2 beifen.cfg.

Sixth step: If you want to download the configuration file to be effective, you must restart the switch, execute the command Switch#reset.

2.4 Software version upgrade

The switches support online updating of software versions. The upgrade is achieved by using TFTP.

The main contents are as follows:

- Software version upgrade commands
- Software upgrade process

2.4.1 Software version upgrade commands

Upgrade the image file of the switch in global configuration mode. The commands are as follows:

download image <ip-address> <file-name>

Where <ip-address> is the IP address of the PC running the TFTP server and <file-name> is the image file name saved on the TFTP server.

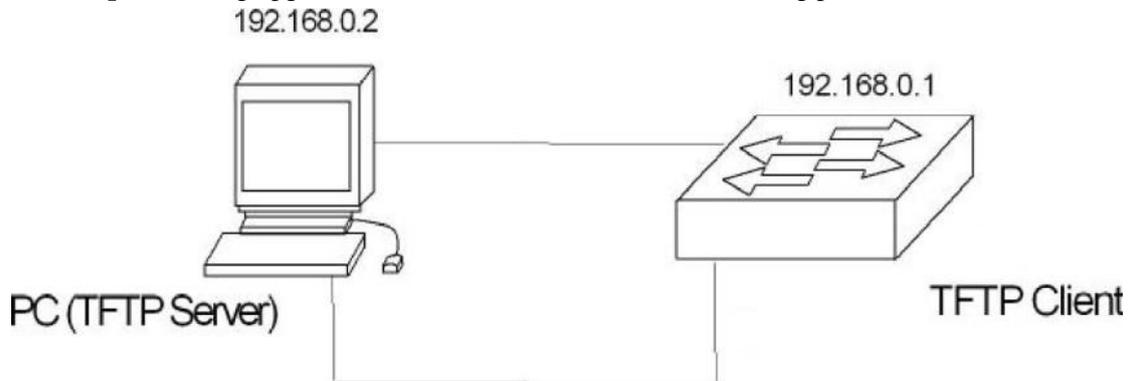
In the process of upgrading cannot power or switch the image file may be damaged and cause the switch cannot start. After the download is complete, you need to restart the switch to run the newly downloaded image file program. The whole upgrade process takes a few minutes. Please be patient.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

2.4.2 Software upgrade process

Update the image file steps as follows :

First step: Building upgrade environment. As shown in the following picture.

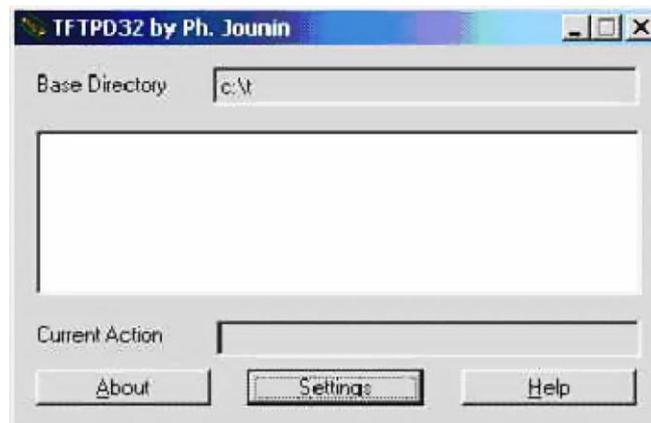


The construction process is as follows :

- Connect the console port of the switch to a console terminal (PC).
- Install TFTP Server on PC.
- Copy the new image file to a path of PC, where the path is assumed to be c:\t;
- Configure the Ethernet port IP address of PC, where the IP address of PC is assumed to be 192.168.0.2 .
- Configure the IP address of the switch, where the IP address of the switch is assumed to be 192.168.0.1.

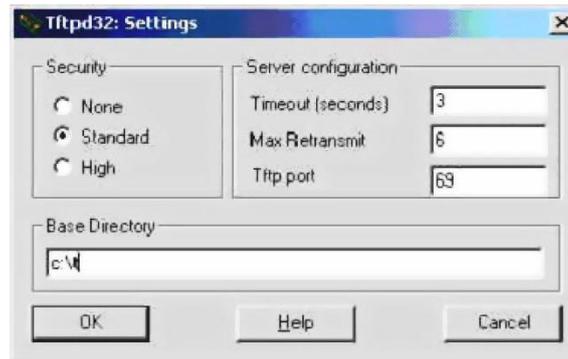
Second step: Run TFTP Server and configure the TFTP server.

First Run your TFTP Server. TFTP32 window interface as shown below :



Then: Setting the TFTP Server file directory. After you start TFTP Server, reset the TFTP Server file directory and copy the image files that you want to load into this directory. The specific operation is, click the [Settings] button, there TFTP32 settings interface, as shown below.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch



Enter the file path in the "Base Directory". Click the [OK] button to confirm.

Third step: Upgrade file.

Then: Connect the port of the switch to the PC of the TFTP Server program through the Ethernet network. The ping command is used to check the connection between the host and the switch.

Next: Enter the command at the super terminal Switch# prompt:

Switch# download image 192.168.0.2 switch.img, Enter and wait for the upgrade file to finish. Software is updating. Please wait and don't power down!

.....

Updating is completed. Do you wish to reset?[Y/N]

After the file transfer is completed, the system will indicate whether you need to restart the switch. In general, we recommend that you choose 'Y' to restart the switch, because the system upgrade can only take effect after restarting. If your configuration file is not saved, you can choose "N" first, do not restart then complete the configuration and other operations, then restart the switch.

Switch#

note:

The switch Must Not be switched off during the upgrade process.

Fourth step: Reboot.

Switch# reset

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

3 PORT CONFIGURATION

This chapter introduces port related configuration, including the following contents:

- Common configuration for ports
- Configuration MIRROR
- Configuring STORM-CONTROL
- Configuring STORM-CONSTRAIN
- Configuring FLOW-CONTROL
- Configuring port bandwidth
- Configuring TRUNK
- Configure super large frame
- Configuring redundant ports
- Configuring LLDP

3.1 Common configuration for ports

The administrator can switch off a port by configuring that port via the console port on the switch. If a user is not allowed to access the network via the port, the administrator can turn off the port.

This section describes the general configuration of the port, including:

- Opening and closing ports
- Port rate configuration
- Display port information

3.1.1 Port rate configuration

The default rate configuration for all ports is adaptive (autonegotiate).

The following command configures the port rate in the interface configuration mode:

- Speed { autonegotiate |full-1000 |full-100 |full-10 |half-100 |half-10 }
- Autonegotiate--- self-adaption
- Full-1000----- Full duplex Gigabit
- Full-100----- Full duplex fast
- Full-10 ----- Full duplex ten million
- Half-100----- Half duplex Gigabit
- Half-10----- Half duplex ten million

For example, the rate of port 1/1 is configured by full duplex 100M:

```
Switch(config-ge1/1)# speed full-100
```

3.1.2 Display port information

The following command displays information about one or more ports in common mode or privileged mode:

```
show interface [if-name]
```

For example, display port 1/1 information:

```
Switch# show interface ge1/1
```

For example, displays all ports information:

```
Switch# show interface
```

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

3.2 Configuring Port Mirroring

Port mirroring is a very useful function for monitoring the flow of packets received and sent by one or more ports. It can be used to mirror ports to monitor packets received and sent from one or more other ports. The switch supports port mirroring capabilities, mirroring the port's ability to monitor incoming data from other ports and the data that goes out. A mirrored port can monitor multiple ports at the same time. This section focuses on the configuration of MIRROR, including the following:

- Configuration of the MIRROR listen on port and is listening on port
- Display the configuration of MIRROR

3.2.1 Configuring the Port to listen to (MIRROR) and listening on a port

When the administrator configures the monitoring port, you need to enter the interface configuration mode to set up the monitored port. For example, setting port ge1/1 monitoring port ge1/2, you need to enter the port ge1/1 and type the command:

Switch(config-ge1/1)# mirror interface ge1/2 direction both

At this point, the port ge1/1 is set to the listening port, and the ge1/2 is set to the listening port. The command to set up the monitored port is as follows:

Switch(config-ge1/1)#mirror interface <if-name> direction {both | receive | transmit}

At this time, ge1/1 port is set to monitor port, <if-name> is set to be listening port, while behind the {both receive transmit} || pointed out the direction of monitoring: Receive represents the received packets; transmit monitors the packets sent; both monitors all packets sent and received. such as:

Switch(config-ge1/1)#mirror interface ge1/2 direction both

Represents the sending and receiving packets of the port ge1/1 monitoring port ge1/2.

If you want to set multiple monitored ports, you need to execute multiple commands.

In the interface configuration mode, the administrator can cancel the monitored port, and the command is as follows:

Switch(config-ge1/1)#no mirror interface <if-name> direction { receive | transmit}

When the <if-name> is no longer listening port, {receive | transmit} pointed out the direction is not listening: Receive indicates that the packet is not monitored; transmit indicates that the packet is not monitored. such as:

Switch(config-ge1/1)# no mirror interface ge1/2 receive

Indicates that the port ge1/1 no longer listens to the packets received by the port ge1/2.

When all the monitored ports are cancelled, the listening port will also be cleared.

3.2.2 Display the configuration of MIRROR

The administrator can view the configured MIRROR configuration through the following command in normal mode or privileged mode:

Switch# show mirror

The network manager should note following points:

- A port cannot be set as a mirror port and a mirrored port simultaneously.
- There can only be one port to monitor, but there are multiple ports to be monitored.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

3.3 Configuring STORM-CONTROL

In real life, a NIC card with a high rate of unicast, multicast, broadcast packets can cause a network failure, in this case the suppression function built into the switch is particularly important, it can prevent the packets going into the Network and causing congestion, all ports of the switch support the suppression of broadcast packets, multicast packets, and DLF packets.

This section gives a detailed description of the configuration of STORM-CONTROL, including the following :

- Default configuration
- Broadcast suppression configuration
- Multicast suppression configuration
- DLF suppression configuration
- Inhibition rate configuration
- Display STORM-CONTROL configuration

3.3.1 Default configuration

The switch supports setting broadcast, multicast, DLF switches for each port separately, and the three setting has a separate rate limit. The broadcast packet rejection of the default port is open, with a rejection rate of 64K. The purpose is to prevent the network from forming a broadcast storm. The DLF package and multicast package are not suppressed by default.

3.3.2 Broadcast suppression configuration

The following command configures the broadcast suppression of this port in the interface configuration mode:

storm-control broadcast

The following command cancels the broadcast suppression configuration for this port in the interface configuration mode:

no storm-control broadcast

3.3.3 Multicast suppression configuration

The following command configures multicast suppression for this port in the interface configuration mode:

storm-control multicast

The following command cancels the configuration of multicast suppression for this port in the interface configuration mode:

no storm-control multicast

3.3.4 DLF suppression configuration

The following command configures the DLF suppression of this port in the interface configuration mode:

storm-control dlf

The following command cancels the DLF suppression configuration of this port in the interface configuration mode:

no storm-control dlf

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

3.3.5 Inhibition rate configuration

The following command configures the inhibit rate of this port in the interface configuration mode:

```
storm-control ratelimit { broadcast | dlf | multicast } <1- 1048575 >
```

3.3.6 Display STORM-CONTROL configuration

The following command displays the STORM-CONTROL configuration in normal mode or privileged mode:

```
show storm-control
```

3.4 Configuring STORM-CONSTRAIN

Storm Constraint is a method used to control message storms on Ethernet. On ports with this function enabled they can detect the unicast traffic, multicast traffic and broadcast message traffic at the destination port at regular intervals. If a class of message traffic exceeds a preset upper limit threshold, the user can be configured to determine whether to block the port or to shut the port, and whether to send Trap and Log information.

When a certain type of message traffic exceeds the upper limit specified by the message, the system provides two processing methods:

(1) **Block:** if the port of unicast, multicast or broadcast in a message flow is greater than the upper threshold, the port will suspend forwarding the packets (other types of packet forwarding, as usual) port in the blocking state, but the port is still statistics of the kind of message flow. When this kind of message traffic is below the low threshold, the port will resume the forwarding this kind of message.

(2) **Shutdown mode:** if a class of unicast, multicast or broadcast on the port is larger than the upper limit, the port will be closed, and the system will stop forwarding all packets. The port state can be restored by executing the undo shutdown command, and it can also be restored by cancelling the port traffic threshold configuration.

Note: a certain type of message traffic, can be suppressed by the function or the storm suppression facility on the Ethernet port, but the two functions cannot be configured at the same time.

For example, the unicast traffic threshold control function and unicast storm suppression function cannot be configured at the same time.

The CLI configuration commands are as follows:

Command	Description	CLI mode
storm-constrain (broadcast multicast unicast) min-rate <1-1488100> max-rate <1-1488100>	Storm control for broadcast, multicast, or unknown unicast messages under the interface	Interface configuration mode
no storm-constrain (broadcast multicast unicast all)	Cancel storm control	Interface configuration mode
storm-constrain action (block shutdown)	Configure storm control actions and, without default, storm control for messages	Interface configuration mode
no storm-constrain action	Cancel the configured storm control action	Interface configuration mode
storm-constrain enable (log trap)	Switch to record or report	Interface

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

	alarm when storm control is opened	configuration mode
no storm-constrain enable (log trap all)	Switch to log or report alarm when storm control is closed	Interface configuration mode
storm-constrain interval <6-180>	Configure the storm control detection interval, by default, the storm control detection time interval is 5 seconds	Interface configuration mode
no storm-constrain interval	The detection interval of storm control is restored to the default value	Interface configuration mode
no storm-constrain	Delete the storm control function of the interface	Interface configuration mode
show storm-constrain	View storm control information for all interfaces	Privileged mode
show storm-constrain interface IFNAME	View the storm control information of the interface	Privileged mode

Configuration specification :

(1) View the storm control information description table of the interface

Project	Description
interface	Interface name
type	Message type (1) broadcast- broadcast message; (2) multicast-multicast message; (3) unicast- unicast message
rate	Min- low threshold; max- high threshold
action	Storm control actions include (1) block- blocking messages; (2) shutdown- closing the interface
punish-status	The message state of the current interface includes (1) block- when the speed is greater than max-rate and the storm control action is a blocking message, the state is a blocking message; (2) Normal - normal forwarding; (3) shutdown-When the rate is greater than max-rate and the storm control action is to close the interface, the state is closed interface
trap	Alarm switch status, on/off
log	Log switch status, on/off
interval	The detection interval of storm control is in seconds, and the default value is 5 seconds
last-punish-time	Finally, the time of storm control punishment

(2) **By executing the storm-** we configure the action for storm control, and executing the storm-constrain command configures the high-low threshold for storm control, the storm message can be controlled to prevent flooding. In the storm control detection interval, when the average rate of broadcast, multicast, or unicast packets on the interface is greater than the specified threshold, the

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

storm control will block the packets according to the configuration or shut down the interface. When the storm control action is blocked, if the traffic is below the minimum threshold, the interface resumes to the normal forwarding state. When the storm control action is closed, the interface cannot be restored automatically. You need to manually execute the no shutdown command to restore the interface. Port storm control shutdown action configuration to restore. (3The port traffic exceeds the upper threshold or falls from the upper limit to the lower threshold. Output log / trap information

3.5 Configuring FLOW-CONTROL

FLOW-CONTROL (flow control) is used to prevent packet loss in the case of port blocking. In half duplex mode, the flow control is achieved by back pressure (Backpressure), which reduces the sending speed from the source of the information. In full duplex mode, the flow control follows the IEEE802.3x standard. The blocking port sends the "Pause" packet to the information source to suspend the transmission.

This section gives a detailed description of the configuration of FLOW-CONTROL (flow control), including the following :

- Default configuration
- Set port receive and send side flow control
- Closed port flow control
- Display flow control information

3.5.1. Default configuration

The switches support flow control for sending and receiving data on r each port. The default port does not open the flow control function.

3.5.2. Set port receive and send side flow control

The following command configures the port receive and send side flow control in the interface configuration mode:

```
flowcontrol
```

3.5.3. Closed port flow control

The following command closes the port send and receive side flow control in the interface configuration mode:

```
no flowcontrol
```

3.5.4 Display flow control information

The following command displays flow control information for all ports in normal mode or privileged mode:

```
show flowcontrol
```

The following command displays the flow control information of a port in common mode or privileged mode:

```
show flowcontrol interface <if-name>
```

Among them, <if-name> is the port name to query flow control information.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

3.6 Configuring port bandwidth

Port bandwidth control is used to control the rate of port sending and receiving.

This section gives a detailed description of the port bandwidth configuration, including the following:

- Default configuration
- Set port send or receive bandwidth control
- Cancellation of port transmit or receive bandwidth control
- Bandwidth control of display port configuration

3.6.1 Default configuration

The switches support sending and receiving bandwidth to each port, respectively. The default port does not support bandwidth control.

3.6.2 Set port send or receive bandwidth control

The following command sets the port to send or receive bandwidth control in the interface configuration mode:

portrate {egress | ingress} <rate>

Egress represents bandwidth control over packets sent.

Ingress represents bandwidth control of the received packets.

<rate> said to set the bandwidth value range is 11024000, unit is kbits.

3.6.3 Cancellation of port transmit or receive bandwidth control

The following command cancels the bandwidth control of the port in the interface configuration mode:

no portrate {egress | ingress}

Egress represents bandwidth control to cancel sending packets.

Ingress represents the bandwidth control of the cancelled packet.

3.6.4 Bandwidth control of display port configuration

The following command looks at bandwidth control of port configuration in common mode or privileged mode:

show portrate interface <if-name>

<if-name> is the port name to query bandwidth control information.

3.7 Configuring Trunks

A trunk is the integration of multiple ports into a single logical port, which can be used to increase bandwidth, provide redundant backup connections and can also be used for load balancing. When the TRUNK group is used as the logical output port, the switch will send a packet from the port group by selecting a port according to the aggregation policy set by the user. The configuration of port and aggregation strategy in the TRUNK group is undertaken by software, but the forwarding of the data stream is accomplished by hardware.

All ports in the TRUNK group must be configured at the same speed, and in full duplex mode. switches can support up to 8 groups in each TRUNK.

Each port can only belong to one TRUNK group.

The LACP protocol is a protocol based on the IEEE802.3ad standard. LACP protocol interacts

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

with the client via LACPDU (Link Aggregation Control Protocol Data Unit).

The interface in the aggregation group enables the LACP protocol. The interface advertises the LACP protocol priority, the system MAC address, the LACP priority of the port, the port number, and the operation key to the peer through the LACPDU. After receiving the LACPDU, the peer compares the information with the information received by other interfaces to select the interface that can be in the selected state, so that the two parties can agree on the interface in the selected state.

The operation key is a configuration combination that is automatically generated according to some configurations of member ports during link aggregation. It includes port rate, duplex mode, up / down status, VLANs allowed on port, VLAN default VLAN ID , The link type of the port (that is, Trunk, Hybrid, Access type) and so on. In the aggregation group, the member ports in the selected state have the same operation Key.

This section gives a detailed description of the configuration of TRUNK, including the following:

- LACP protocol configuration
- Configuration of TRUNK group
- TRUNK group member port configuration
- TRUNK load balancing policy configuration
- Display a TRUNK

3.7.1 LACP protocol configuration

Command	Description	CLI mode
lacp system-priority <1-65535>	Setting priority of LACP system	Global configuration mode
no lacp system-priority	Restore system priority defaults 32768	Global configuration mode
lacp max-active-link-number <1-8>	Set LACP to activate the upper bound of the polymerization port	Global configuration mode
no lacp max-active-link-number	Restore LACP to activate aggregate port default limit 8	Global configuration mode
lacp port-priority <1-65535>	Set LACP port priority	Interface configuration mode
no lacp port-priority	Restore port priority defaults 32768	Interface configuration mode
lacp timeout (short long)	Set LACP port timeout, missing governor timeout	Interface configuration mode
show lacp summary	Shows all the simple things about LACP polymerization	Privileged mode
show lacp detail	Show all the LACP polymerization scenarios	Privileged mode
show lacp <1-8>	Details of the LACP polymerization port are shown	Privileged mode
show lacp port IFNAME	Show the details of the LACP port	Privileged mode
show lacp system-id	Display the LACP system	Privileged

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

		mode
show lacp counter <1-8>	Show the statistics of LACP polymerization port	Privileged mode
show lacp counter	Show the statistics of all LACP ports	Privileged mode
clear lacp <1-8> counters	Clear the statistics of LACP polymerization port	Privileged mode
clear lacp counters	Clear statistics of all LACP ports	Privileged mode

3.7.2 Configuration of a TRUNK group

The following command creates a manual TRUNK group in global configuration mode:

trunk <trunk-id>

To create a TRUNK group, use <trunk-id>

The allowable value range is 1-8, indicating the TRUNK group ID number with 8 as the maximum;

After successfully creating the TRUNK group interface name is trunk+id, with the id being the number you just assigned.

You can configure the mode using the "interface trunk+id" command to enter the interface configuration mode, and then select the TRUNK group. For example use the interface command interface mode trunk1, TRUNK 1, to configure TRUNK 1.

The following command creates a static LACP TRUNK group in global configuration mode:

trunk <1-8> dynamic

The following command deletes a TRUNK group in global configuration mode:

no trunk <trunk-id>

When you delete a TRUNK group, you must ensure that the TRUNK group does not have any member ports.

3.7.3 TRUNK group member port configuration

The following command in the interface configuration mode for new members of TRUNK port:

trunk interface IFNAME (passive)

<if-name> is the port name that needs to be added to the TRUNK group and must be the two layer interface. Each group of TRUNK can add 8 two layer interfaces at most. If the TRUNK group is a static LACP TRUNK group, the add interface defaults to the active state and can be configured as a passive state.

The following command deletes all the member ports of the TRUNK group in the interface configuration mode: **no trunk interface**

The following command deletes the specified TRUNK group member port in the interface configuration mode: **no trunk interface <if-name>**

You can use this command multiple times to delete the multiple member ports of the TRUNK group.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

3.7.4 TRUNK load balancing policy configuration

The following command sets the load balancing policy of TRUNK in the interface configuration mode:

```
trunk load-balance {dst-mac | dst-ip | src-dst-mac | src-dst-ip | src-mac | src-ip}
dst-mac----- Equilibrium strategy based on objective MAC
dst-ip----- Equilibrium strategy based on objective IP
src-dst-mac--- Equilibrium strategy based on source MAC and destination MAC
src-dst-ip----- Equilibrium strategy based on source IP and destination IP
src-mac----- Equilibrium strategy based on source MAC
src-ip----- Equilibrium strategy based on source IP
```

The following command sets the default TRUNK load balancing policy in the interface configuration mode:

no trunk load-balance

The default port load balancing policy is src-dst-mac (a balanced strategy based on source MAC and destination MAC).

3.7.5 Display of TRUNK

The following command looks at all TRUNK group configurations in common mode or privileged mode:

show trunk

The following command looks at the specified TRUNK group configuration in common mode or privileged mode:

show trunk <trunk-id>

<trunk-id> is the ID number of the TRUNK group to be checked.

3.8 Configure super large frame

3.8.1 Oversize introduction

The port can be configured to receive super large frame, you can set the port to support the specific super frame length.

3.8.2 Oversize configuration

The port configuration supports super frame length, in config mode, into the port configuration mode, such as interface ge1/1, execute the following command:

Switch(config-ge1/1)# jumbo frame 2000

Super large frame length supported by display portSwitch#show jumbo frame ge1/1

Port	Jumbo frame(bytes)
ge1/1	2000

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

3.9 Configuring redundant ports

In some special cases, such as the need to focus on the protection of certain servers linked to the stability of the network, the switch's redundant port can provide two ports linked to the server, and to ensure that at a time the server only one LINK UP is operational in the network , When a port occurs LINK DOWN, the system immediately enable another port.

When a port in the redundant port group in the LINK UP, we call the Active state; the other hand, if a redundant port group in the LINK DOWN, we call the Disable state.

This section focuses on the configuration of redundant ports, including the following :

- Configuration of redundant ports
- Display of redundant ports

3.9.1 Configuration of redundant ports

It's possible to configure 8 sets of redundant ports, a group of redundant ports can only consist of 2 ports; one port can only be configured to a redundant port group.

A redundant port group can configure a primary-port and secondary-port. When configuring redundant port groups:

1. When the two ports are in the LINK UP state at the same time, the primary-port is set to the Active state, and the secondary-port is placed in the Disable state ;
2. If only one port is in the LINK UP state, the current LINK UP port is set to the Active state, and the other port is in the Disable state ;
3. Otherwise, the two ports are out of the Disable state.

If the Active port fails, then another port will be configured to go into the Active state.

There is also a configuration parameter called 'force-switch', which is when the secondary-port in the Active, primary-port has been Disabled. If the primary-port LINK UP event occurs when the decision to re-switch to primary-port. For Active, secondary-port is in the Disable state. If the 'force-switch' command is enabled, then it is forced to switch, otherwise the port state of the original redundant port group will be retained.

Command	Description	CLI mode
redundant-port <1-8> primary-port IFNAME secondary-port IFNAME [force-switch]	Configuring a group of redundant ports, <1-8> is a group of primary-port IFNAME is the name of the main port interface, Secondary-port IFNAME is the alternate port interface name, Does force-switch use a mandatory toggle switch?	Global configuration mode
redundant-port <1-8> force-switch	Mandatory switch with redundant ports.	Global configuration mode
no redundant-port <1-8>	Delete redundant port groups.	Global configuration mode
no redundant-port <1-8> force-switch	Forced switch for closing redundant ports.	Global configuration mode

3.9.2 Display of redundant ports

Commands to display redundant ports

Command	Description	CLI mode
show redundant-port	Configuration of all redundant port groups in the display system	Privileged mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

3.10 Configuring LLDP

The numbers and types of network device are increasingly numerous and their configuration is complex. In order to enable different vendors' devices to discover and interact with each other in the network, they need a standard information exchange platform.

LLDP (Link Layer Discovery Protocol) is the protocol used to provide this facility, it provides a standard link layer discovery, the local equipment can be the main ability, management address, device identification, interface identification and other information organization (Type / Length / Value), and encapsulated in the LLDPDU (Link Layer Discovery Protocol Data Unit) issued to the neighbours directly connected with their neighbours to receive this information after the standard MIB (Management Information Base) allowing a network management system to query and determine the link status of the communication.

This section focuses on the configuration of LLDP, including the following:

- LLDP configuration
- LLDP display

3.10.1 LLDP configuration

There are 4 types of LLDP port working modes:

- TxRx: send and receive LLDP message.
- Tx: send only not receive LLDP message.
- Rx: only receive not send LLDP message.
- Disable: neither sends nor receives LLDP messages.

When the port's LLDP operating mode changes, the port will initialise the protocol 'state machine'. In order to avoid the frequent change of port operation mode, causing the port to perform an initialisation operation continuously, the configurable port initialisation delay time is delayed and the initialization operation is delayed when the port operation mode changes.

Command	Description	CLI mode
lldp global enable	LLDP global enable command.	Global configuration mode
lldp hold-multiplier <num>	Lldp TTL multiples.	Global configuration mode
lldp timer [<reinit-delay><time>][< tx-delay><time>][< tx-interval ><time>]	Configure LLDP various timers.	Global configuration mode
lldp enable	Enable interface LLDP	Interface configuration mode
lldp admin-status{ disable rx tx rxtx }	Configuring the LLDP port mode of operation.	Interface configuration mode
lldp check-change-interval <time>	Configuring refresh interface information interval	Interface configuration mode
lldp management-address <A.B.C.D>	Configuring the interface LLDP to manage the address	Interface configuration mode
lldp tlv-enable{ dot1-tlv dot3-tlv med-tlv }	Configure interface LLDP extended capability set switch	Interface configuration mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

3.10.2 LLDP display

LLDP command

Command	Description	CLI mode
show lldp configuration [ifname]	Display lldp configuration information	Privileged mode
show lldp local-information [ifname]	Display lldp local information	Privileged mode
show lldp neighbor-information [ifname]	Display lldp neighbor information	Privileged mode
show lldp statistics [ifname]	Display lldp message statistics	Privileged mode
show lldp status [ifname]	Display lldp status information	Privileged mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

4 Port based MAC security

This chapter introduces the port based MAC security configuration, including the following contents:

- Brief introduction
- MAC binding configuration
- MAC filter configuration
- Port learning constraint configuration

4.1 Brief introduction

Port based MAC security can provide three functions for MAC binding, MAC filtering and port learning control, to improve the security performance of the two layer forwarding of the switch.

MAC binding - can be a combination of the MAC address and port together, limiting a specified MAC address to only be in a specified port to access the network; the same time, the port can only allow these binding MAC address to access the network; a port can simultaneously Bind multiple MAC addresses. MAC binding can be applied to a designated port at the same time as 802.1x. This function is very useful for some devices that do not have 802.1x functionality or are not convenient to use 802.1x devices, such as printers, file servers, etc.

MAC filtering - allows some designated MAC addresses to prevent access the network. The main purpose is to prevent illegal devices from accessing the network. When an MAC address is configured as a MAC filter, the MAC address cannot be accessed at any port on the switch in the network, also cannot receive the purpose of MAC is the specified MAC address data packets, and MAC binding, a port can also configure multiple MAC address filtering. In applications, if virus software attacks the network through a forged MAC address, besides ACL, the attack of controlling these forged packets can be accessed by MAC filtering.

Port learning control can control a port to dynamically learn the number of MAC addresses. If a port specifies that it can dynamically learn the number of MAC addresses, when the number of MAC addresses learned by this port is equal to the number in the port configuration, the new MAC address will no longer be learned and the packets will be discarded.

It's important to note that the MAC address here is actually MAC+VID.

In addition, the MAC binding function and 802.1x can be configured on one port at the same time. MAC filtering and port learning limit can be configured on one port at the same time. The MAC binding function, 802.1x and MAC filtering, port learning limit between the two groups cannot be simultaneously configured to the same port.

4.2 MAC binding configuration

The MAC binding configuration supports manually binding MAC addresses and automatically binding MAC addresses. Manual binding MAC address is configured via the user through the command one by one input MAC address and port binding. Automatically binding the MAC address is to read the existing entries of the port in the two layer hardware forwarding table, and directly bind the MAC address. The command to read the two layer hardware table is Show bridge FDB.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Configuration commands

Command	Description	CLI mode
switchport-security mac-bind HHHH.HHHH.HHHH vlan <1-4094>	Manually bind a MAC address to an interface.	Interface configuration mode
switchport-security mac-bind auto-conversion number <1-16383>	Automatically converts a specified number of MAC addresses to a MAC binding configuration.	Interface configuration mode
switchport-security mac-bind auto-conversion vlan <1-4094>	Automatically converts a MAC address of a specified VLAN to a MAC binding configuration.	Interface configuration mode
show port-security mac-bind [IFNAME]	Display MAC binding configuration	Privileged mode

Note:

The reason for invalid or failed MAC address binding may be as follows:

The port has been configured with 802.1x

The port has been configured with MAC filtering or configured port learning restrictions;

The MAC address has been bound to other ports, or configured with MAC filtering;

The L2 table of the switch is full.

4.3 MAC filter configuration

The MAC filter configuration supports manually binding MAC addresses and automatically binding MAC addresses. Manual configuration of MAC filter is the user through the command input one by one to filter the MAC and port binding. Automatic configuration MAC filtering is to read the existing entries of the port in the two layer hardware forwarding table, and directly configure the MAC filter. The command to read the two layer hardware table is Show bridge FDB.

Command	Description	CLI mode
switch port-security mac-filter HHHH.HHHH.HHHH vlan <1-4094>	Manually configure an interface for MAC filtering	Interface configuration mode
switch port-security mac- filter auto-conversion number <1-16383>	Automatically converts a specified number of MAC addresses to a MAC filter configuration	Interface configuration mode
switch port-security mac-filter HHHH.HHHH.HHHH vlan <1-4094>	Automatically converts the MAC address of a specified VLAN of an interface to the MAC filter configuration	Interface configuration mode
show port-security mac-filter [IFNAME]	Display MAC binding configuration	Privileged mode

Note:

The reason for invalid or failed MAC filter configuration may be as follows:

The port has been configured with MAC bindings or enabled the 802.1x protocol function;

The MAC address has been bound to other ports, or configured with MAC bindings;

The L2 table of the switch is full.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

4.4 Port learning constraint configuration

The Case Communications Layer 3 switches can be configured to limit the maximum number of dynamic learning addresses per port. If a port is configured to restrict the maximum number of dynamic learned MAC address, then the port can only learn the corresponding number of MAC address, when beyond this number of MAC address, then it stops learning and forwarding. With no learning constraints, a port can learn at most 16383 MAC addresses.

Configuration command

Command	Description	CLI mode
switchport port-security learn-limit <0-16383>	Configure the number of MAC addresses that an interface can learn.	Interface configuration mode
no switchport port-security learn-limit	Deletes the number of MAC addresses that an interface can learn.	Interface configuration mode
show port-security learn-limit [IFNAME]	Display port learning configuration	Privileged mode

Configuration example

Configuring port ge1/5 can only learn 7 MAC addresses

Switch#configure terminal

Switch(config)interface ge1/5

Switch(config-ge1/5)switchport port-security learn-limit 7

Note:

The reasons for invalid or failed port learning may be as follows:

The port has been configured with MAC bindings or enabled the 802.1x protocol function.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

5. Port IP and MAC binding

This chapter introduces the port IP and MAC binding configuration, including the following contents:

- Brief introduction
- IP and MAC binding configurations
- Configuration example
- Configuration misarrangement

5.1 Brief introduction

Configuring IP and MAC binding on Layer 2 switch ports provides defence against ARP attacks. ARP attackers attack users MAC addresses by sending ARP messages with false MAC addresses, which causes the local ARP cache table to be covered with the attacker's address so that the normal data flows to the attacker. In the switch port configuration command static binding user IP address and MAC address can effectively filter ARP attack packets.

In addition to the anti-ARP spoofing function, IP MAC binding function can protect the IP and MAC using a one by one mapping relationship, that is an IP can only correspond to a MAC, and MAC can only correspond to an IP. If an incoming device modifies this mapping then it will not be able to communicate in this network. 802.1x anti ARP spoofing function and DHCP SNOOPING protocol are dynamic implementations of this function.

The four functions of IP MAC binding, ACL, 802.1x anti ARP spoofing and DHCP SNOOPING all use the same system resource CFP and pay attention to whether the resources of CFP are exhausted when configuring. We have developed a compatibility relationship between them in the design. Following table:

	IP MAC binding	ACL	802.1x	DHCP SNOOPING
IP MAC binding	compatible	Incompatible	compatible	compatible
ACL	Incompatible	compatible	Incompatible	Incompatible
802.1x	compatible	Incompatible	compatible	Incompatible
DHCP SNOOPING	compatible	Incompatible	Incompatible	compatible

CFP is a limited hardware resource where each port can only be configured with 16 IP MAC binding entries, so is used in a network if it only has a few ports or a small number of IP and MAC addresses that need to be controlled. If so then you can use static the IP MAC binding function.

Avoiding CFP function exhaustion leads to data forwarding failure.

In addition, if you use 802.1x or DHCP SNOOPING protocol, or if you use a static IP address configuration and the 802.1x protocol to access the network, the 801.1x anti-ARP spoofing can also be effective. If you're using a dynamic access to IP address then use the DHCP SNOOPING protocol.

5.2 IP and MAC binding configurations

IP binds to MAC in the interface mode configuration

- Configuring port IP and MAC binding **Switch#configure terminal**
- **Switch(config)#interface ge1/1**
- **Switch(config-ge1/1)#ip mac-bind A.B.C.D MAC**

Delete port IP and MAC binding

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

- **Switch#configure terminal**
- **Switch(config)#interface ge1/1**
- **Switch(config-ge1/1)#no ip mac-bind A.B.C.D MAC**

Display configuration

Displays the bound entries of all ports

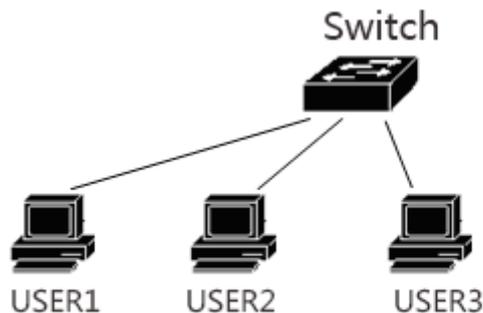
show ip mac-bind

Displays the binding table entry of an interface

show ip mac-bind IFNAME

5.3 Configuration example

There are 3 users in the network, USER12, USER2 and USER3 and the IP and MAC of the user are bound at the port, to defend against the ARP attacks.



```

Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#ip mac-bind 192.168.1.100 0011.5b34.42ad
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#ip mac-bind 192.168.1.101 0011.6452.135d
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#ip mac-bind 192.168.1.102 0011.804d.a246
Switch(config-ge1/3)#end
Switch#show ip mac-bind
[ge1/1] sum: 1
    MAC                IP
    0011.5b34.42ad     192.168.1.100
[ge1/2] sum: 1
    MAC                IP
    0011.6452.135d     192.168.1.101
[ge1/3] sum: 1
    MAC                IP
    0011.804d.a246     192.168.1.102
Switch#show ip mac-bind ge1/1
[ge1/1] sum: 1
    MAC                IP
    0011.5b34.42ad     192.168.1.100
Switch#show running-config
  
```

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

```

!
spanning-tree mst configuration
!
Interface vlan1
ip address 192.168.0.1/24
!
interface ge1/1
ip mac-bind 192.168.1.100 0011.5b34.42ad
!
interface ge1/2
ip mac-bind 192.168.1.101 0011.6452.135d
!
interface ge1/3
ip mac-bind 192.168.1.102 0011.804d.a246
!
line vty
!
End

```

5.4 Configuration misarrangement

If the IP MAC binding configuration fails, it may be caused by the following reasons:

1. System CFP resource exhaustion.
2. The current interface is configured with the ACL filter function.
3. The configured interface is a three layer interface or a TRUNK interface.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

6. VLAN CONFIGURATION

A VLAN is an important concept in networks and it is used in many practical applications. It allows the internal division of multiple networks on the switch. VLAN is the abbreviation of Virtual Local Area Network (LAN). It is a network that logically connects multiple devices, regardless of the physical location of the device. Each VLAN is a logical network, which has all the functions and attributes of the traditional physical network. Each VLAN is a broadcast domain, broadcast packets can only be forwarded within a VLAN, cannot cross to a different VLAN. VLAN data communication must be transmitted through three layers.

The main contents of this chapter are as follows:

- VLAN introduction
- VLAN configuration
- VLAN configuration example
- MAC, IP subnet, protocol VLAN
- VOICE VLAN
- VLAN mapping
- QINQ

6.1 VLAN introduction

This section gives a detailed introduction to VLAN, including the following contents:

- The benefits of VLAN
- VLAN ID
- VLAN port member type
- Default VLAN of port
- Port VLAN mode
- VLAN relay
- Data flow is forwarded in VLAN

6.1.1 The benefits of VLAN

VLANs greatly extend the scale of a physical network. The traditional physical network can only be built on a scale maybe supporting thousands of devices, while the physical network using VLANs can accommodate tens of thousands or even hundreds of thousands of devices. VLAN has the same function and attribute as the traditional physical network.

The use of VLAN has the following advantages:

- VLAN can effectively control the traffic in the network.

In traditional networks, all broadcast packets are transmitted to all devices, increasing the load on the network and equipment. A VLAN can organize the devices into a logical network and VLAN broadcast domain, broadcast packets are only transmitted within the VLAN, not across the VLAN. By dividing the VLAN the traffic in the network can be effectively controlled.

- VLAN can improve the security of network.

VLAN equipment only works at two levels with communication equipment.

If you want to communicate with another VLAN, data must be forwarded through the three layers. Therefore we are required to allow the data through 3 layers between the VLANs if not then no communication can occur between the VLANs. This allows VLANs to ensure isolation, to and VLAN data security.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

- VLAN makes the device easy to move.

In the traditional network, if the device moves from one location to another, and belongs to different networks, it is necessary to modify the network configuration of the mobile device, which is very inconvenient for the user. VLAN is a logical network and can be put in the same physical location of the equipment designated in the same network, when the mobile device can also make the equipment belonging to the VLAN, so the mobile device does not need to modify any configuration.

6.1.2 VLAN ID

Each VLAN has an identification number, called VLAN ID (VID). The range of VLAN ID ranges from 0 to 4095, of which 0 and 4095 are not used, and the actual efficiency is only 1 to 4094. VLAN ID uniquely identifies a VLAN.

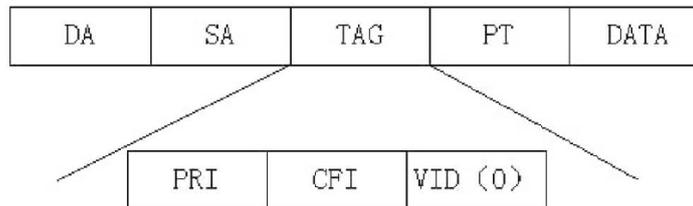
Your Case Communications RT Layer 3 Series Switch supports 4094 VLANs and when you create a VLAN, you choose a VLAN ID ranging from 2 to 4094. Switches create VLAN1 by default and VLAN1 cannot be deleted.

There are three kinds of data frames transmitted in a VLAN network: A data frame without tags, a data frame with VID 0, a data frame with VID 0 Non marked. As shown below, there are three different formats of data frames.

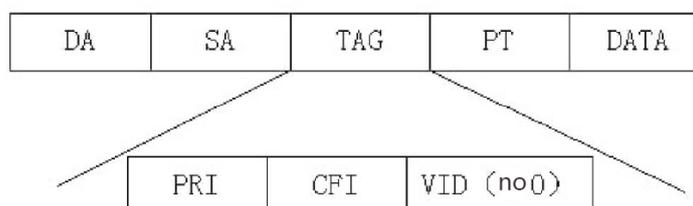
Marker free data frame



Tagged data frame, but VLAN ID is 0



Tagged data frames, but VLAN ID is not 0



All data frames within a switch are marked. If a marker free data frame is entered into the switch, the switch adds a tag to the data frame and selects a VLAN ID value to fill in the marked VID. If a data frame with VID 0 is entered into the switch, the switch selects a VLAN ID value to fill in the marked VID. If a data frame with VID non 0 tag is input to the switch, the frame remains unchanged.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

6.1.3 VLAN port member type

The Case Communications RT Layer 3 Switches support port based VLAN and 802.1Q based VLAN. A VLAN consists of two port member types: untagged members and tagged members. A VLAN can include both an untagged port member and a tagged port member.

A VLAN can have no port member and can also have one or more port members. When a port belongs to a VLAN, it can be a member of the VLAN as either a tagged or untagged member. A port can belong to one or more VLAN tagged or untagged members. If a port belongs to two or more tagged members of VLAN, this port is also called the VLAN relay port. A port can also belong to one or more untagged members of VLAN and to tagged members belonging to another or more VLAN.

6.1.4 Default VLAN of port

The port has only one default VLAN, and the default VLAN is used to determine the VLAN tag that any packet that enters requiring a tag will have. The default VLAN is also referred to as Port VID or PVID. By default, the default VLAN of a port is 1.

6.1.5 Port VLAN mode

There are three VLAN modes possible on the ports: ACCESS mode, TRUNK mode and HYBRID mode. When the user configured the port to be a member of a VLAN, the VLAN mode of the port must first be specified.

ACCESS mode - is an access port, which is directly connected to a user. The port can only belong to an untagged VLAN member or a tagged VLAN Member, and the default VLAN is the user specified VLAN.. The Port can provide a VLAN Tag to an untagged user coming in via the Access Port.

TRUNK port - is a trunk port, and the switch is directly connected to another switch with a tagged port or equipment that has tagged VLAN enabled. The port can belong to one or more VLAN members with tagged VLAN but does not belong to any untagged VLANs.

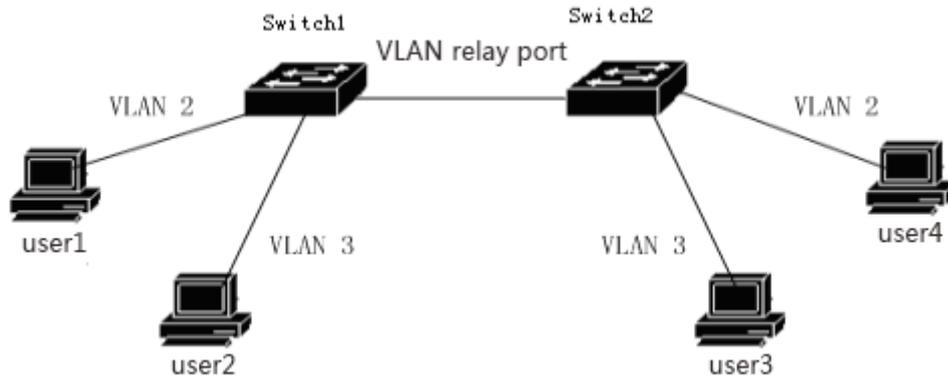
HYBRID port – is a port that is a relay port, which is directly connected to the switch. The port can belong to one or more tagged members of the VLAN and / or one or more untagged members of the VLAN. The default VLAN of this port can be changed.

In practical application, the user can select the VLAN mode of the port according to the specific situation.

6.1.6 VLAN relay

If a port belongs to two or more tagged members of VLAN, then this port is also called the VLAN relay port. The two switches can be connected to the VLAN relay port, so that the two switches can be divided into two or more common VLAN.

The diagram below shows a VLAN relay for example, between two switches connected to VLAN relay port, VLAN 2 and VLAN 3 relay port, each switch is divided into two VLANs respectively, VLAN 2 and VLAN 3, each VLAN has a user. In this way, user 1 can communicate with the user 3, and the user 2 can communicate with the user 4 and the user 1 and the user 3 cannot communicate with the user 2 and user 4.



6.1.7 Data flow is forwarded in VLAN

When the switch receives a packet from one port, the data is forwarded in two steps, according to the following :

- Determines the VLAN to which the packet belongs.
- Determine whether the packet is broadcast data packet, multicast packet or unicast packet.
- According to different packets to determine the output port (can be zero, one or more output ports), if there is no output port, discard the packet.
- Send out from the output port.

1) How to determine the VLAN of a packet:

If the data packet label is received and the VID field in the tag is not 0, the VLAN to which the packet belongs is the VID value in the tag.

If the received packet is not marked or marked, but the VID value in the tag is 0, the VLAN of the packet belongs to the default VLAN of the port.

2) How to determine the type of packets:

If the destination MAC address of the received packet is FF:FF:FF:FF:FF:FF, the packet is a broadcast packet.

If the received packets are not broadcast packets and the fortieth (40th) bits of their destination MAC addresses are 1, then the packets are multicast packets.

If it is neither a broadcast packet nor a multicast packet, the packet is a unicast packet.

3) How to determine the output port of a packet:

If the input packet is a broadcast packet, all the member ports of the VLAN to which the packet belongs is the output port of the packet.

If the input data packet is multicast data packets, according to the purpose of multicast MAC address and the VLAN for the two layer hardware multicast forwarding table entries, if found, is multicast, multicast entries in the output port and an VLAN member of the port in the common port (and operation) as the output port packet and if there is no common port, the packet is discarded. If the two hardware multicast forwarding multicast, find no entries in the table, according to the two layer multicast forwarding mode hardware forwarding decision output port, if it is not registered in the multicast forwarding mode, multicast packets as radio treatment, the VLAN of all members of the port are packet output ports, if the forwarding mode is registered no, the output port, the data packet discard.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

If the input data packet is unicast packets, according to the VLAN to find the two-hardware destinations MAC address and the forwarding table, if it finds a match, then the output port of entry and the members of the VLAN port in the common port (and operation) for the data packet output port, if not the common port, the packet is discarded. If no matching entries are found in the two layer hardware forwarding table, the packet is treated as a broadcast packet, and all the member ports of the VLAN belong to the output port of the packet.

4) Send data packet:

The output port of the incoming packet has decided to send the packet out to all the output ports. If an output port is an untagged member of the VLAN that belongs to the packet, the packet is not marked when it is sent from the output port.

If an output port is a tagged member of the VLAN that belongs to the packet, the packet is tagged when it is sent out of the output port, and the VID value in the tag is the value of the VLAN to which the packet belongs.

6.2 VLAN configuration

This section gives a detailed introduction to the configuration of VLAN, including the following:

- Creating and deleting VLAN
- Configuring port VLAN mode
- VLAN configuration of ACCESS mode
- VLAN configuration of TRUNK mode
- HYBRID mode VLAN configuration
- View VLAN information

6.2.1 Creating and deleting VLAN

Before creating and deleting VLAN, users need to use the VLAN database command in the global configuration mode to enter the VLAN configuration mode and create and delete VLAN in this mode.

The system has created VLAN 1 by default, and VLAN 1 cannot be deleted by the user. The commands for creating and deleting VLAN are as follows:

Command	Description	CLI mode
vlan <vlan-id>	Create a VLAN. If the VLAN already exists, it does not do the processing, otherwise the VLAN is created. Parameters range from 2 to 4094.	VLAN configuration mode
no vlan <vlan-id>	Delete a VLAN, if the VLAN does not exist, do not do processing, otherwise delete the VLAN. Parameters range from 2 to 4094.	VLAN configuration mode

6.2.2 Configuring port VLAN mode

Before configuring the port VLAN, you need to specify the VLAN mode of the port. By default, the VLAN mode of the port is ACCESS mode. The VLAN mode command of the specified port follows the table:

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Command	Description	CLI mode
switchport mode access	The VLAN mode of the specified port is ACCESS mode. After executing this command, the port is the untagged member of VLAN1, and the default VLAN of the port is 1.	Interface configuration mode
switchport mode trunk	The VLAN mode of the specified port is TRUNK mode. After executing this command, the port is the tagged member of VLAN1, and the default VLAN of the port is 1.	Interface configuration mode
no switchport trunk	The VLAN mode of the port is no longer TRUNK mode, back to the default, that is, the ACCESS mode.	Interface configuration mode
switchport mode hybrid	The VLAN mode of the specified port is HYBRID mode. After executing this command, the port is the untagged member of VLAN1, and the default VLAN of the port is 1.	Interface configuration mode
no switchport hybrid	The VLAN mode of the port is no longer HYBRID mode, back to the default, that is, the ACCESS mode.	Interface configuration mode

6.2.3 VLAN configuration of ACCESS mode

Before the port is configured for VLAN, the VLAN mode of the port should be specified as the ACCESS mode. In this VLAN mode, the port defaults to an untagged member of VLAN1 and the default VLAN of the port is 1. The VLAN configuration command of ACCESS mode is as follows:

Command	Description	CLI mode
switchport access vlan <vlan-id>	The configuration port is the untagged member of the specified VLAN, and the default VLAN of the port is the specified VLAN. Parameters range from 2 to 4094.	Interface configuration mode
no switchport access vlan	The VLAN configuration of the port goes back to the default, that is, the port is the untagged member of VLAN1, and the default VLAN of the port is 1.	Interface configuration mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

6.2.4 VLAN configuration of TRUNK mode

Before the port is configured for VLAN, the VLAN mode of the port should be specified as the TRUNK mode. In this VLAN mode, the port defaults as a tagged member of VLAN1 and the default VLAN of the port is 1. The VLAN configuration command of TRUNK mode is as follows:

Command	Description	CLI mode
switchport trunk allowed vlan all	The configuration port is the tagged member of all VLAN. For the newly created VLAN, the port is also the tagged member of these VLAN.	Interface configuration mode
switchport trunk allowed vlan none	Except for VLAN1, the port is no longer a member of all other VLAN tagged.	Interface configuration mode
switchport trunk allowed vlan add <vlan-list>	Configure the port to be the tagged member of the specified one or more VLAN. The parameter <vlan-list> can be a VLAN, a VLAN range or a plurality of VLAN. For example, the parameters can be "1", "2-4" or "1,3,5".	Interface configuration mode
switchport trunk allowed vlan remove <vlan-list>	The port is cleared from the specified one or more VLAN and is no longer the tagged member of these VLAN. The parameter <vlan-list> can be a VLAN, a VLAN range or a plurality of VLAN. For example, the parameters can be "1", "2-4" or "1,3,5".	Interface configuration mode

6.2.5 HYBRID mode VLAN configuration

Before the port is configured for VLAN, the VLAN mode of the port should be specified as the HYBRID mode. In this VLAN mode, the port defaults as a tagged member of VLAN 1 and the default VLAN of the port is 1. The VLAN configuration command of HYBRID mode is as follows:

Command	Description	CLI mode
switchport hybrid vlan <vlan-id>	The configuration port is the untagged member of the specified VLAN, and the default VLAN of the port is the specified VLAN. Parameters range from 2 to 4094.	Interface configuration mode
no switchport hybrid vlan	The port is cleared from the default VLAN, no longer the default VLAN's tagged or untagged member, and the	Interface configuration mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

	default VLAN of the port returns to 1.	
switchport hybrid allowed vlan all	Configuration ports are all tagged members except VLAN (except VLAN1). For the newly created VLAN, the port is also the tagged member of these VLAN.	Interface configuration mode
switchport hybrid allowed vlan none	Except for VLAN1, the port is no longer a member of all other VLAN's tagged or untagged, and the default VLAN of the port returns to 1.	Interface configuration mode
switchport hybrid allowed vlan add <vlan-list> egress-tagged enable	Configure the port to be the tagged member of the specified one or more VLAN. The parameter <vlan-list> can be a VLAN, a VLAN range or a plurality of VLAN. For example, the parameters can be "1", "2-4" or "1,3,5".	Interface configuration mode
switchport hybrid allowed vlan add <vlan-list> egress-tagged disable	Configure the port to be the untagged member of the specified one or more VLAN. The parameter <vlan-list> can be a VLAN, a VLAN range or a plurality of VLAN. For example, the parameters can be "1", "2-4" or "1,3,5".	Interface configuration mode
switchport hybrid allowed vlan remove <vlan-list>	The port is cleared from the specified one or more VLAN and is no longer the tagged or untagged member of these VLAN. If the default VLAN of the port belongs to the specified VLAN, then the default VLAN is returned to 1.	Interface configuration mode

6.2.6 View VLAN information

The commands for viewing VLAN information are listed below:

Command	Description	CLI mode
show vlan [vlan-id]	If you don't input parameters, display all the VLAN information, if you input parameters, display a specified VLAN information. Parameters range from 1 to 4094.	Normal mode, privileged mode
show interface switchport	Display the VLAN related information of all ports of the system, such as VLAN mode, default VLAN and so on.	Normal mode, privileged mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

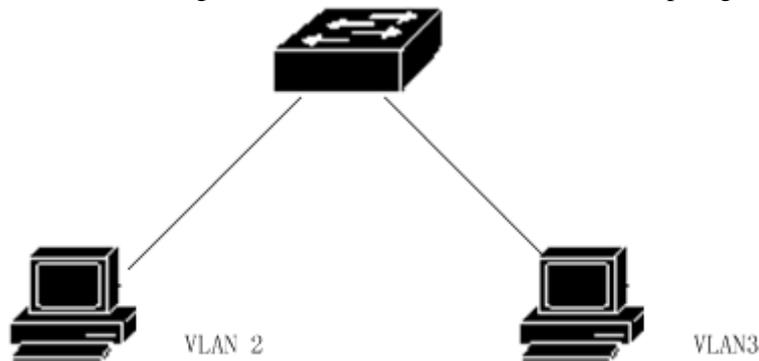
show running-config	Viewing the current configuration of the system, you can see the configuration of the VLAN.	privileged mode
---------------------	---	-----------------

6.3 VLAN configuration example

6.3.1 VLAN based on PORT

1) Configuration

There are two users, User 1 and User 2. The two users need to be in different VLANs because of their different network functions and environments. User 1 belongs to VLAN2, and connects the switch port ge1/1, User 2 belongs to VLAN3, and connects to the switch port ge1/2.



The configuration of the switch is as follows:

Creating VLAN

```
Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
```

Assigning ports to VLAN

```
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode access
Switch(config-ge1/1)#switchport access vlan 2
Switch(config-ge1/1)#exit
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 3
```

2) Troubleshooting

If, after the configuration, it is found that the PC between different VLAN cannot communicate which is a normal phenomenon because for different VLAN to communicate they must go through three layers of routing forwarding. If the PC in the same VLAN cannot communicate with each other, the following verification must be made:

show vlan

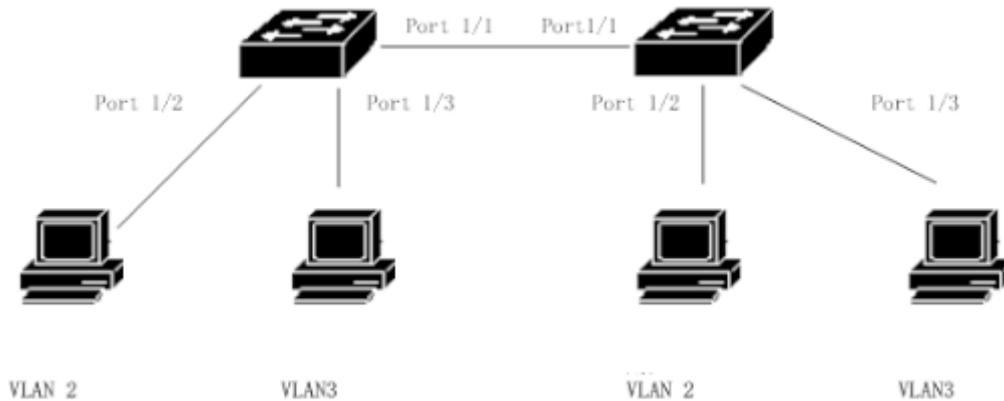
See all the VLAN member ports

show vlan <vlan-id>

See if the port connecting a particular PC machine is within the specified VLAN

6.3.2 VLAN based on 802.1Q

1) Configuration



There are two switches connected to two users:

User	VLAN belongs to	Connection port	Owned switch	Cascade port
User 1	2	1/2	Switch 1	1/1
User 2	3	1/3	Switch 1	1/1
User 3	2	1/2	Switch 2	1/1
User 4	3	1/3	Switch 2	1/1

You need to configure on two switches.

Switch 1 configuration:

```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch#config t
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk allowed vlan add 2
Switch(config-ge1/1)#switchport trunk allowed vlan add 3
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 2
Switch(config-ge1/2)#exit
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 3
```

Switch 2 configuration:

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

```

Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch#config t
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk allowed vlan add 2
Switch(config-ge1/1)#switchport trunk allowed vlan add 3
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 2
Switch(config-ge1/2)#exit
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 3

```

2) Troubleshooting

Inter switch VLAN, within the same VLAN PC can communicate, if not then see below :

- Connect the PC port that belongs to the corresponding VLAN and the application of ACCESS model to join the VLAN.
- The cascade port 1/1 is added to each VLAN, and port 1/1 is TRUNK mode.

6.4 MAC, IP subnet, protocol VLAN

A VLAN based on MAC addresses is based on the source text MAC address to be divided. After receiving the untagged (or tag 0) message from the port, the VLAN of the message is determined according to the source MAC address of the message, and then the message is automatically divided into the designated VLAN transmission.

A VLAN based on IP subnet is divided according to IP address and subnet mask of the source. After receiving an untagged message from the port, the VLAN in the message is determined according to the source address of the message, and then the message is automatically divided into the designated VLAN transmission.

This feature is mainly used to send messages from a designated network segments or IP addresses in specified VLAN.

Protocol based VLAN assigns different VLAN ID to the message according to the protocol type of the message received by the port. The protocols that can be used to divide VLAN are IP, IPV6, IPX, etc.

Before configuring VLAN based on MAC, IP subnet and protocol, the corresponding VLAN must be created first.

Command	Description	CLI mode
mac-vlan mac WORD vlan <1-4094>	Create a VLAN based on the source MAC address	Interface configuration mode
no mac-vlan mac WORD	Deleting a VLAN based on the source MAC address	Interface configuration mode
no mac-vlan	Delete all VLAN based on the source MAC address	Interface configuration mode
show mac-vlan	Displays all VLAN based on the source MAC address	Privileged mode
ip-subnet-vlan ip A.B.C.D	Creating a VLAN based on	Interface

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

A.B.C.D vlan <1-4094>	source IP subnet	configuration mode
no ip-subnet-vlan ip A.B.C.D A.B.C.D	Deleting a VLAN based on the source IP subnet	Interface configuration mode
no ip-subnet-vlan	Delete all VLAN based on source IP subnet	Interface configuration mode
show ip-subnet-vlan	Display all VLAN based on source IP subnet	Privileged mode
protocol-vlan ether-type (ip ipv6 ipx ... <0-65535>) vlan <1-4094>	Creating a protocol based VLAN	Interface configuration mode
no protocol-vlan ether-type (ip ipv6 ipx ... <0-65535>)	Deleting a protocol based VLAN	Interface configuration mode
no protocol-vlan	Delete all protocol based VLAN	Interface configuration mode
show protocol-vlan	Show all protocol based VLAN	Privileged mode
show vlan-partition interface IFNAME	The display interface enables VLAN based on MAC, IP subnet, protocol	Privileged mode

6.5 Voice VLAN

A Voice VLAN is a specialised VLAN for voice or user data streams. By dividing the voice connection port of the device to join a Voice VLAN, for voice data configuration of QoS (Quality of Service, to improve the quality of service) parameters, voice data message priority, ensures the quality of communication.

The device can determine whether the data stream is a voice data stream according to the source MAC address OUI field in the data packet entering the port. The source MAC address conforms to the system settings of the voice device OUI address of the packet is considered to be voice data stream, is divided into Voice VLAN transmission.

The user can preset the OUI address or use the default OUI address as the judgment standard, as follows

Serial number	OUI address	Manufacturer
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	00d0-1e00-0000	Pingtel phone
5	0060-b900-0000	Philips/NEC phone
6	00e0-7500-0000	Polycom phone
7	00e0-bb00-0000	3com phone

Manually add an IP access port to Voice VLAN. Identify the source MAC of the message and matching the OUI address. If the match is successful, the system will send priority to the ACL rules and configuration messages.

Voice VLAN security mode and common mode, safe mode: Only OUI matched language streams are allowed to be transmitted in Voice VLAN, while OUI mismatched data streams are not allowed to be transmitted in Voice VLAN; **Normal mode:** All data streams can be transmitted in the voice VLAN.

Before configuring Voice VLAN, you must first create the corresponding VLAN.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Command	Description	CLI mode
voice-vlan security (enable disable)	Voice VLAN security mode enable	Global configuration mode
voice-vlan oui WORD mask WORD	Configuring user OUI	Global configuration mode
voice-vlan oui WORD mask WORD description WORD	Configure user OUI and name	Global configuration mode
no voice-vlan oui WORD mask WORD	Deleting user OUI configuration through OUI address and mask	Global configuration mode
no voice-vlan oui description WORD	Delete user OUI configuration by name	Global configuration mode
no voice-vlan oui	Delete all user OUI configuration	Global configuration mode
no voice-vlan default-oui WORD mask WORD	Deleting default OUI configuration through OUI address and mask	Global configuration mode
no voice-vlan default-oui description WORD	Delete default OUI configuration by name	Global configuration mode
no voice-vlan default-oui	Delete all default OUI configurations	Global configuration mode
voice-vlan default-oui resume	Restore all default OUI configurations	Global configuration mode
show voice-vlan oui	Display all default and user OUI configuration	Privileged mode
voice vlan <1-4094> (enable disable)	Interface enable Voice VLAN	Interface configuration mode
voice vlan qos map-queue <0-7> remark-dscp <0-63>	The interface configuration QoS priority, default queue is 6, DSCP is 46	Interface configuration mode
no voice vlan qos	Restore interface QoS priority default configuration	Interface configuration mode
no voice vlan	Delete interface configuration Voice VLAN	Interface configuration mode
show voice-vlan state	Display all interfaces configured with Voice VLAN	Privileged mode

6.6 VLAN mapping

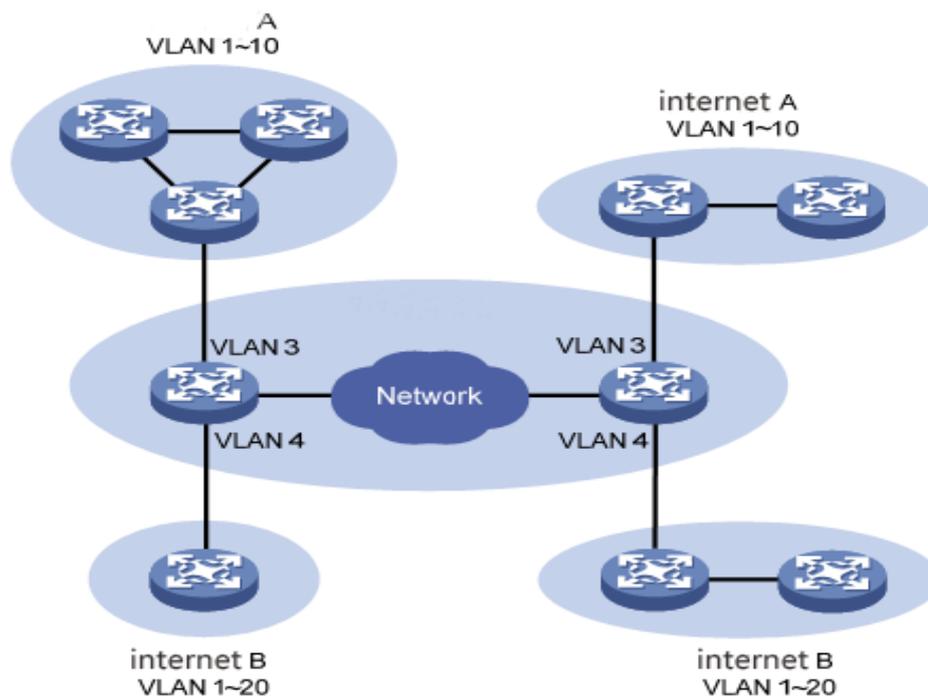
The VLAN mapping (i.e., VLAN Mapping) function can modify the message carried in the VLAN Tag, providing the following mapping relationship: 1:1 VLAN mapping: the message carrying VLAN Tag in VLAN ID is modified to another VLAN ID.

Before configuring the VLAN map, the corresponding VLAN must be created first.

Command	Description	CLI mode
vlan-mapping vlan <1-4094> map-vlan <1-4094>	A VLAN mapping relation for configuring ports	Interface configuration mode
no vlan-mapping vlan <1-4094>	A VLAN mapping relation for deleting ports	Interface configuration mode
no vlan-mapping	All VLAN mapping relationships for deleting ports	Interface configuration mode
show vlan-mapping	Display the VLAN mapping of all configurations	Privileged mode

6.7 QinQ

The QinQ port is provided with a simple and flexible two layer VPN technology. The private networks VLAN TAGS are carried encapsulated inside packets on a third party network. The QinQ feature enables an operator to use a VLAN to serve a network of users with multiple VLANs. As shown below, the user network (marked A) is a private network with VLANs 1~10, the user network (Marked B) is a private network with VLANs marked 1~20. The network operator allocates the VLANS on network A to be VLAN 3, and the users on network B are allocated VLAN 4. In this way, packets from different user networks are completely separated from each other in public network transmission. Even if the VLAN range of two user networks overlaps, there is no confusion in the public network transmission.



The QinQ features enables the network to provide 4094 x 4094 VLANs at most, and meet the requirement of large scale VLANs in metropolitan area network, It solves the following problems:

- (1) Alleviate the increasingly shortage of public network VLAN ID resources.
- (2) Users can plan their own private network VLAN ID, and will not lead to conflict with the public network VLAN ID.
- (3) Provides a relatively simple two layer VPN solution for small metropolitan area network or enterprise network.

QinQ can be divided into two types: basic QinQ and flexible QinQ.

(1) Basic Q in Q: basic QinQ is implemented on a port mode. After opening the basic QinQ function of the port, when the port receives the message, the device will send the message default VLAN Tag for this message. If the received message is already VLAN Tagged, the message becomes a double Tagged message; if the received message is not VLAN Tagged, the message becomes a message with the port default VLAN Tag.

(2) Flexible QinQ: flexible QinQ is a more flexible implementation of QinQ, which is based on

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

the combination of port and VLAN. In addition to all the basic functions of the QinQ, the message received by the same port can also undertake different actions according to the different VLANs, so as to add different external VLAN Tags for packets with different inner layer VLAN ID.

Command	Description	CLI mode
qinq tpid WORD	Configure the TPID value carried in port VLAN Tag, default to 0x8100	Interface configuration mode
no qinq tpid	Recovery port default TPID	Interface configuration mode
qinq uplink	Configuration port is uplink port	Interface configuration mode
no qinq uplink	Uplink configuration for canceling ports	Interface configuration mode
qinq customer	Configuration port is customer port	Interface configuration mode
no qinq customer	Customer configuration for canceling ports	Interface configuration mode
qinq outer-vid <1-4094> inner-vid VLAN_ID	A VLAN conversion for configuring interfaces	Interface configuration mode
no qinq inner-vid VLAN_ID	A VLAN conversion for deleting interfaces	Interface configuration mode
no qinq outer-vid <1-4094>	A VLAN conversion for deleting interfaces	Interface configuration mode
show qinq	Display all configured QinQ conditions	Privileged mode

7. QoS CONFIGURATION

This chapter describes the QoS and its configuration, including the following :

- QoS introduce
- QoS configuration
- Example of basic QoS configuration
- Policy QoS configuration example

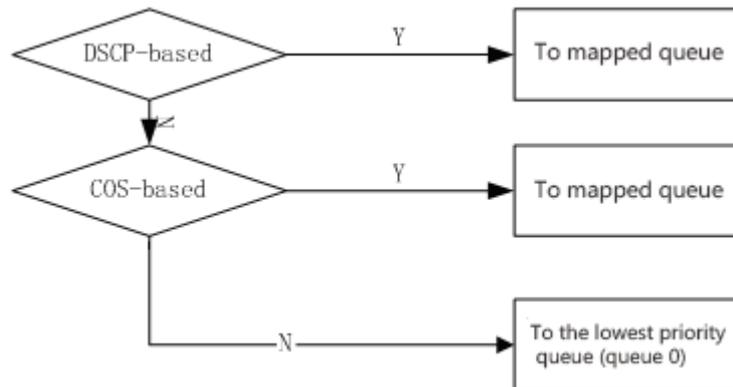
7.1 QoS Introduction

Using the QoS function of the switch, you can configure important data streams to be given more predictable.

The packet is determined at the input to the network according to the priority information in the packet.

The switch implements QoS based on COS (802.1p), QoS based on DSCP (DiffServ) and QoS based on the MAC address. A DSCP based QoS can be configured on a physical port; the physical port defaults to start the QoS based COS.

The following is a QoS enabled packet forwarding flow :



The RT Series of Switches support 0~7 eight priority queues. Queue 7 has the highest priority, and queue 0 has the lowest priority. There are three kinds of priority queue scheduling methods:

1. SP is the strict priority scheduling, the priority queue is always forwarding 7 data packets, until the queue 7 packets forwarding is completed, began to queue 6 queue 6 packets, packet forwarding is completed before forwarding queue 5 packets, the packet forwarding queue 0.
2. WRR is a weighted priority polling switch in forwarding packets, according to the distribution of the rights of the high priority queue to low priority queue polling packet forwarding, forwarding number first right from the high priority data packet forwarding in the right time the number of data packets with high priority and low priority queue forward until the end. From the high priority class began to push forward.. WFQ and WRR queue scheduling algorithm is similar, in the weight algorithm support byte-count and weight, also support SP packet, can replace each other. The difference is as follows: WRR supports a maximum delay, can guarantee the maximum delay of the configuration message in the queue from entering the queue to the maximum time to leave the queue does not exceed the set;

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

- WFQ supports guaranteed bandwidth, minimum queue bandwidth can guarantee the port traffic congestion when available.

In order to facilitate user configuration, we introduce the concept of Qos Profile. Qos Profile is an attribute of the mapping relationship configured with 802.1p and priority queues, which cannot be configured by the user. Their mapping relationships are as follows:

QosProfile	802.1p(CoS)	Priority queuing
Qp0	0	0
Qp1	1	1
Qp2	2	2
Qp3	3	3
Qp4	4	4
Qp5	5	5
Qp6	6	6
Qp7	7	7

7.1.1 QoS based on COS

The port is enabled by default based on COS QoS. The exchange opportunity obtains the priority value of the VLAN TAG in the packet entering the port and determines the output queue of the packet according to the mapping relationship between the user configured COS value and the queue. If the data packet is not VLAN TAG or VLAN TAG VID is 0, then the switch will according to the user configuration of the port and the port of the VID default priority fill the data package, and then according to the output queue of the packet determines the default priority.

7.1.2 QoS based on DSCP

If a port is enabled with DSCP based on QoS, then it exchanges IP data packets in the incoming port to DSCP values in the output port and configures the packet according to the mapping relation between the DSCP value and user configuration of the queue.

The cos-dscp type is an extension based on the DSCP type cos type, which is essentially a DSCP type or a cos type. If the cos-dscp type is used, the IP message system will automatically match the DSCP priority, and the non IP message system will be based on the cos priority. According to the priority type (dscp/cos), the corresponding scheduling is carried out.

7.1.3 Policy based QoS

The QoS policy includes classes and policy actions. The class is used to identify the stream, and the user can define a series of rules by the command to classify the packet; the policy action is used to define the QoS action of the message of the matching rule. In a port enabled strategy based on QoS, the switch will enter the packet classification associated with the port to meet the requirements of the classification of data packets. The packet switch will act according to the strategy of the port. If it does not meet the packet classification requirements it is not processed.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

7.2 QoS Configuration

7.2.1 Default configuration for QoS

Configuration item	Value	Configurable?
Queue number	8	No
Dispatching mode	WRR	Yes
Whether to enable SP scheduling	disable	Yes
Whether to enable WFQ scheduling	disable	Yes
Queue weight	qp0[1],qp1[2],qp2[4],qp3[8],qp4[16] qp5[32],qp6[64],qp7[127]	Yes
The mapping relation between COS and qosprofile	COS0[qp0] COS1[qp1] COS2[qp2] COS3[qp3] COS4[qp4] COS5[qp5] COS6[qp6] COS7[qp7]	No
The mapping relation between DSCP and qosprofile	DSCP0~DSCP7[qp0] DSCP8~DSCP15[qp1] DSCP16~DSCP23[qp2] DSCP24~DSCP31[qp3] DSCP32~DSCP39qp4] DSCP40~DSCP47[qp5] DSCP48~DSCP55[qp6] DSCP56~DSCP64[qp7]	Yes
The attributes of Qosprofile	qp0 cos[0] 0 qp1 cos[1] 1 qp2 cos[2] 2 qp3 cos[3] 3 qp5 cos[4] 4 qp5 cos[5] 5 qp6 cos[6] 6 qp7 cos[7] 7	No
Whether the interface enables DSos based on DSCP	disable	No
Whether the interface enables COS-based qos	enable	No
Interface user priority (COS value)	0	Yes

7.2.2 Configuration scheduling mode

The default scheduling of switches is WRR. The configuration of SP and WFQ can be configured by command.

Command	Description	CLI mode
qos sched { sp wrr wfq }	Configuring QoS scheduling	Interface configuration mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

7.2.3 Configuring queue weights

Command	Description	CLI mode
qos qosprofile (qp0 qp1 qp2 qp3 qp4 qp5 qp6 qp7) weight <1-127>	Configure the weight of each priority queue	Interface configuration mode
no qos qosprofile (qp0 qp1 qp2 qp3 qp4 qp5 qp6 qp7) weight	The weight of the recovery queue is configured as the default configuration	Interface configuration mode

Queue weight is the number of packets forwarded by a priority queue when polling and forwarding. Therefore, when configuring the queue weight, it should be noted that the weight of the low priority queue does not exceed the weight of the high priority queue.

7.2.4 Configure the mapping relationship between DSCP and QosProfile

Command	Description	CLI mode
qos dsc-map-qp <0-63> qosprofile {qp0 qp1 qp2 qp3 qp4 qp5 qp6 qp7}	Mapping relations between DSCP and qosprofile.	Global configuration mode
no qos dscp-map-qp <0-63>	Restoring the mapping between DSCP and qosprofile is the default configuration.	Global configuration mode

7.2.5 Configuring port QoS

QoS policy configuration steps: define class, define policy action, application strategy.

Define a class and define a set of flow classification rules:

A total of 802.1p priority, DSCP, ACL three flow classification rules, a class can only use a set of flow classification rules, a group of flow classification rules can be used by multiple class. The default configuration does not match any rules.

Command	Description	CLI mode
qos class <1-256> name WORD	Naming a specified class	Global configuration mode
qos class <1-256> match cos <0-7> (<0-7>...)	Define a matching 802.1p priority rule, which can configure 8 rules at once	Global configuration mode
qos class <1-256> match dscp <0-63> (<0-63>...)	Defining matching DSCP rules allows you to configure 8 rules at once	Global configuration mode
qos class <1-256> match acl <1-99> <100-199>...	Define matching ACL rules, only 1 groups of rules can be configured at one time	Global configuration mode
no qos class <1-256>	Restore default configuration	Global configuration mode
show qos class (<1-256>)	Displays information about configured classes	Privileged mode

Define a strategy and define a set of QoS actions for matching rules:

There are six kinds of QoS actions, such as mapping message output queue, re marking DSCP, counting, copying to CPU, mirroring, speed limiting, in which a copy to CPU and mirror cannot be configured at the same time. A policy can connect multiple class, and a class can be connected

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

by multiple policy. A group of QoS actions can be used when a policy is connected to a class. In default configuration, policy does not connect to any class, nor does it use any QoS action.

Command	Description	CLI mode
qos policy <1-256> name WORD	Naming the specified policy	Global configuration mode
qos policy <1-256> class <1-256> remark dscp <0-63>	Matching classification rules, marking the DSCP value of the message	Global configuration mode
no qos policy <1-256> class <1-256> remark	The action of removing the re marking message	Global configuration mode
qos policy <1-256> class <1-256> meter <1-1000000> <1-65535>	Matching classification rules restrict the bandwidth and burst traffic of packets	Global configuration mode
no qos policy <1-256> class <1-256> meter	Removal of restricted message bandwidth and burst traffic	Global configuration mode
qos policy <1-256> class <1-256> statistic-packets	Match the classification rules, and count the number of messages	Global configuration mode
no qos policy <1-256> class <1-256> statistic-packets	The action of removing the number of statistical messages	Global configuration mode
qos policy <1-256> class <1-256> mirror-to cpu	Matching classification rules, message mirroring to CPU	Global configuration mode
qos policy <1-256> class <1-256> mirror-to monitor-interface	Matching classification rules, message mirroring to mirror port (mirror port configuration is effective)	Global configuration mode
no qos policy <1-256> class <1-256> mirror	Remove the action of mirroring messages	Global configuration mode
no qos policy <1-256> (class <1-256>)	Strategy deletes corresponding matching rules and actions	Global configuration mode
qos policy <1-256> class <1-256> map-queue <0-7>	Match the classification rules and assign messages to the corresponding output queue	Global configuration mode
no qos policy <1-256> class <1-256> map-queue	Match the classification rules and assign messages to the default output queue 0	Global configuration mode
clear interface IFNAME qos policy statistic-packets	Clear the statistical information of the interface QoS policy	Global configuration mode
show qos policy (<1-256>)	Display information about configured policies	Privileged mode
show qos	Display the information of the configured QoS	Privileged mode

Apply policy and apply corresponding strategy to the interface;

An interface only has one policy and only one policy can be used by multiple interfaces.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

A port can only be enabled to select and enable a QoS. The QoS function can only be configured on the physical port and cannot be configured in the TRUNK group or the three layer interface.

Command	Description	CLI mode
qos {dscp-based cos-based dscp-cos-based apply-policy <1-256>}	Enable port QoS function.	Interface configuration mode
no qos	Restore default port-based.	Interface configuration mode
show qos	Display configuration information for all QoS	Privileged mode
show qos interface IFNAME	Display interface configuration of QoS information	Privileged mode
show qos interface	Display the QoS information of all interface configurations	Privileged mode

7.2.6 Configuring the port user priority (COS value)

Command	Description	CLI mode
qos user-priority <0-7>	Configuring the user priority (COS value) of the port	Interface configuration mode
no qos user-priority	The user priority (COS value) of the recovery port is the default configuration.	Interface configuration mode

7.3 Example of basic QoS configuration

Configuring the ge1/3 user priority (COS value) is 3, and the COS based QoS function defaults to boot:

```
Switch#configure terminal
Switch#(config)#interface ge1/3
Switch#(config-ge1/3)#qos user-priority 3
Switch#(config-ge1/3)#end
```

Configure the interface ge1/3 to start the DSCP based QoS function and map the DSCP value 3 to the priority queue 2:

```
Switch#configure terminal
Switch#(config)#qos dscp-map-qp 3 qosprofile qp2
Switch#(config)#interface ge1/3
Switch#(config-ge1/3)#qos dscp-based
Switch#(config-ge1/3)#end
```

7.4 Policy QoS configuration example

Configure ACL to capture data streams of source MAC1, MAC2, MAC3, respectively (ACL rules can be modified according to requirements, but here are just a few examples)

```
access-list 700 permit host 0000.0000.1111 vid any ip any any
access-list 701 permit host 0000.0000.2222 vid any ip any any
access-list 702 permit host 0000.0000.3333 vid any ip any any
```

Configure the QOS class to match the data streams of source MAC1, MAC2, and MAC3, respectively (You can modify the matching rule cos or DSCP according to the requirement, which

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

is just a simple example)

```

qos class 10 match acl 700
qos class 11 match acl 701
qos class 12 match acl 702

```

Configure the QOS policy to mark the 802.1p priority of the data streams of MAC1, MAC2, and MAC3, respectively

(You can modify policies according to requirements, but here are just a few examples)

```

qos policy 10 class 10 remark cos 7
qos policy 10 class 11 remark cos 5
qos policy 10 class 12 remark cos 3

```

Send QOS policy to port

```

interface ge1/23
qos apply-policy 10

```

Check the configuration information, the analysis of the test results in G1/24 portSwitch#show qos interface ge1/23

8. MSTP CONFIGURATION

This chapter describes the MSTP and its configuration, including the following:

- MSTP introduction
- MSTP configuration
- MSTP configuration example

8.1 MSTP introduction

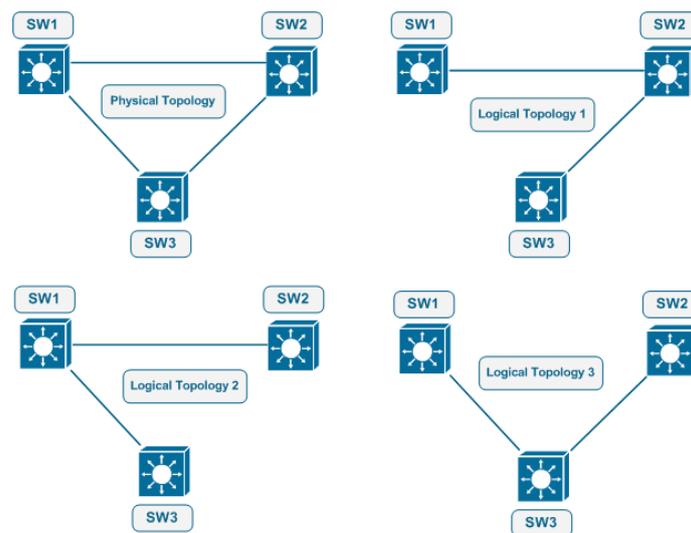
The RT Series of switches support IEEE802.1d, IEEE802.1w, IEEE802.1s and the standard STP protocol.

8.1.1 Overview

MSTP uses RSTP to allow multiple VLANs to be aggregated into a spanning tree instance and each instance has a spanning tree topology that is independent of the other spanning tree instances. This architecture provides multiple forwarding paths for data streams, providing load balancing, and reducing the number of spanning tree instances that are required to support a large number of VLAN.

The core idea of MSTP is utilising the fact that a redundant physical topology only has a small number of different Spanning-Trees (Logical topologies).

The diagram below shows a ring topology showing 3 switched and three different spanning Trees that may result from different root bridges.



Instead of running an STP Instance for every VLAN, MSTP runs a number of VLAN independent STP Instances (representing logical topologies) and then the network manager maps each VLAN to the most appropriate logical topology (STP Instance). The number of STP instanced is kept to a minimum (saving switch resources), but allowing the network capacity to utilised more efficiently by using all possible paths for the VLAN Traffic

8.1.2 Multiple Spanning Tree Domains

For instances involved in multiple spanning tree (MST) configurations, the same MST configuration information must be configured in a consistent manner. A set of connected switches that have the same MST configuration to allow them to form the MST domain.

The MST configuration determines the domain to which each switch belongs. The configuration includes domain name, revision number, and MST instance and VLAN assignment mapping; this information generates a unique abstract (Digest) in the MST configuration. The summaries in the

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

same domain are the same, and they must be the same. You can look at the information through the show spanning-tree MST config command.

One domain can have one or more members with the same MST configuration; each member must have the ability to process RSTP BPDU. There are no restrictions on the number of MST domains in a network, but each domain can only support 16 instances at most. You can only assign one VLAN to one spanning tree instance at a time.

8.1.3 IST, CIST, and CST

The internal spanning tree (IST), is the spanning tree running in the MST domain.

In each MST domain, MSTP maintains multiple instances of creation.

Instance 0 is a special instance of a domain called IST. All other MST instances are numbers 1 to 15.

This IST is just a spanning tree instance receiving and sending BPDU packets; all other spanning tree instance information is compressed in MSTI BPDU. Because MSTI BPDU carries all the instance information, it needs to be handled by a switch that supports multiple spanning tree instances, which means simplifying the number of BPDU. All in the same domain MST instances share the same protocol timer, but each MST instance has its own topology parameters, such as a root switch ID, root path cost etc. By default, all VLANs are assigned to IST.

The common and internal spanning tree (CIST) is a collection of all spanning trees in every MST domain, and the common spanning tree that connects the MST domain and the single spanning tree (IST).

The spanning tree computed in a domain looks like a subtree of CST that contains all the switch domains. CIST is formed by the spanning tree computation that results between switches that support 802.1W and 802.1D protocols. The CIST in MST domain is the same as that in CST domain. Common spanning tree (CST), spanning tree between MST domains.

8.1.4 Intra Domain Operation

IST connects all the MSTP switches in a domain. When IST converges, the root of IST becomes the IST master, which is the minimum bridge ID in the domain and the path overhead of the switch to the CST root. If there is only one domain in the network, the IST master is also the CST root. If the CST root is out of bounds, an MSTP switch at the domain boundary (boundary) is chosen as IST master.

When an MSTP switch is initialized, it sends BPDU packets to itself as the CST root and IST master, and the path cost to the CST root and IST master is set to 0. Switches also initialise all MST instances and require them to be their roots. If the switch receives MST root information then the current port information (low bridge ID, low cost and so on, it gives up the path) it becomes the IST master requirements.

In initialization, a domain may have many sub domains, each of which has its own IST master.

When the switch receives better IST information, it leaves its old sub domain and adds itself to the new sub domain that may contain the real IST master. Therefore, all sub domains are contracted, except for the real IST master subdomain.

In order to operate properly, all switches within the MST domain must recognise the same IST master. So, switches in any two domains synchronize the roles of their ports of one of their MST instances, only if they converge to a common IST master.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

8.1.5 Inter-domain operation

If there are multiple domains or early 802.1D switches in the network, MSTP establishes and maintains CST, which contains all the MST domains in the network and all the early STP switches. MST instances join IST in domain boundaries (boundary) to become CST.

IST connects all switches in the MSTP domain and looks like a subtree of CST (surrounded by all switch domains), and the root of the subtree becomes IST master. The MST domain looks like a virtual switch adjacent to the STP switch and the MST domain.

Only CST instances send and receive BPDU packets, and MST instances increase their spanning tree information to BPDU to interact with their neighbouring switches and compute the last spanning tree topology. Because of this, the spanning tree parameters involved in BPDU transfers (such as hello time, forward time, max-age and max-hops) are configured only in CST instances, but not all MST instances. Parameters involved in the spanning tree topology (e.g., switch priority, port VLAN cost, port VLAN priority) can be configured in CST instances and MST instances. MSTP switches use version 3 RSTP BPDU or 802.1D BPDU and 802.1D switch communication. MSTP switches communicate by using MSTP BPDU and MSTP switches.

8.1.6 Hop count

The IST and MST instances do not use message-age and maximum-age information in the BPDU that configure the spanning tree topology. Instead, use the path to the root and spend the equivalent of IP TTL hop-count mechanism.

You can configure the maximum number of hops for that domain and apply it to that domain IST and all MST instances. The number of hops calculations is the same as the message-age result (decided after initiating a reconfiguration). The instance root switch always sends a BPDU (or-M-record) with cost 0 and hop-count as the maximum. When a switch receives a BPDU, it decrements the remaining hops and propagates the remaining hops in the BPDU it generates. When the count reaches 0, the switch drops the BPDU and age the information for that port. In a domain, the Message-age and maximum-age information in the RSTP BPDU section is consistent, and the same value is spread over the specified port of the domain (boundary).

8.1.7 Boundary port

A boundary is a spanning tree domain that connects an MST region to a single RSTP, or a spanning tree domain of 801.1D alone, or a different MST region. A border port is also connected to a LAN, and the designated switch for this LAN is either a single spanning tree switch or a switch with a different MST region configuration.

At boundary ports, the MST port roles are not important, and their states are forced to be the same as the IST port state (when the IST port is forwarding, the MST port at the boundary is forwarding). An IST port on the boundary can have any role other than the backup port.

In a shared boundary connection, the MST port waits for the forward-delay time expiration in the blocking state before it is converted to the learning state. The MST port waits for another forward-delay time to expire before it is converted to forwarding.

If the boundary port is a point-to-point connection and is the IST root port, the IST port is converted to the forwarding state, and the MST port is converted to the forwarding state.

If a boundary port is converted to a forwarding state in an instance, it is forwarding in all instances, and a topology change is triggered. If a boundary port with an IST root or a specified port role receives a topology change notification, the MSTP switch triggers a topology change on the active port of the IST instance and all the MST instances.

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

8.1.8 MSTP 802.1d and STP interoperability

A switch running MSTP supports a built-in protocol migration mechanism that enables it to coordinate with 802.1D. If the switch receives an 802.1D-configured BPDU from a port, it sends an 802.1D BPDU to that port. When a boundary port of a domain receives an 802.1D BPDU or a different MSTP BPDU or RSTP BPDU, the MSTP switch can detect.

However, if the switch is no longer receiving 802.1D BPDU, it will not automatically revert to the MSTP mode because it cannot determine whether the exchange of the other party has been deleted from the connection unless the other switch is the designated switch. Similarly, when a switch connected to this switch has been added to this domain, the switch may continue to assign a boundary port role to a port. Migration processing of restart protocol (mandatory and neighbour switch negotiation).

If all of the switches on the other side are RSTP switches, they can handle MSTP BPDU and handle RSTP BPDU. Therefore, the MSTP switch is sent to the border port or to send a version 0 configuration and TCN BPDU or version 3 MSTP BPDU. A boundary port that connects to the LAN. This designated switch is either a separate tree switch or a switch with different MST configurations.

8.1.9 Port role

Fast convergence algorithm for MSTP using RSTP. This section briefly introduces the MSTP port role and fast convergence in combination with RSTP.

RSTP provides fast convergence of specified port roles and decision activity topologies. RSTP, based on IEEE802.1D STP, selects high priority switches as root switches. When RSTP specifies a port role to a port:

Root port — When forwarding packets to the root switch provides the optimal path cost.

Designated port — Connection specified switch. When forwarding packets from the LAN to the root switch have the lowest cost path. Specifies that the port through which the switch connects to the LAN is called a specified port.

Alternate port — Provides a replacement path to the root switch of the current root port.

Backup port — Backup of a path that plays a specified port to the spanning tree leaf. A Backup port exists only when the two ports are connected together in a point-to-point loop, or when a switch has two or more connections to a shared LAN segment.

Disable port — There is no port role in the spanning tree operation.

Master port — On the shortest path of the domain root or the total root, it is the port connecting the domain to the total root.

The root port or the specified port role is included in the active topology. The replacement port or backup port role is not included in the active topology.

In a stable topology and fixed port role of the entire network, RSTP to ensure that every root port and the designated port immediately moved to the forwarding state when all the replacement port and backup port is always in the state of discarding. Port state control forwarding and learning processing.

Fast convergence

In the following case, RSTP provides fast recovery: switch failure, port failure, or LAN fault, which provides fast restoration for edge ports, new root ports, and connections to a point-to-point connection:

Edge ports — If you configure a port as an edge port, the edge port is immediately migrated to the forwarding state. You can open it as a boundary port only when this port is connected to a single terminal or to determine the device that does not need to compute the spanning tree.

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Root ports — If RSTP selects a new root port. It blocks an old root port and immediately moves the new root port to the forwarding state.

Point-to-point links — If you connect a port to other ports through a point-to-point connection and local port into a designated port and other ports, it passes through the proposal-agreement handshake negotiation a rapid migration to determine a fast convergence without loop topology (loop-free).

Topological change - This section describes the differences between RSTP and 802.1D in dealing with topological changes in spanning-tree.

Detection — Any transfer between blocking and 802.1D as the forwarding state will cause topology changes, only to migrate from blocking to forwarding to RSTP (state topology change just to increase the connectivity of the considered topology change). The state changes at one edge of the port (edge port) does not cause topology changes. When a RSTP switch investigates a topology modification, it is flooding it to learn information to all non-edge ports (non-edge ports), in addition to receiving ports of TC information.

Notification — Unlike 802.1D, using TCN BPDU, RSTP doesn't use it. However, in order to 802.1D and interoperability, RSTP switch and TCP BPDU treatment.

Acknowledgement — When an RSTP switch receives a TCN message from an 802.1D switch at a specified port, it responds with an 802.1D BPDU and sets the TCA flag bit. However, if TC-while timer (the same as 802.1D topology-change timer) is active, it connects to the 802.1D switch at the root port and receives a configuration BPDU with TCA, TC-while timer restart (reset). This behaviour is only required to support the 802.1D switch. RSTP BPDU never has a TCA flag bit.

Propagation — When a RSTP switch receives a TC message from another switch through a specified port or root port, it propagates to all non-edge ports, designated ports and root ports (except for the receiving port). All of these ports start TC-while timer and flood the information they learn.

Protocol migration — In order to backward compatible 802.1D switches, RSTP selectively sends 802.1D configuration BPDU and TCN BPDU based on each port.

When one is initialized and migrate-delay timer starts (the specified minimum value is sent during RSTP BPDU), the RSTP BPDU is sent. When this timer is active, the switch handles all the BPDU received from the port and ignores the protocol type.

After the port migration-delay timer has stopped, if the switch receives an 802.1D BPDU, it assumes that it is connected to an 802.1D switch and starts using the 802.1D protocol BPDU.

However, if the RSTP switch is using 802.1D BPDU on a port, after receiving timer, a RSTP BPDU is received, which restarts the timer and starts using RSTP BPDU.

8.1.10 A brief introduction to 802.1D spanning tree

The spanning tree protocol is based on the following points :

- 1) There is a unique group address (01-80-C2-00-00-00) that identifies all switches on a particular LAN. This group of addresses can be identified by all switches.
- 2) Each switch has a unique identifier (Bridge Identifier).
- 3) The port of each switch has a unique port identifier (Port Identifier).

Spanning tree configuration management also requires for each switch tuning a relative priority, each port of each switch is a relative priority of each port, take a path of coordination.

The switch with the highest priority is called the root (root) switch. Each switch port has a root path cost, and the root path cost is the sum of the cost of each segment of the switch to the root

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

switch. The minimum value of the root path in a switch is called the root port, and if there are multiple ports with the same root path cost, the port with the highest priority is the root port. In each LAN, there is a switch called the designated (designated) switch, which belongs to the least cost switch in the root path of the LAN. The port that connects the LAN to the specified switch is the designated port of the LAN (designated port). If more than two ports in the specified switch are connected to this LAN, the port with the highest priority is selected as the specified port.

The essential factors that determine the formation of a spanning tree:

1) Decision root switch

- a. At first, all switches considered themselves to be root switches;
- b. The switch sends the configuration BPDU to the connected LAN broadcast, whose root_id is the same as the bridge_id;
- c. When the switch receives another switch configuration BPDU, if it is found that the root_id field is received in the configuration BPDU value is greater than the value in the root_id parameter of the switch, the frame is discarded, or root_id, update the switch takes root path parameters such as root_path_cost value, the switch will continue to broadcast to a new value the configuration of BPDU.

2) Decision root port

The minimum value of the root path in a switch is called the root port.

If multiple ports have the same minimum root path cost, the port with the highest priority is the root port. If two or more ports have the same minimum root path cost and the highest priority, the port with the smallest port number is the default root port.

3) Designated switch for LAN

- a. At first, all switches consider themselves to be the designated switches of LAN.
- b. When the switch receives the BPDU sent by other switches in the same LAN (the same) with a lower root path, the switch no longer claims that it is the designated switch. If there are two or more switches with the same root path cost in a LAN, the switches with the highest priority are selected as the designated switches.
- c. If you specify a switch at a time one other LAN switch due to competition and sent to the specified switch configuration BPDU, the specified switch will send a response to the BPDU configuration, to re determine the designated switch.

4) Determining the specified port

The specified port in the specified switch of LAN is connected to the LAN port. If the specified switch has two or more ports connected to the LAN, then the port with the lowest identification port is the specified port.

In addition to the root port and the specified port, the other ports are blocked. In this way, the topology of a spanning tree is determined after deciding the root switch of the root switch, the switch, and the designated switch and designated port of each LAN.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

8.2 MSTP configuration

8.2.1 Default configuration

Command parameter	Default value
spanning-tree mst enable(Start MSTP)	Close
Spanning-tree mst priority(Switch CIST priority)	32768
spanning-tree mst hello-time(switch cist hello-time)	2
spanning-tree mst forward-time(switch cist forward-time)	15
spanning-tree mst max-age(switch cist max-age)	20
spanning-tree mst max-hopsswitch cist max-hops)	20
instance 1 priority (Instance priority)	32768
spanning-tree mst instance 1 priority(Port instance priority)	128
spanning-tree mst instance 1 path-cost(Port instance path-cost)	20000000
spanning-tree mst priority (port cist priority)	128
spanning-tree mst path-cost (port cist path-cost)	20000000

8.2.2 General configuration

Start MSTP

When the system is started, the default configuration MSTP is closed.

The configuration process for starting MSTP is:

Switch#configure terminal

Switch(config)#spanning-tree mst enable

The command to close MSTP is:

Switch#configure terminal

Switch(config)#no spanning-tree mst

Configuration of max-age:

Configuring max-age is the configuration of all instances. Max-age is the number of seconds when the switch waits for the configuration information of the spanning tree before triggering a reconfiguration.

The default configuration is 20 seconds, and the configuration range is 6 to 40 seconds.

Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst max-age <seconds>

Configuration of max-hops:

Max-hops is the number of hops specified before a BPDU is discarded in a domain.

The default value is 20, and the configuration range is 1 to 40.

Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst max-hops <hop-count>

Configuration of forward-time:

Configuring forward-time is for all instances. Forward-time is the number of seconds that ports wait from discarding to learning and from learning to forwarding.

The default configuration is 15 seconds, and the configuration range is 4 to 30 seconds.

According to the generation number protocol forward-time, the following conditions must be satisfied: $2 * (\text{forward-time} - 1) \geq \text{max-age}$.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst forward-time <seconds>

Configuration of hello-time:

Configuring hello-time is the configuration of all instances. Hello-time is the time interval for root switches to generate configuration information.

The default configuration time is 2 seconds, and the configuration range is 1 to 10 seconds.

According to the generation number protocol hello-time, the following conditions must be satisfied: $2 * (\text{hello-time} + 1) = < \text{max-age}$.

Configuration process:

Switch#configure terminal

Switch(config)# spanning-tree mst hello-time <seconds>

Configure the priority of CIST bridge (priority):

The default configuration 32768, the configuration range <0-61440>; the CIST priority value is only 4096 multiples.

Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst priority <priority>

Configuration and CISCO compatibility:

The network switch uses the MSTP protocol based on 802.1s, each MSTI message length is 16 bytes; and CISCO switch BPDU, each MSTI message length is 26 bytes. In order to interact with the CISCO switch, switches that configure the network need to start the CISCO compatible switch.

In the case of starting and CISCO compatible configuration, the same domain is considered as long as the domain name and the revision number are the same when judging whether the domain is the same.

The default system does not start this function.

Open and CISCO compatible :

Switch#configure terminal

Switch(config)#spanning-tree mst cisco-interoperability enable

Close and CISCO compatible :

Switch#configure terminal

Switch(config)#spanning-tree mst cisco-interoperability disable

Reset protocol checking task

In order to be compatible with the 802.1D STP protocol, the system can automatically detect the protocol of the other system running. Determine the protocol for the port running according to the protocol running by the other party.

In some cases reset protocols are required. For example, the system negotiated a port to run the STP protocol, and after a period of time, the other side of the device running STP protocol has been replaced by a host. When I need to configure the port for fast port, but the port has been running the STP protocol, and the protocol negotiation task has stopped; then need to reset this protocol negotiation task let it re negotiation between it and the host protocol.

Reset the protocol reconnaissance task of the whole device :

Switch#clear spanning-tree detected protocols

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

The protocol reconnaissance task of resetting a port:

Switch#clear spanning-tree detected protocols interface <if-name>

8.2.3 Domain configuration

Two or more devices in the same domain, must have the same VLAN instance mapping relationship, the same modified version number and the same domain name.

Once a domain has one or more members with the same MST configuration, each member can handle the RSTP BPDU capability. There are no restrictions on the number of members in a network, but each domain can only support up to 16 instances.

The configuration of the instance is explained in the instance configuration, which only introduces the domain name configuration and the revision version number configuration.

Configuring domain names:

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#region <region-name>

Configuration revision number:

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)# revision <revision-num>

8.2.4 Instance configuration

The system supports 16 instances, and the scope of the instance ID number is 0-15. A VLAN can only be assigned to a spanning tree instance at a time.

By default, there is only one instance 0, and all of the VLAN belong to this instance.

The process of configuring an instance:

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#instance <instance-id> vlan <vlan-id>

Configure the priority of MSTI bridge (priority)

The default configuration 32768, the configuration range <0-61440>; the MSTI priority value is only 4096 multiples.

Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#instance <instance-id> priority <priority>

8.2.5 port configuration

The port configuration information associated with MSTP is described below. Here only the simple configuration section, port fast and root guard, are introduced separately.

The process of configuring a port to join an instance:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst instance <instance-id>

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Configure the priority of the CIST port (priority)

The default configuration is 128, the configuration range is <0-240>, and the priority value of the CIST port is only multiples of 16.

Configuration process:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst priority <priority>

Configure the priority of the MSTI port (priority)

The default configuration is 128, the configuration range is <0-240>, and the priority value of the MSTI port is only multiples of 16.

Configuration process:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst instance <instance-id> priority <priority>

Configure the CIST port path cost (path-cost)

The default configuration is 20000000 and the configuration range is 1-200000000. The following is the bandwidth and path change mapping table:

Bandwidth(bps)	Path cost
100,000(100K)	200000000
1,000,000(1M)	20000000
10,000,000(10M)	2000000
100,000,000(100M)	200000
1,000,000,000(1G)	20000
10,000,000,000(10G)	2000
100,000,000,000(100G)	200
1,000,000,000,000(1T)	20
>1000000000000	2

Configuration process

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst path <path-cost>

Configure the MSTI port path cost (path-cost)

The default configuration is 20000000 and the configuration range is 1-200000000.

Bandwidth and path and the above table costs.

Configuration process

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst instance <instance-id> path-cost <path-cost>

Configure the version number of the send protocol package

The default configuration sends the MSTP protocol package with a configuration range of 0-3 and a mapping relationship of 0-stp, 2-rstp, 3-mstp.

Configuration process:

Switch#configure terminal

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Switch(config)#interface <if-name>
Switch(config)# spanning-tree mst force-version <version-id>

Brief introduction to the negotiation process of proposal-agreement.

When a switch receives a proposal message on one of its ports and the port is selected as the new root port, RSTP forces all other ports to synchronize the new root port information.

If all other ports are synchronized with the better root information received from the root port, the switches are synchronized.

When RSTP forces it to synchronize the new root information, if a specified port is in the forwarding state and is not configured as an edge port, it migrates to the blocking state. Typically, when the RSTP forces a port to synchronize a new root message and the port does not satisfy the above conditions, the port state is set to blocking.

When all ports are synchronized, the switch sends an agreement message to the corresponding port of the root port. When the switch is connected to a point-to-point connection in their port role of agreement, the RSTP immediately transfers the port state to forwarding.

If shared connection, the 802.1D port is calculated to determine the state of the port.

The default port connection type is point-to-point connection.

The connection type of the configuration port is point-to-point connection:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst link-type point-to-point

The connection type of configuration port is shared connection:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config-ge1/2)#spanning-tree mst link-type shared

8.2.6 PORTFAST related configuration

1) Port Fast

Port Fast immediately transfers an access or trunk port from the blocking state to the forwarding state, bypassing the listening and learning states. You can connect to a separate workstation and server using Port Fast, which allows these devices to connect to the network immediately without waiting for spanning tree to converge.

Configure a port for fast port:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst portfast

2) BPDU Filtering

BPDU filtering can be opened globally based on switches or based on each port, but their characteristics are different.

In the global layer, you can use the spanning-tree MST portfast bpdu-filter command to start the BPDU filtering function on the port of the portfast bpdu-filter default state.

In the port layer, you can open BPDU filter on any port with spanning-tree MST portfast bpdu-filter enable.

This function prevents port fast ports from receiving or sending BPDU.

Configuring BPDU Filtering

In global configuration mode:

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Switch#configure terminal

Switch(config)# spanning-tree mst portfast bpdu-filter

Under the interface configuration mode :

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst portfast bpdu-filter enable

3) BPDU Guard

BPDU protection features can be opened globally or based on each port, but their characteristics are different.

In the global layer, you can use the spanning-tree MST portfast bpdu-guard to open the BPDU guard function on the port of the portfast bpdu-guard default state.

In the port layer, you can open BPDU guard on any port.

When the port configured with BPDU guard receives BPDU, spanning tree will port the shutdown. In an efficient configuration, the port of Port Fast-enabled does not receive BPDU. A BPDU is received at a Port Fast-enabled port to represent an invalid configuration, for example, a connection to an unauthorized device, and BPDU guard enters an error-disabled state.

Error-disabled is when the port of starting BPDU guard receives BPDU, if the system configured error-disable mechanism, it would start error-disable timer. Error-disable restarts the port after the timeout time of the system configuration.

In global configuration mode :

Switch#configure terminal

Switch(config)# spanning-tree mst portfast bpdu-guard

Under the interface configuration mode :

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst portfast bpdu-guard enable

Configuration of error-disable

Start error-disable mechanism

Switch#configure terminal

Switch(config)#spanning-tree mst errdisable-timeout enable

Configuring timeout time for error-disable

Switch#configure terminal

Switch(config)#spanning-tree mst errdisable-timeout interval <seconds>

8.2.7 Root Guard configuration

A two tier network of SP can contain many switches that are not connected to their own. In such a topology, the spanning tree can reconfigure itself and select a client switch as the root switch. You can avoid this by configuring 'root guard' in the SP switch on the port of the switch in the client network. If the spanning tree calculation causes the port in the client network to be chosen as the root port, the root guard configured as blocked, to prevent the customers switch from becoming a root switch or to the root path.

If a switch outside the SP network becomes a root switch, the port is blocked (root-inconsistent STAT) and the spanning tree selects a new root switch. The client's switch does not become a root switch and there is no path to the root.

If the switch operates in MST mode, the root guard mandatory port becomes the specified port. If a boundary port, because root guard is in the blocked state in the IST instance, this port is blocked in all MST instances.

A boundary port is a port connected to a LAN, which specifies that the switch is either an 802.1D switch or a switch configured in different MST domains.

When a port is opened, the Root guard is applied to all the VLAN that this port belongs to. VLAN can be aggregated and mapped to an MST instance.

Configuration process

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst guard root

8.3 MSTP configuration example

(1) Configuration

The three switches are connected in a ring, and the spanning tree protocol of each switch is needed to avoid a loop. Perform this configuration on each switch separately.

Configuration of switch 1:

Switch>en

Switch#configure terminal

Switch(config)#spanning mst enable

Configuration of switch 2:

Switch>en

Switch#configure terminal

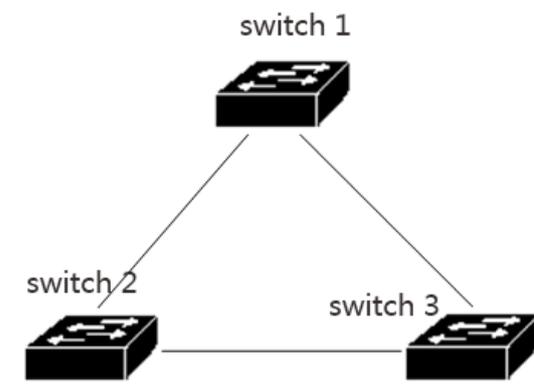
Switch(config)#spanning mst enable

Configuration of switch 3:

Switch>en

Switch#configure terminal

Switch(config)#spanning mst enable



(2) Troubleshooting:

See which switch is selected as root bridge:

Show spanning-tree MST is executed, and the value of CISTRoot is observed as the least one of the three MAC addresses in the exchange, that is, the root result is correct.

Switch#show spanning-tree mst

View the port state of the switches in the spanning tree:

Execute the instruction of show spanning-tree MST interface ge1/1, and observe the State value of PORT ge1/1 in instance 0

Switch#show spanning-tree mst interface ge1/1

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

9. EAPS configuration

This chapter describes the EAPS and its configuration, including the following :

- EAPS brief introduction
- Basic concepts of EAPS
- EAPS protocol introduction
- EAPS configuration
- Restrictive conditions
- A brief introduction to the EAPS command
- Single - loop configuration example
- Example of cross ring data forwarding configuration

9.1 EAPS brief introduction

EAPS is an abbreviation for Ethernet Automatic Protecting Switching. EAPS uses standard Ethernet and VLAN technology to provide loop topology and loop recovery mechanism. When a fault occurs in the loop, EAPS has the ability to recover data communication within a second. The EAPS running is not restricted by the number of nodes, and the recovery time of the loop is not limited by the number of nodes. EAPS does not rely on other devices, that is, EAPS rings can have devices that do not support the EAPS protocol.

9.2 Basic concepts of EAPS

Here are some of the basic concepts involved in EAPS :

- 1. EAPS Domain** - in an EAPS network, the EAPS Domain is running in a single loop. It is a series of nodes that consist of a single loop. The EAPS Domain contains one Master Node and one or more Transit Nodes.
- 2. Master Node** - the EAPS domain, has only one Master Node.
- 3. Transit Node** - a switch that runs EAPS, or an EAPS device, in an EAPS Domain, other nodes except Master Node.
- 4. Primary Port** - a port for connecting EAPS node devices in EAPS Domain. A node device has only one Primary Port connected to this loop in an EAPS Domain.
- 5. Secondary Port** - a port for connecting EAPS node devices in an EAPS Domain. A device only has one Secondary Port connected to this loop in an EAPS Domain.
- 6. Control VLAN** - control VLAN, responsible for the EAPS Domain protocol packet transmission of VLAN, an EAPS Domain has only one Control VLAN.
- 7. Protected VLAN** – a protected VLAN, transfers VLAN data in the EAPS Domain, an EAPS Domain must have a Protected VLAN, or more than one Protected VLAN.

9.3 EAPS protocol introduction

An EAPS Domain runs an EAPS ring.

- An EAPS Domain contains an RPL Owner (Master) Node with one or more Transit Nodes;
- Each node contains the same Control VLAN and multiple Protected VLANs;
- Each EAPS node contains a Primary Port and a Secondary Port in an EAPS Domain.
- The two ports belong to this ring's Control VLAN and Protected VLAN.
- Through the Primary Port and Secondary Port connections of each EAPS node device, all nodes in the EAPS Domain compose an EAPS ring.
- Under normal circumstances, when the EAPS Domain and Secondary Port detect all Primary Ports are in LINK UP state, the RPL Owner (Master Nodes) Secondary Port will

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

block the Secondary Port. (port state Blocking).

- If the EAPS Domain fails, the Secondary port of the Master Node is opened immediately (the state of the Secondary Port is changed to Forwarding), allowing it to forward the business data and resume normal forwarding of the service data.

The Transit Node doesn't make any difference to Primary Port and Secondary Port processing.

The two fault checks and loop recovery of EAPS are described below :

9.3.1. Link-Down alarm

When a Transit Node finds that either its Primary Port or Secondary Port appears to have failed (LINK DOWN), it will send a LINK-DOWN BDPDU protocol message to the Master Node (RPL Owner) via the other working EAPS port (LINK UP) via the Control VLAN

When the Master Node receives this LINK-DOWN BDPDU message :

- The Master Node immediately sets a link failed message which is 'Complete Failed' which immediately opens the Secondary Port, i.e. the RPL link (link between the RPL Master/ Owner and one of the Transit node) changes state to Forwarding.
- When the RPL Owner secondary port detects that it's got a local LINK Down, and that the RPL Owner has a Complete Failed State. It immediately refreshes the forwarding table (MAC and IP Addresses) and sends RING-DOWN-FLUSH-FDB packets to let the other switches know the ring has been broken. This notifies the other transit switch to refresh their forwarding.
- Recovery – This link recovers and two switches where the link broke will tell the RPL Owner that they have recovered. The RPL Owner then starts a timer and during the period of that timer the status of the now recovered link is checked.
- At the end of the time if the link is still stable the RPL Owner will then block the RPL Link between itself the Transit node. If the link fails again during the timer and recovers then the timer will restart.

9.3.2. Loop inspection

The RPL Owner is configured with a primary port and a secondary port. This node transmits the ring detection packets via the control VLAN through the primary port. If the secondary port receives the packets, it verifies that the topology of the ring network is intact. With the ring intact, all the transit ports in the ring are in a forwarding state transmitting tagged data traffic via data VLAN and EAPS control message via control VLAN. However, the secondary port on the master node is logically blocked to this tagged data traffic in order to prevent loops. When a link or node fault occurs between two nodes, they will immediately feedback to the master node via the control VLAN. Then the master node removes the blocking state of the secondary port to make the data traffic flow on the ring without interruption. The RPL Owner will be in a Failed state.

9.3.3. Ring restoration

The RPL Owner sends ring detection packets from its Primary Port, regardless of the status of the ring, i.e. Complete or Failed. When the RPL Owner is in the Failed state, once the ring detection packet is received from its Secondary Port, the loop will revert to the Complete state.

Then RPL Owner will set the Secondary Port state to blocking state, refresh its own MAC forwarding table, and send a RING-UP-FLUSH-FDB packet which instructs the other switches to refresh their own MAC forwarding table.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

9.3.4. Extreme compatible with EAPS

The company Extreme (Switches) were the first to support EAPS. Their devices support EAPS protocol following the RFC3619 standard; The EAPS protocol and RFC3619 Extreme protocol have some differences. The EAPS protocol supported by the Case Switches are fully compatible with the Extreme devices, and the compatible switch is open under default.

9.3.5. Multi EAPS Domain

The Case switches supports up to 16 EAPS Domains

9.4 EAPS configuration

The basic configuration of the EAPS protocol includes the following basic elements:

- Control VLAN, node mode (mode),
- Primary Port,
- Secondary Port,
- Protected VLAN,
- Hello Time
- Fail Time.

Hello Time and Fail Time have the default configuration, Hello Time is 1 second, Fail Timer is 3 second.

9.5 Restrictive conditions

- 1. Primary Port** - must belong to an EAPS Domain Control VLAN and all Protected VLAN TRUNK schema members.
- 2. EAPS protocol** - cannot run with any kind of Spanning Tree Protocol at the same time. EAPS protocol cannot be enabled if STP is enabled or STP has been configured.
- 3. A VLAN starts the VLLP (VRRP Layer2 Loop Protection)** – VLAN used for VLLP cannot be used for EAPS VLAN Control.
- 4. EAPS VLAN Control** - VLAN used for EAPS can only contain the Primary and Secondary Ports and these ports can only be in TRUNK mode.
- 5. If a VLAN is configured as Control Domain** - of EAPS VLAN, and this Domain has been started, then the VLAN cannot be deleted, and its port members cannot be modified or deleted. Control VLAN cannot be configured on a Layer3 interface.
- 6. In Protected VLAN** - The Primary and Secondary Ports can only be in the TRUNK mode. Other member ports can be configured as required, e.g. Access, Hybrid or Trunk.
- 7. An EAPS port can only be configured** - as either an EAPS Domain Primary Port or a Secondary Port.
- 8. The same VLAN** - can only belong to the EAPS Domain Control VLAN or Protected VLAN.
- 9. The control VLAN** - of all nodes in the EAPS Domain must be the same.

9.6 A brief introduction to the EAPS command

To create an EAPS Domain, first of all, make sure that the configuration of the VLAN and ports conforms to the above conditions.

Configuration of EAPS has a certain order requirements.

- 1 To create an EAPS Domain** - check you are in accordance with the requirements of the previous configuration and parameters; otherwise, the configuration will not be accepted.
- 2. If you want to change the ‘Hello’ time** - to the value of the current fail time, you must first

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

modify the fail time to a larger number; otherwise it will not be configured successfully. Other configuration sequences do not require special requirements.

3. Items you cannot change when an EAPS Domain has been started - The Control-VLAN, Mode, Primary-Port, Secondary-Port cannot be modified.

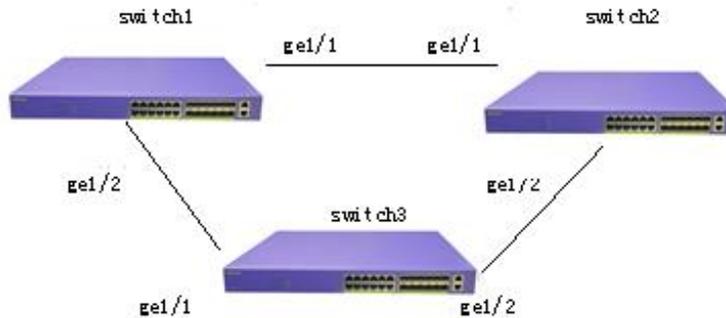
4. Items you can modify you can modify when the EAPS Domain has been started - The Protected-VLAN, Fail-timer, Hello-time, and Extreme-interoperability can be modified, Primary-port and secondary-port support LACP ports (that is, TRUNK groups).

9.6.1 EAPS configuration command

Command	Description	Mode
eaps create <ring-id>	Create an EAPS Domain	Global configuration mode
eaps control-vlan <ring-id> <vlan-id>	Configuring an EAPS Domain control VLAN.	Global configuration mode
eaps protected-vlan <ring-id> <vlan-id>	Add a protected VLAN for EAPS Domain.	Global configuration mode
eaps mode <ring-id> <master transit>	Configure a run node mode of EAPS Domain.	Global configuration mode
eaps primary-port <ring-id> <ifname>	Configure an EAPS Domain Primary Port.	Global configuration mode
eaps secondary-port <ring-id> <ifname>	Configure an EAPS Domain Secondary Port.	Global configuration mode
eaps data-span <ring-id>	Configuring EAPS ring data trans ring forwarding	Global configuration mode
eaps fail-time <ring-id> <secs>	Configure the timeout time of an EAPS Domain fail-period timer. The default is 3 seconds. Units are seconds.	Global configuration mode
eaps hello-time <ring-id> <secs>	Configuring an EAPS Domain to send HEALTH packets at regular intervals. The default is 1 second. Units are seconds. Hello-timer must be less than fail-time.	Global configuration mode
eaps extreme-interoperability <ring-id> <enable disable>	Boot or shutdown compatible with Extreme device, default is startup compatibility.	Global configuration mode
eaps enable <ring-id>	Start an EAPS Domain	Global configuration mode
eaps disable <ring-id>	Close an EAPS Domain	Global configuration mode
show eaps	The EAPS Domain information is displayed in the display system	Normal mode / privilege mode
Show eaps <ring-id>	Displays detailed information about an EAPS Domain	Normal mode / privilege mode

9.7 Single - loop configuration example

In our example below there are three switches. Switch1, Switch2 and Switch3. These are configured to use VLAN2 for EAPS protocol management. Switch1 is configured as RPL Owner (Master node) Switch2 and Switch3 are configured as Transit. Switch3's ge1/1 port will be the RPL port used by Switch1



Configuration of Switch1:

Switch1 is configured as the EAPS Domain ring 1 master (RPL Owner) , the control VLAN is VLAN 2, the protected VLAN is VLAN 1, the primary-port is ge1/1, the secondary-port is ge1/2, other configurations use default values.

Switch#configure terminal

```
#Adding VLAN 2
```

```
Switch(config)#vlan database
```

```
Switch(config-vlan)#vlan 2
```

```
Switch(config-vlan)#exit
```

```
#Configure ge1/1 to be a trunk member of VLAN 1 and VLAN 2
```

```
Switch(config)#interface ge1/1
```

```
Switch(config-ge1/1)#switchport mode trunk
```

```
Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2
```

```
#Configure ge1/2 to be a trunk member of VLAN 1 and VLAN 2
```

```
Switch(config-ge1/1)#interface ge1/2
```

```
Switch(config-ge1/2)#switchport mode trunk
```

```
Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2
```

```
Switch(config-ge1/2)#exit
```

```
Switch(config)#exit
```

```
Switch#show vlan
```

```

VLAN Name    State    Member ports ([u]-Untagged, [t]-Tagged)
-----
 1  vlan1    active  [t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5
                               [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10
                               [u]ge1/11 [u]ge1/12
 2  vlan2    active  [t]ge1/1 [t]ge1/2
  
```

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Switch#configure terminal

#Create an EAPS Domain ring 1

Switch(config)#eaps create 1

#Configure VLAN 2 to control VLAN

Switch(config)#eaps control-vlan 1 2

#Configuring VLAN 1 to be protected VLAN

Switch(config)#eaps protected-vlan 1 1

#Configure Switch1 to be a master node

Switch(config)#eaps mode 1 master

#Configure ge1/1 to primary-port

Switch(config)#eaps primary-port 1 ge1/1

#Configure ge1/2 to secondary -port

Switch(config)#eaps secondary-port 1 ge1/2

#Start EAPS Domain ring 1

Switch(config)#eaps enable 1

Configuration of Switch2

Switch2 is configured as EAPS Domain ring 1 transit, control VLAN is VLAN 2, protected VLAN is VLAN 1, primary-port is ge1/1, secondary-port is ge1/2, other configurations use default values.

Switch#configure terminal

#Adding VLAN 2

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#exit

#Configure ge1/1 to be a trunk member of VLAN 1 and VLAN 2

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode trunk

Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

#Configure ge1/2 to be a trunk member of VLAN 1 and VLAN 2

Switch(config-ge1/1)#interface ge1/2

Switch(config-ge1/2)#switchport mode trunk

Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2

Switch(config-ge1/2)#exit

Switch(config)#exit

Switch#show vlan

```

VLAN Name      State   Member ports ([u]-Untagged, [t]-Tagged)
-----
1   vlan1    active [t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5
                                [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10

```

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

2 vlan2 active [t]ge1/1 [t]ge1/2

Switch#configure terminal

#Create an EAPS Domain ring 1

Switch(config)#eaps create 1

#Configure VLAN 2 to control VLAN

Switch(config)#eaps control-vlan 1 2

#Configuring VLAN 1 to be protected VLAN

Switch(config)#eaps protected-vlan 1 1

#Configure switch to be a transit node

Switch(config)#eaps mode 1 transit

#Configure ge1/1 to primary-port

Switch(config)#eaps primary-port 1 ge1/1

#Configure ge1/2 to secondary -port

Switch(config)#eaps secondary-port 1 ge1/2

#Start EAPS Domain ring 1

Switch(config)#eaps enable 1

Configuration of Switch3

Switch3 is configured as EAPS Domain ring 1 transit, control VLAN is VLAN 2, protected VLAN is VLAN 1, primary-port is ge1/1, secondary-port is ge1/2, other configurations use default values.

Switch#configure terminal

#Adding VLAN 2

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#exit

#Configure ge1/1 to be a trunk member of VLAN 1 and VLAN 2

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode trunk

Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

#Configure ge1/2 to be a trunk member of VLAN 1 and VLAN 2

Switch(config-ge1/1)#interface ge1/2

Switch(config-ge1/2)#switchport mode trunk

Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2

Switch(config-ge1/2)#exit

Switch(config)#exit

Switch#show vlan

VLAN Name State Member ports ([u]-Untagged, [t]-Tagged)

```
-----
1  vlan1  active  [t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5
```

```

[u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10
[u]ge1/11 [u]ge1/12
2 vlan2 active [t]ge1/1 [t]ge1/2

```

```

Switch#configure terminal
#Create an EAPS Domain ring 1
Switch(config)#eaps create 1

#Configure VLAN 2 to control VLAN
Switch(config)#eaps control-vlan 1 2

#Configuring VLAN 1 to be protected VLAN
Switch(config)#eaps protected-vlan 1 1

#Configure switch3 to be a transit node
Switch(config)#eaps mode 1 transit

#Configure ge1/1 to primary-port
Switch(config)#eaps primary-port 1 ge1/1

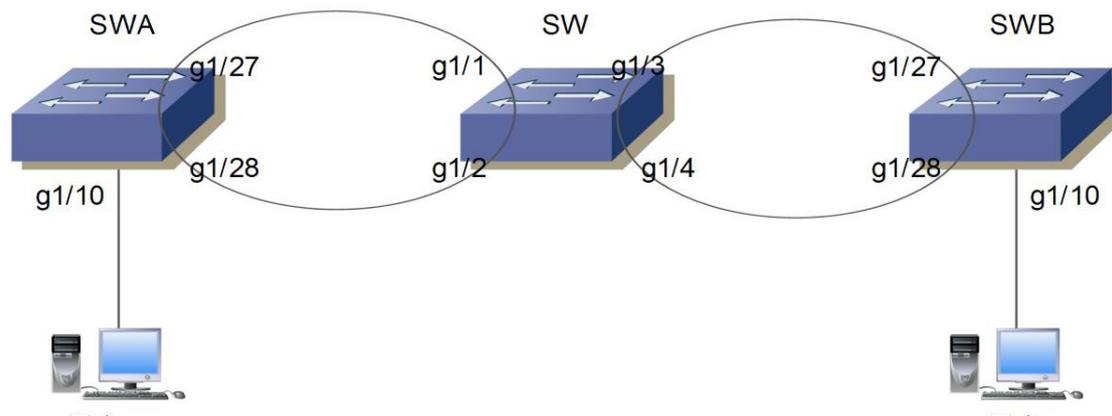
#Configure ge1/2 to secondary -port
Switch(config)#eaps secondary-port 1 ge1/2

#Start EAPS Domain ring 1
Switch(config)#eaps enable 1

```

9.8 Example of cross ring data forwarding configuration

There are three devices SWA, SW and SWB, through the EAPS protocol inter ring to achieve vlan1 vlan2 interworking. The topology is as follows :



SWA loop 1 controls vlan111, protects vlan1, 2, configured as follows:

```

vlan database
vlan 2
vlan 111

```

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

```

interface ge1/10
switchport access vlan 2
interface ge1/27
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 111
interface ge1/28
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 111

```

```

eaps create 1
eaps mode 1 Transit
eaps primary-port 1 ge1/27
eaps secondary-port 1 ge1/28
eaps control-vlan 1 111
eaps protected-vlan 1 1
eaps protected-vlan 1 2
eaps enable 1

```

SW loop 1 and SWA docking, control vlan111, protect vlan1, 2. Ring 2 and SWB docking, control vlan222, protect vlan3333 (virtual VLAN, while the interface needs to add). If you want to achieve ring 1 and ring 2 data trans ring forwarding, you need to configure the command EAPs data-span

Configuration is as follows:

```

vlan database
vlan 2
vlan 111
vlan 222
vlan 3333

```

```

interface ge1/1
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 111
interface ge1/2
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 111
interface ge1/3
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 222
switchport trunk allowed vlan add 3333   ###Add virtual VLAN 3333
interface ge1/4
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 222
switchport trunk allowed vlan add 3333   ###Add virtual VLAN 3333

```

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

```

eaps create 1
eaps mode 1 Master
eaps primary-port 1 ge1/1
eaps secondary-port 1 ge1/2
eaps control-vlan 1 111
eaps protected-vlan 1 1
eaps protected-vlan 1 2
eaps data-span 1
eaps enable 1

```

```

eaps create 2
eaps mode 2 Transit
eaps primary-port 2 ge1/3
eaps secondary-port 2 ge1/4
eaps control-vlan 2 222
eaps protected-vlan 2 3333      ###Here is the virtual protection VLAN
eaps data-span 2
eaps enable 2

```

SWB ring 2 and SW ring 2 butt, control vlan222, protect vlan1, 2. Configuration is as follows :

```

vlan database
vlan 2
vlan 222

```

```

interface ge1/10
switchport access vlan 2

```

```

interface ge1/27
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 222

```

```

interface ge1/28
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 222

```

```

eaps create 2
eaps mode 2 Master
eaps primary-port 2 ge1/27
eaps secondary-port 2 ge1/28
eaps control-vlan 2 222
eaps protected-vlan 2 1
eaps protected-vlan 2 2
eaps enable 2

```

After this configuration is completed, the user 1 and user 2 interworking, vlan1 data is also interoperability. EAPS node mode can be modified according to requirement.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

10 ERPS configuration

10.1. ERPS overview

ERPS (Ethernet Ring Protection Switching) is a ring network protection protocol developed by the ITU, this protocol is also known as G.8032. It is a link layer protocol specially used in an Ethernet ring network. It can prevent broadcast storms caused by data loops and can quickly recover the communication between the nodes on the Ethernet ring when a link is disconnected. The ERPS protocol provides a fast Ethernet ring protection mechanism, which can quickly restore network transmission when the ring network fails, thus ensuring high availability and high reliability of the switch under the condition of the ring network topology.

NB ERPS is not the same as EAPS described in chapter 9

10.2. Introduction of ERPS Technology

10.2.1 ERPS ring

ERPS (Ethernet Ring Protection Switching) rings are based on minimizing rings. Each ring must be the smallest ring, divided into the main ring and the sub ring: the main ring is a closed ring. Each Ethernet Ring Node is connected to an adjacent Ethernet Ring Node participating in the same Ethernet Ring, using two independent links. A ring link is bounded by two adjacent Ethernet Ring Nodes. A port for a ring link is called a **ring port**. The minimum number of Ethernet Ring Nodes in an Ethernet Ring is three.

In ERPS there is a central node called an **RPL Owner Node** which blocks one of the ports to ensure that there is no loop formed for the Ethernet traffic. The link blocked by the RPL Owner node is called the **Ring Protection Link** or **RPL Port**. The node at the other end of the RPL Port is known as **RPL Neighbour Node**. It uses R-APS control messages to coordinate the activities of switching on/off the RPL link.

Each ERPS ring (whether the main ring or ring) has five states:

- (1) Idle state: ring of each physical link is connected to the state.
- (2) Protection state: the state of one or multiple physical links open loop network.
- (3) Manual switch hand: change ring state.
- (4) Forced switch state: the forced change ring state.
- (5) Pending state: intermediate state in suspense.

10.2.2 ERPS node

The layer two switches that are a part of the ERPS ring are called nodes. Each node cannot use more than two ports to join the same ERPS ring.

For the overall situation, the role of the nodes is divided into two types as follows:

(1) The intersection nodes: nodes that belong to multiple rings or separate networks are called the intersection nodes.

(2) Non-intersection nodes: nodes that only belong to a single ERPS ring is called non-intersection nodes.

There are three types of node modes in ERPS protocol:

(1) RPL Owner nodes: a ERPS ring will only have a single RPL Owner node which is determined by the user configuration. The RPL Owner prevents a loop in the ERPS ring by blocking its RPL port. When the RPL Owner node receives a fault message that another node has failed or there is a link failure on the ERPS ring it will automatically open its RPL port so that it can send and receive traffic to ensure the data flow will not be interrupted.

(2) RPL Neighbour node: This node is directly connected with the RPL Owner node's RPL port and, under normal circumstances, the RPL Owner node RPL port and RPL Neighbour node RPL port will be blocked in order to prevent a loop from occurring. When the ERPS ring fails the RPL Owner node RPL port and RPL Neighbour node RPL port will be opened.

(3) Ordinary ring node in the ERPS ring: the nodes except the RPL Owner nodes and RPL Neighbour nodes are ordinary ring nodes sometime known as Transit nodes. The ERPS ring ports on these nodes behave as ordinary ring ports that monitor their ERPS protocol and change status if there is any failure and notify the ring of the change.

10.2.3 Link and channel

(1) RPL (Ring Protection Link): each ERPS ring has only one RPL link.

When the Ethernet ring is in the Idle state, the RPL link is in the blocking state and does not forward any data packets to prevent forming a loop.

(2) Sub loop link: in the intersection ring this link belonging to the sub ring.

(3) RAPS (Ring Auto Protection Switch): is a virtual channel in the intersection ring. The intersection nodes are used to transfer the ring protocol message, but the path not belonging to the sub ring is called the RAPS virtual channel of the ring.

10.2.4 ERPS VLAN

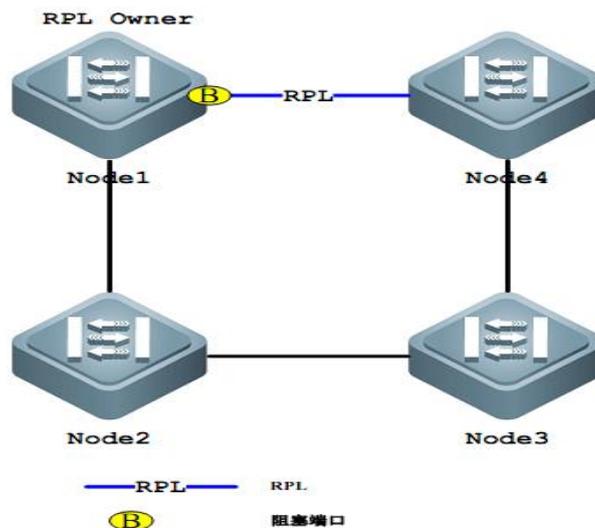
There are two types of VLAN:

(1) RAPS VLAN in ERPS: which are used to transfer ERPS protocol packets, and the ports that access the ERPS ring on the device belong to the RAPS VLAN and only the ports accessing the ERPS ring can join the VLAN. RAPS VLAN of different rings must have different. RAPS VLAN IDs. Note that these VLAN IDs interface are not allowed to have IP addresses configured.

(2) Data VLAN: relative to RAPS VLAN, Data VLANs are used to transmit data packets. Data VLANs can include an ERPS ring port and can include non-ERP ring port.

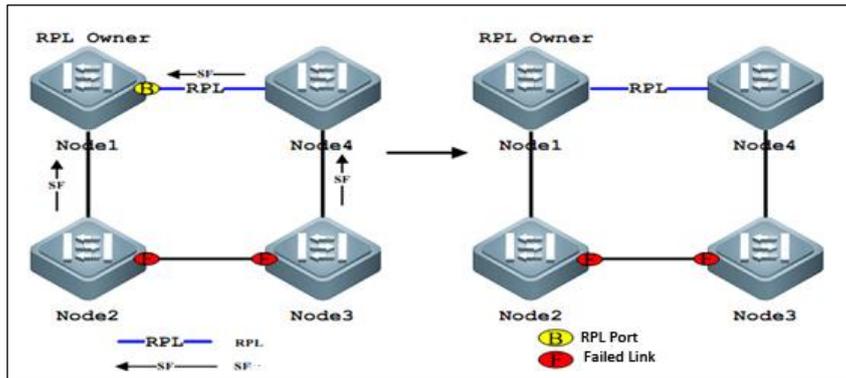
10.3. ERPS Working principle

10.3.1. Normal state



- (1) All nodes are connected in a ring by physical topology.
- (2) Loop protection protocols ensure that loops are not blocked by blocking the RPL link. As shown in the figure above, the link between Node1 and Node 4 is RPL link.
- (3) Fault detection is performed for each link between adjacent nodes.

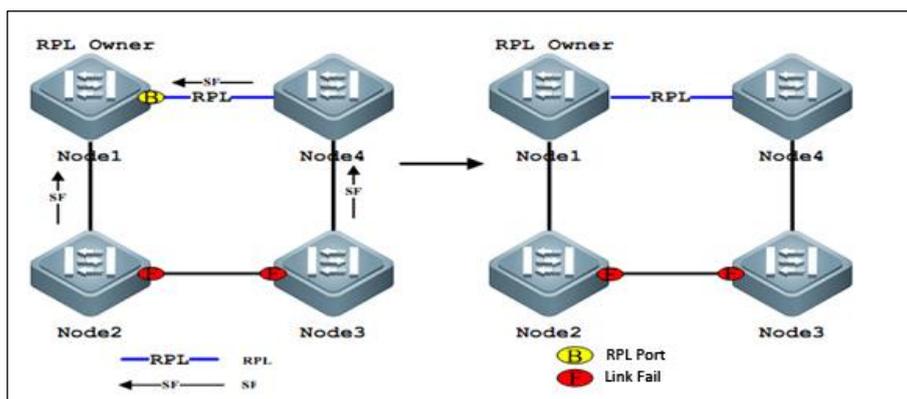
10.3.2. Link failures



(1) **The nodes adjacent to the fault** - and fault link congestion, and the use of RAPS (SF) message to the other nodes report the fault on the ring, as shown above, assuming the link between Node2 and Node3 have failed, waiting for the hold-off timer after a timeout. It will block the link fault, respectively so the ring network nodes send the RAPS message (SF):

(2) **RAPS (SF) message trigger** - RPL has the node to open the RPL port. The RAPS (SF) message also triggers all nodes to update their respective MAC table entries, and then the nodes enter the protection state.

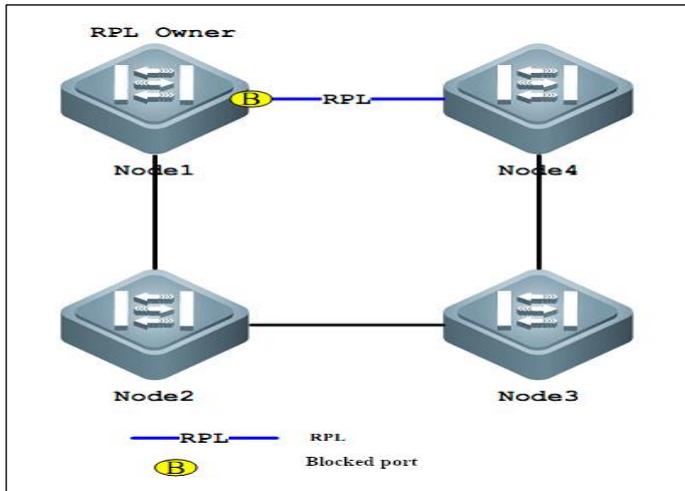
10.3.3. Link recovery



- (1) When the fault is resumed, the neighbouring nodes to the faulty link continue to block and send RAPS (NR) messages to indicate that there is no local fault;
- (2) After the guard timer runs out, the RPL Owner node starts the WTR timer after the first RAPS (NR) message is received;
- (3) When the WTR timer runs out, the RPL Owner node blocks the RPL and sends RAPS (NR, RB) messages;
- (4) When other nodes receive this message, they update their respective MAC table entries, and the node that sends the RAPS (NR) message stops sending messages periodically and opens the previously blocked ports. The ring network has returned to its original normal state.

10.4. Technical features of ERPS

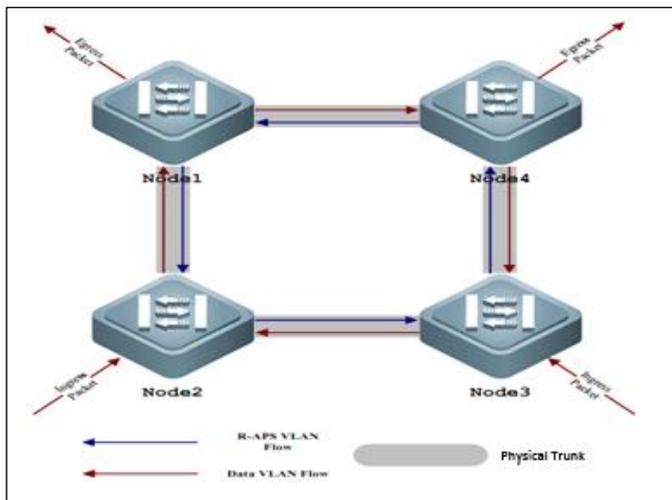
10.4.1. ERPS load balancing



With the switches in the same physical ring, we can configure multiple instances of ERPS rings. Each ERPS ring VLAN sends different (called VLAN protection) traffic. The network has two data networks with different VLAN IDs in each ring network being different, so as to achieve of load sharing. As shown in the figure above, a physical ring network corresponds to two instances of two ERPS rings, and two ERPS rings.

Each protects the VLAN differently. Node 2 is the RPL Owner node of ERP1, and Node3 is ERP2 RPL Owner node. By configuring, two different VLANs the network can be used to block different links, so as to realize the load sharing of single loop.

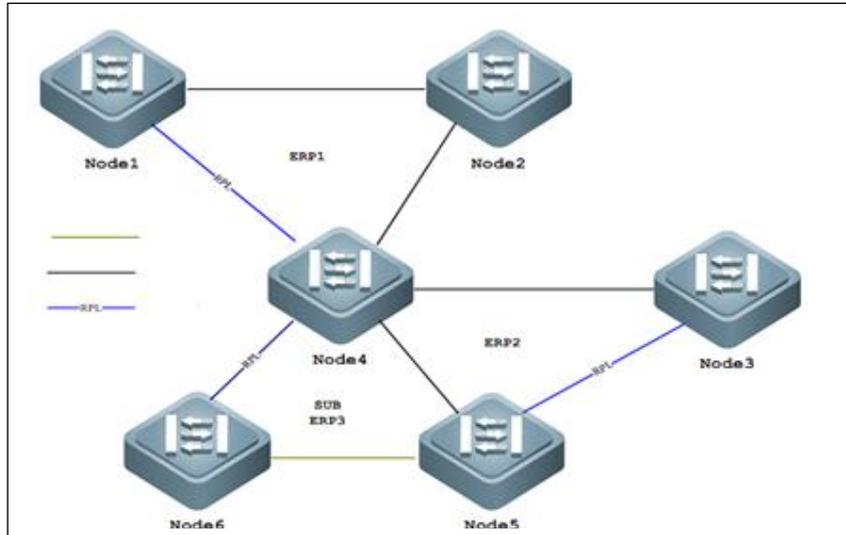
10.4.2. Good safety



There are two types of VLAN in ERPS, one is RAPS VLAN, and the other is a DATA VLAN. The RAPS VLAN is only used for transmitting ERPS protocol packets; ERPS also only deals with protocol packets from the RAPS VLAN. The RAPS VLAN does not handle any protocol attack packets from the DATA VLAN and improves the security of ERPS.

10.4.3. Multi-loop intersecting is supported

As shown in the figure below, ERPS supports the addition of multiple rings in the same node (Node4) as tangent or intersection, greatly increasing the flexibility of networking.



10.5. ERPS protocol commands

Command	Description	CLI mode
erps <1-8>	Create an instance of ERPS	Global configuration mode
no erps <1-8>	Deleting an instance of ERPS	Global configuration mode
node-role (interconnection none-interconnection)	The role of the configuration node in the ERPS loop, the interconnect node or the non-interconnect node	ERPS mode
ring <1-32>	Create a ERPS ring	ERPS mode
no ring <1-32>	Deleting a ERPS ring	ERPS mode
ring <1-32> ring-mode (major-ring sub-ring)	Configure the ERPS ring pattern, the main ring or the child ring	ERPS mode
ring <1-32> node-mode (rpl-owner-node rpl-neighbor-node ring-node)	Configure ERPS ring node pattern, RPL Owner node, RPL neighbor node or common ring node	ERPS mode
ring <1-32> raps-vlan <2-4094>	Configuring ERPS ring protocol VLAN	ERPS mode
no ring <1-32> raps-vlan	Deleting ERPS ring protocol VLAN	ERPS mode
ring <1-32> traffic-vlan <1-4094>	Configuring ERPS ring data VLAN	ERPS mode
no ring <1-32> traffic-vlan <1-4094>	Deleting ERPS ring data VLAN	ERPS mode

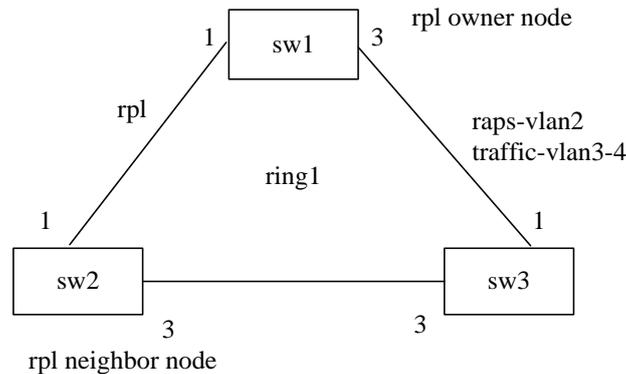
Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

ring <1-32> (rpl-port rl-port) IFNAME	Configure ERPS ring port, RPL port or common ring port	ERPS mode
no ring <1-32> (rpl-port rl-port)	Delete ERPS ring port	ERPS mode
ring <1-32> revertive-behaviour (revertive non-revertive)	Configuring ERPS loops to restore behaviour can be recoverable or not recoverable	ERPS mode
ring <1-32> hold-off-time <0- 10000>	Configuring ERPS ring hold- off time	ERPS mode
no ring <1-32> hold-off-time	Restore ERPS ring hold-off default time	ERPS mode
ring <1-32> guard-time <10- 2000>	Configuring ERPS ring guard time	ERPS mode
no ring <1-32> guard-time	Restore ERPS ring guard default time	ERPS mode
ring <1-32> wtr-time <1-12>	Configuring ERPS ring WTR time	ERPS mode
no ring <1-32> wtr-time	Restore ERPS ring WTR default time	ERPS mode
ring <1-32> wtb-time <1-10>	Configuring ERPS ring WTB time	ERPS mode
no ring <1-32> wtb-time	Restore ERPS ring WTB default time	ERPS mode
ring <1-32> raps-send-time <1- 10>	Configuring ERPS ring protocol packet delivery time	ERPS mode
no ring <1-32> raps-send-time	Restore ERPS ring protocol message default sending time	ERPS mode
ring <1-32> (enable disable)	Turn on or off the ERPS ring	ERPS mode
ring <1-32> forced-switch IFNAME	Forced switching ERPS ring port	ERPS mode
ring <1-32> clear forced-switch	Forced handoff of clear ERPS ring	ERPS mode
ring <1-32> manual-switch IFNAME	Manually switch the ERPS ring port	ERPS mode
ring <1-32> clear manual-switch	Manual switching to clear ERPS ring	ERPS mode
ring <1-32> clear recovery	Manual restoration of ERPS loop's non recoverable behaviour or manual recovery prior to WTR/WTB expiration	ERPS mode
show erps	Display all the ERPS instances and loops in the device	Privileged mode
show erps <1-8>	Display device single ERPS instance and loop details	Privileged mode

10.6. Typical use of ERPS

10.6.1. Example of single ring

The following diagram: SW1, SW2 and SW3 nodes constitute a single ERPS ring called Ring 1. Ports 1 and 3 of each node are the ERPS ring ports using protocol VLAN is 2 to send ERPS traffic. The Data VLAN IDs are 3 and 4 and are used for the network traffic. SW1 is the RPL Owner, SW2 is the RPL Neighbour, SW1 and SW2 is a Transit node.



(1) Configuring SW1:

```
Switch>enable
```

```
Switch#configure terminal
```

Creating ERPS protocol and data VLAN

```
Switch(config)#vlan database
```

```
Switch(config-vlan)#vlan 2-4
```

```
Switch(config-vlan)#exit
```

Configure ring port VLAN mode as trunk, join ERPS protocol and data VLAN

```
Switch(config)# interface xe1/1
```

```
Switch(config-xe1/1)# switchport mode trunk
```

```
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
```

```
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
```

```
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
```

```
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
```

```
Switch(config-xe1/1)#exit
```

```
Switch(config)# interface xe1/3
```

```
Switch(config-xe1/3)# switchport mode trunk
```

```
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
```

```
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
```

```
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
```

```
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
```

```
Switch(config-xe1/3)#exit
```

Configure ERPS instance 1, ERPS single ring 1

```
Switch(config)#erps 1
```

```
Switch(config-erps-1)#ring 1
```

```
Switch(config-erps-1)# ring 1 ring-mode major-ring
```

```
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node
```

```
Switch(config-erps-1)# ring 1 raps-vlan 2
```

```
Switch(config-erps-1)# ring 1 traffic-vlan 3
```

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

```
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

(2) Configuring sw2:

```
Switch>enable
Switch#configure terminal
Creating ERPS protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure ring port VLAN mode as trunk, join ERPS protocol and data VLAN
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure ERPS instance 1, ERPS single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-neighbor-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

(3) Configuring SW3:

```
Switch>enable
Switch#configure terminal
Creating ERPS protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure ring port VLAN mode as trunk, join ERPS protocol and data VLAN
```

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

```

Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure ERPS instance 1, ERPS single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit

```

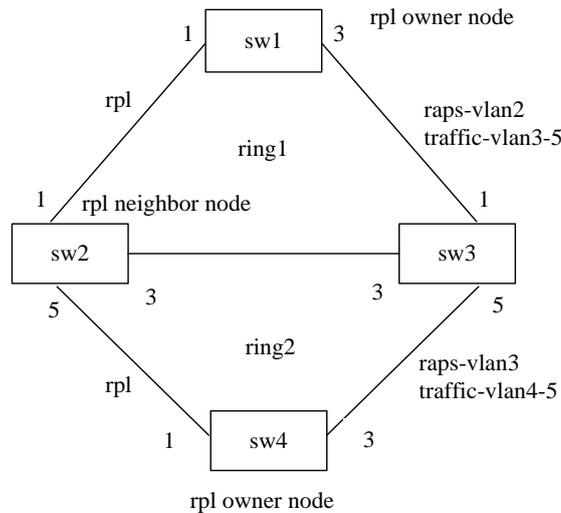
10.6.2. Multi ring example

In the following diagram, SW1, SW2 and SW3 nodes are in the ERPS main ring called Ring1 and use ports 1 and 3 for the ERPS ring. SW1 is the RPL Owner and SW2 is the RPL Neighbour and the link between them is the RPL link. This ring uses VLAN 2 for ERPS traffic and VLANs3, 4 and 5 for network traffic.

SW4 is the RPL Owner for Ring 2 and SW2 and SW3 are also members of ring2 with SW2 also being the RPL Neighbour for Ring 2. Ring 2 using VLAN 5 for ERPS traffic and VLANs 4 and 5 for network traffic.

Ring 2 is not configured to allow VLAN 2 (Ring 1 ERPS traffic) through to Switch 4. However, Ring 1 is configured to allow VLAN 3 (Ring 2 ERPS traffic) this is done to allow a virtual channel for Ring2 ERPS traffic.

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch



(1) Configuring SW1:

```
Switch>enable
```

```
Switch#configure terminal
```

Creating ERPS protocol and data VLAN

```
Switch(config)#vlan database
```

```
Switch(config-vlan)#vlan 2-5
```

```
Switch(config-vlan)#exit
```

Configure ring port VLAN mode as trunk, join ERPS protocol and data VLAN

```
Switch(config)# interface xe1/1
```

```
Switch(config-xe1/1)# switchport mode trunk
```

```
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
```

```
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
```

```
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
```

```
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
```

```
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
```

```
Switch(config-xe1/1)#exit
```

```
Switch(config)# interface xe1/3
```

```
Switch(config-xe1/3)# switchport mode trunk
```

```
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
```

```
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
```

```
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
```

```
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
```

```
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
```

```
Switch(config-xe1/3)#exit
```

Configure ERPS instance 1, ERPS main ring 1

```
Switch(config)#erps 1
```

```
Switch(config-erps-1)#ring 1
```

```
Switch(config-erps-1)# ring 1 ring-mode major-ring
```

```
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node
```

```
Switch(config-erps-1)# ring 1 raps-vlan 2
```

```
Switch(config-erps-1)# ring 1 traffic-vlan 3
```

```
Switch(config-erps-1)# ring 1 traffic-vlan 4
```

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

```
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

(2) Configuring SW2:

```
Switch>enable
Switch#configure terminal
Creating ERPS protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-5
Switch(config-vlan)#exit
Configure ring port VLAN mode as trunk, join ERPS protocol and data VLAN
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Switch(config)# interface xe1/5
Switch(config-xe1/5)# switchport mode trunk
Switch(config-xe1/5)# switchport trunk allowed vlan add 3
Switch(config-xe1/5)# switchport trunk allowed vlan add 4
Switch(config-xe1/5)# switchport trunk allowed vlan add 5
Switch(config-xe1/5)# switchport trunk allowed vlan remove 1
Switch(config-xe1/5)#exit
Configure ERPS instance 1, ERPS main ring 1, sub ring 2
Switch(config)#erps 1
Switch(config-erps-1)# node-role interconnection
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-neighbor-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
```

```
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode ring-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port xe1/5
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit
```

(3) Configuring SW3:

```
Switch>enable
Switch#configure terminal
Creating ERPS protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-5
Switch(config-vlan)#exit
Configure ring port VLAN mode as trunk, join ERPS protocol and data VLAN
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Switch(config)# interface xe1/5
Switch(config-xe1/5)# switchport mode trunk
Switch(config-xe1/5)# switchport trunk allowed vlan add 3
Switch(config-xe1/5)# switchport trunk allowed vlan add 4
Switch(config-xe1/5)# switchport trunk allowed vlan add 5
Switch(config-xe1/5)# switchport trunk allowed vlan remove 1
Switch(config-xe1/5)#exit
Configure ERPS instance 1, ERPS main ring 1, sub ring 2
Switch(config)#erps 1
Switch(config-erps-1)# node-role interconnection
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
```

```
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode ring-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port xe1/5
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit
```

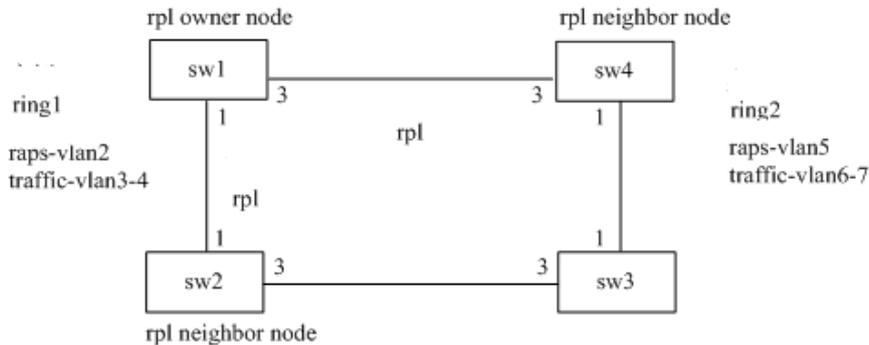
(4) Configuring SW4:

```
Switch>enable
Switch#configure terminal
Creating ERPS protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 3-5
Switch(config-vlan)#exit
Configure ring port VLAN mode as trunk, join ERPS protocol and data VLAN
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure ERPS instance 1, ERPS sub ring 2
Switch(config)#erps 1
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode rpl-owner-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port xe1/1
Switch(config-erps-1)# ring 2 rl-port xe1/3
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit
```

10.6.3. Multi instance load balancing example

In the following diagram, SW1, SW2, SW3 and SW4 nodes constitute an ERPS single loop Ring1. Ports 1 and 3 of each node are the ERPS ring ports. Protocol VLANs are 2 and 5, the data VLANs are 3 and 4. SW1 node is the RPL Owner node, SW2 node is the RPL Neighbour node, the link between SW1 and SW2 is the RPL link.

SW1, SW2, SW3 and SW4 nodes constitute an ERPS a single loop Ring2. Using ports 1, and 3 ports of each node as the ERPS ring port. protocol VLAN is 5. VLAN 6 & 7 is used for data. SW1 node is the RPL Owner node. SW4 node is RPL Neighbour node. The RPL Link is between SW4 and SW1.



(1) Configuration instance 1.

Configuring SW1 :

Switch>enable

Switch#configure terminal

Creating ERPS protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-4

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPS protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 2

Switch(config-xe1/1)# switchport trunk allowed vlan add 3

Switch(config-xe1/1)# switchport trunk allowed vlan add 4

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 2

Switch(config-xe1/3)# switchport trunk allowed vlan add 3

Switch(config-xe1/3)# switchport trunk allowed vlan add 4

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Configure ERPS instance 1, ERPS single ring 1

Switch(config)#erps 1

Switch(config-erps-1)#ring 1

Switch(config-erps-1)# ring 1 ring-mode major-ring

Switch(config-erps-1)# ring 1 node-mode rpl-owner-node

```

Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
Configuring SW2:
Switch>enable
Switch#configure terminal
Creating ERPS protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure ring port VLAN mode as trunk, join ERPS protocol and data VLAN
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure ERPS instance 1, ERPS single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-neighbor-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
Configuring SW3:
Switch>enable
Switch#configure terminal
Creating ERPS protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure ring port VLAN mode as trunk, join ERPS protocol and data VLAN

```

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

```

Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure ERPS instance 1, ERPS single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
Configuring SW4:
Switch>enable
Switch#configure terminal
Creating ERPS protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure ring port VLAN mode as trunk, join ERPS protocol and data VLAN
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure ERPS instance 1, ERPS single ring 1

```

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

(2) Configuration instance 2:

Configuring SW1 :

```
Switch>enable
```

```
Switch#configure terminal
```

Creating ERPS protocol and data VLAN

```
Switch(config)#vlan database
```

```
Switch(config-vlan)#vlan 5-7
```

```
Switch(config-vlan)#exit
```

Configure ring port VLAN mode as trunk, join ERPS protocol and data VLAN

```
Switch(config)# interface xe1/1
```

```
Switch(config-xe1/1)# switchport mode trunk
```

```
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
```

```
Switch(config-xe1/1)# switchport trunk allowed vlan add 6
```

```
Switch(config-xe1/1)# switchport trunk allowed vlan add 7
```

```
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
```

```
Switch(config-xe1/1)#exit
```

```
Switch(config)# interface xe1/3
```

```
Switch(config-xe1/3)# switchport mode trunk
```

```
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
```

```
Switch(config-xe1/3)# switchport trunk allowed vlan add 6
```

```
Switch(config-xe1/3)# switchport trunk allowed vlan add 7
```

```
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
```

```
Switch(config-xe1/3)#exit
```

Configure ERPS instance 2, ERPS single ring 2

```
Switch(config)#erps 2
```

```
Switch(config-erps-2)#ring 2
```

```
Switch(config-erps-2)# ring 2 ring-mode major-ring
```

```
Switch(config-erps-2)# ring 2 node-mode rpl-owner-node
```

```
Switch(config-erps-2)# ring 2 raps-vlan 5
```

```
Switch(config-erps-2)# ring 2 traffic-vlan 6
```

```
Switch(config-erps-2)# ring 2 traffic-vlan 7
```

```
Switch(config-erps-2)# ring 2 rpl-port xe1/3
```

```
Switch(config-erps-2)# ring 2 rl-port xe1/1
```

```
Switch(config-erps-2)# ring 2 enable
```

```
Switch(config-erps-2)#exit
```

Configuring SW2:

```
Switch>enable
```

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Switch#configure terminal

Creating ERPS protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 5-7

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPS protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 5

Switch(config-xe1/1)# switchport trunk allowed vlan add 6

Switch(config-xe1/1)# switchport trunk allowed vlan add 7

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 5

Switch(config-xe1/3)# switchport trunk allowed vlan add 6

Switch(config-xe1/3)# switchport trunk allowed vlan add 7

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Configure ERPS instance 2, ERPS single ring 2

Switch(config)#erps 2

Switch(config-erps-2)#ring 2

Switch(config-erps-2)# ring 2 ring-mode major-ring

Switch(config-erps-2)# ring 2 node-mode ring-node

Switch(config-erps-2)# ring 2 raps-vlan 5

Switch(config-erps-2)# ring 2 traffic-vlan 6

Switch(config-erps-2)# ring 2 traffic-vlan 7

Switch(config-erps-2)# ring 2 rpl-port xe1/1

Switch(config-erps-2)# ring 2 rl-port xe1/3

Switch(config-erps-2)# ring 2 enable

Switch(config-erps-2)#exit

Configuring SW3:

Switch>enable

Switch#configure terminal

Creating ERPS protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 5-7

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPS protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 5

Switch(config-xe1/1)# switchport trunk allowed vlan add 6

Switch(config-xe1/1)# switchport trunk allowed vlan add 7

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

```

Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan add 6
Switch(config-xe1/3)# switchport trunk allowed vlan add 7
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure ERPS instance 2, ERPS single ring 2
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode ring-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port xe1/1
Switch(config-erps-2)# ring 2 rl-port xe1/3
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
Configuring SW4:
Switch>enable
Switch#configure terminal
Creating ERPS protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
Configure ring port VLAN mode as trunk, join ERPS protocol and data VLAN
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 5-7
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 5-7
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure ERPS instance 2, ERPS single ring 2
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode rpl-neighbor-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port xe1/3
Switch(config-erps-2)# ring 2 rl-port xe1/1
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit

```

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

11. AAA configuration

This chapter describes how to configure the 802.1x and RADIUS of switches to prevent unauthorised users from accessing the network. For the use of the 802.1x client and HyperBoss, see the respective operating manuals. The main contents of this chapter are as follows:

- 802.1x introduce
- RADIUS introduce
- Configuring 802.1x
- configuration RADIUS

AAA is an abbreviation of Authentication, Authorisation and Authentication (Authorization, and Accounting). It provides a consistent framework for configuring authentication, authorisation, and billing for these three security functions. The configuration of AAA is actually part of network security, where network security mainly refers to access control. Which users can access the network? What services can users get access to? How to account for the users who are using the network resources?

Authentication (Authentication): verify whether the user can access access.

Authorization (Authorization): what services can authorized users use?

Accounting (Accounting): recording the user's use of network resources.

The network company launched a set of AAA solutions, the product has 802.1x client, a variety of supporting authentication switches and authentication billing system HyperBoss. The 802.1x client is installed on the PC which users access to the Internet. When the user needs to access the network, it needs to use the 802.1x client to authenticate. Only the authenticated user can use the network.

AAA is an authentication exchange, which receives the authentication request of client, transfers the username and password to the authentication and billing system HyperBoss, and the switch itself doesn't do the actual authentication work. HyperBoss receives the authentication request sent by the switch and carries out the actual authentication and carries on the billing processing to the successful authentication user.

The 802.1x protocol is used between the 802.1x client and the switch to communicate, and the RADIUS protocol is used between the switch and the HyperBoss.

11.1 802.1x introduction

The 802.1x protocol is based on access control and authentication protocol port, the port refers to the logical port and can be a physical port, MAC address or VLAN ID. The network switch realization is based on the MAC address and the port is based on 802.1x Protocol.

802.1x is a two-layer protocol, the authenticated switch and the user's PC must be in the same subnet and the protocol packet cannot cross the network segment. 802.1x authentication uses the model of client server and must have a server to authenticate all users.

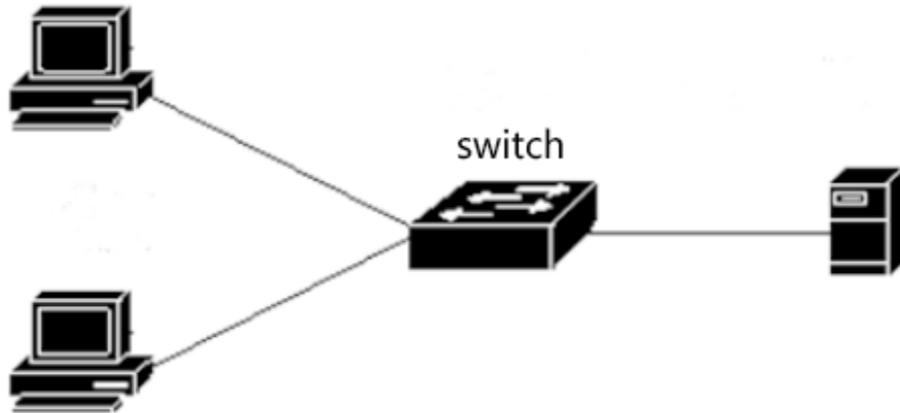
In MAC mode, the user goes through the authentication, as before, only authentication flow can go through the switch port, only after successful authentication, data can flow through the switch port, which means that users must access the network after the adoption of the certification. In Port mode, you can open the Guest VLAN function. The default is closed.

Turn off Guest VLAN and MAC data through the same pattern, but after authentication opens the port, with an un-registered MAC address; open the Guest VLAN when the user is authenticated before data is sent by the Guest VLAN, the authentication succeeds, by Auth Vlan, this method can be used to specify the scope of limited access limited user authentication before, after the public network access authentication.

11.1.1 802.1x device composition

802.1x consists of three parts:

- Client (Supplicant System).
- Authentication system (Authenticator System).
- Authentication server (Authentication Server System).
- As shown in the following picture.



The client (supplicant system) - requests access to network equipment, in general user terminal system, such as PC users, the user terminal system must install an 802.1x client software.

The client initiates the 802.1x authentication request and requests the authentication server to verify its user name and password. If the authentication is successful, the user can access the network.

The Authentication system - refers to authenticated devices, such as switches. The user authentication system by logical port (refer to the MAC address) state control whether a user can access the network, if the user is non logical port state authority, the user cannot access the network, if the user is authorised to a logical port state, the user can access the network.

Authentication system - is a relay between the client and the authentication server. The authentication system requests the identity information from the user and forwards the identity information of the user to the authentication server. It then forwards the authentication result sent by the authentication server to the client.

The server system needs to implement the 802.1x protocol near the users. The client part of the authentication server implements the RADIUS protocol. The RADIUS protocol client authentication system 802.1x client sends EAP information to the authentication server in RADIUS, and from the authentication server to the RADIUS protocol in the EAP information solution package out and sent by the 802.1x server to 802.1x client.

The Authentication server refers to the device that actually authenticates the user. Identity authentication server receives the user authentication system and verifies it, if authentication is successful. The authentication server authorisation authentication system allows the user to access the network, if authentication fails, the authentication server authentication system tells the user that authentication has failed. The user cannot access the network. Communication between the authentication server and authentication system through EAP extended RADIUS protocol. network provides authentication and billing system, HyperBoss authentication and billing for users.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

11.1.2 Brief introduction of protocol package

The 802.1x protocol authentication data transmission on the network flow is EAPOL (EAP Over LAN) frame format, all the user identity information (including user name and password) is encapsulated in EAP (Extensible Authentication Protocol), EAP encapsulated in EAPOL frames. The username exists in the form of plaintext in the EAP, and the password exists in the form of MD5 encryption in the EAP.

The frame format of EAPOL is as follows. PAE Ethernet Type is the Ethernet protocol type number of EAPOL, and the value is 0x888E. Protocol Version is the EAPOL version number, which is 1. Packet Type refers to the type of EAPOL frame. Packet Body Length is the length of the EAPOL frame content. Packet Body refers to the content of the EAPOL frame.

	Octet Number
PAE Ethernet Type	1-2
Protocol Version	3
Packet Type	4
Packet Body Length	5-6
Packet Body	7-N
EAPOL Frame Format	

Switches use three EAPOL protocol frames, respectively:

The value of EAPOL-Start:Packet Type is 1 - the authentication frame is initiated, and when the user needs authentication, the frame is first launched, and the client is sent to the switch.

The value of EAPOL-Logoff:Packet Type is 2 - The request frame is exited and the frame is notified when the user does not need to use the network.

The value of EAP-Packet:Packet Type is 0 - and the authentication information frame is used to bear authentication information.

EAP package format as follows.

- Code refers to the type of EAP package, including Request, Response, Success and Failure.
- Identifier refers to identifiers, which are used to match Response and Request. Length refers to the length of the EAP packet, including Baotou. Data refers to the EAP packet data.

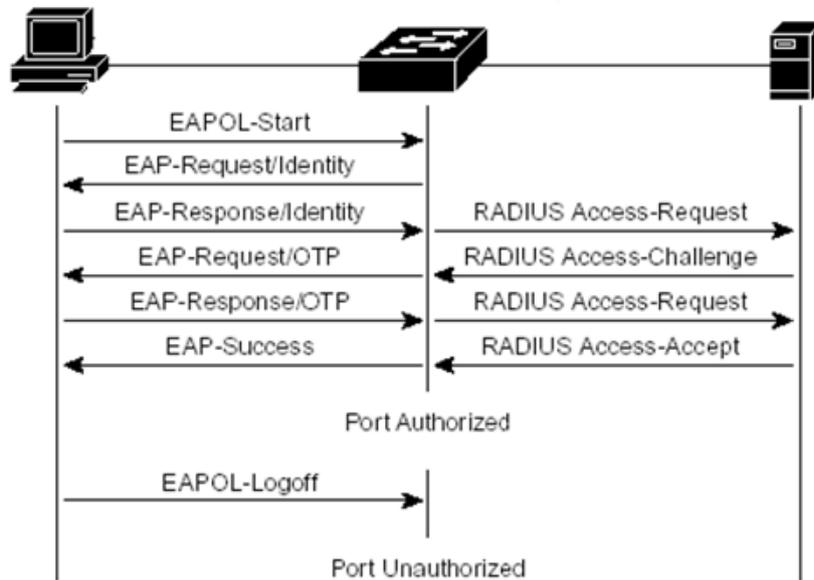
The EAP package consists of the following four types:

- The EAP-Request:Code value is 1, the EAP requests the packet and requests the user name and / or password from the switch to the client.
- The EAP-Response:Code value is 2, the EAP response packet is sent from the client to the switch, and the user name and / or password are sent to the switch.
- EAP-Success:Code value is 3, EAP is successfully packaged, sent from the switch to the client, told the client user authentication success.
- The EAP-Failure:Code value is 4, the EAP failure packet is sent from the switch to the client, and the client is told that the authentication failed.

	Octet Number
Code	1
Identifier	2
Length	3-4
Data	5-N
EAP Packet Format	

11.1.3 Protocol flow interaction

When the switch enables 802.1x and the port state is ‘Auto’, all access users accessing the port must pass authentication to access the network. The protocol interaction as shown below.



Client initiated authentication protocol interaction

When users need to access the network, the client first sends the following;

EAPOL-Start to exchange - requests received after the authentication request authentication.

The switch sends the EAP-Request - requests user name.

The client sends an EAP-Response - switch EAP information extracted from the package in the RADIUS.

The RADIUS send an Access Challenge - to the authentication server.

The authentication server requests the user password.

The switch sends an EAP-Request to the client to request user password.

The client EAP-Response - echo switch, EAP information is encapsulated in the RADIUS authentication server.

The authentication server - authenticates the user name and password. If the authentication is successful, the authentication server notifies the switch.

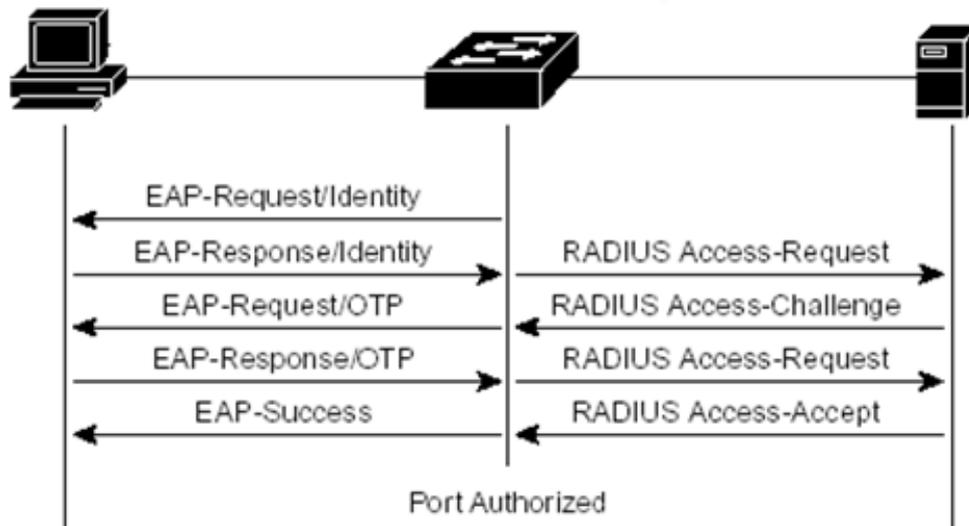
The switch sends EAP Success - to the client and the user's logical port is in the authorised state.

When the client receives EAP Success - the authentication is successful, and the user can access the network.

When the user no longer needs to use the network, the client sends EAPOL-Logoff to the switch, and the switch transfers the user's logical port state to an unauthorized state, when the user can no longer access the network.

In order to prevent the abnormal client offline, the switch provides a mechanism for re-certification, the time interval can be set in the “re-certification” setting on the switch, when the authentication time arrives, the switch initiates re-certification, if authentication is successful, the user can continue to use the network, if authentication fails, the user cannot use the network.

The Protocol interaction as shown below.



Authenticated protocol interaction

11.1.4 802.1x port state

The port state is the physical port state of the switch. There are four states in the physical port of the switch:

- N/A state,
- Auto state,
- Force-authorized state,
- Force-unauthorized state.

When the switch does not open the 802.1x, all ports are in the N/A state. When the switch port is set into Auto state, Force-authorized state or Force-unauthorized state, 802.1x must first be enabled.

N/A State - When the port on the switch is in the N/A state, all the users under the port can access the network without authentication. If the switch receives an 802.1x protocol packet from the port, the protocol packets are discarded.

Force-Authorisation State - When the port of the switch is in the Force-authorized state, all the users under the port can access the network without authentication. When the switch receives the EAPOL-Start packet from the port, the switch sends the EAP-Success packet. When the switch receives the other 802.1x protocol packets from the port, the protocol packets are discarded.

Force un-authorized state - When the port of the switch is in the Force-unauthorized state, all users under the port cannot access the network at any time, and the authentication request will never be passed. When the switch receives the 802.1x protocol packet from the port, the protocol packets are discarded.

Auto State - When the port on the switch is in the 'Auto' state, the authentication mode should be in Port mode, if the Guest VLAN is not configured, the user port must access the network through certification, closing the port if not certified;

Using the configuration for the Guest VLAN port, the user can access Auth VLAN through certification. If not certified they can access the Guest VLAN. All users under the port must be authenticated to access the network. The interaction of the 802.1x protocol is shown in the

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

diagram. If the user needs authentication, the port is generally set to the Auto state.

When the switch port is set to the Auto state, and anti-spoofing is enabled ARP function; anti spoofing ARP function will control the IP package, MAC source and source IP are consistent with the information provided by the client authentication data packet and ARP packet's sender IP and MAC are in line with the sender authentication client provides information packets to is this port forwarding, otherwise it will be discarded.

This function must be configured as static in the client's configuration IP address, if it is to obtain an IP address through the DHCP protocol dynamic circumstances to achieve this function to enable the DHCP SNOOPING protocol; if you need more details please refer to the IP MAC binding configuration.

11.2 RADIUS introduction

When the user authenticates, the exchange and the authentication server interact with the RADIUS protocol that supports the EAP extension. The RADIUS protocol uses client / server model, switches need to implement the RADIUS client, and authentication server needs to implement the RADIUS server.

In order to ensure the security of the interaction between the switch and the authentication server, and to prevent the interaction between illegal switches or illegal authentication servers, mutual authentication between the switch and the authentication server is needed. The switch and the authentication server need the same key, when the switch or the authentication server sends the RADIUS protocol packets, all packets according to the key using the HMAC algorithm to generate a message digest, when the switch and the authentication server receives the RADIUS protocol packet, all protocol packets to verify the message digest using the key, if verified by that is, the legal RADIUS, otherwise it is illegal RADIUS packets discarded.

The main contents of this section are as follows :

- Brief introduction of protocol package
- Protocol flow interaction
- User authentication method

11.2.1 Brief introduction of protocol package

The RADIUS protocol is based on UDP and encapsulates authentication information and billing information. The early RADIUS authentication port is 1645, while the current use port 1812, the early RADIUS billing port is 1646, the current use port 1813.

Because RADIUS is hosted on UDP, RADIUS has a timeout retransmission mechanism. At the same time, in order to improve the reliability of communication between authentication system and RADIUS server, two RADIUS server schemes are adopted, that is to say, a mains and a standby server mechanism is adopted.

The RADIUS message format is as follows.

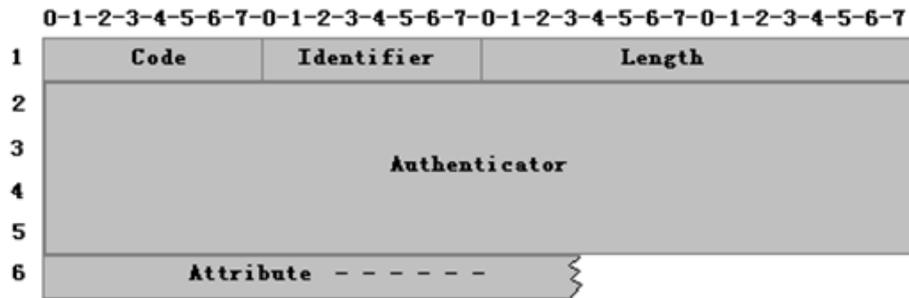
Code - refers to the type of RADIUS protocol message.

Identifier index - identifier for matching requests and responses.

Length - refers to the length of the entire message (including the header).

Authenticator - is a 16 byte string, a random number for the request packet, and a message digest for the response packet that is generated by MD5.

Attribute - refers to the attributes in the RADIUS protocol package.



RADIUS message format

The network uses the following RADIUS protocol packages :

The Access-Request:Code - value is 1, the authentication request packet is sent to the authentication server from the authentication system, and the user name and password are encapsulated on the package.

The Access-Accept:Code - value is 2, from the authentication server to the response packet of the authentication system, which means the user authentication is successful.

The Access-Reject:Code - value is 3, and the authentication packet is sent to the authentication system from the authentication server, which indicates the failure of user authentication.

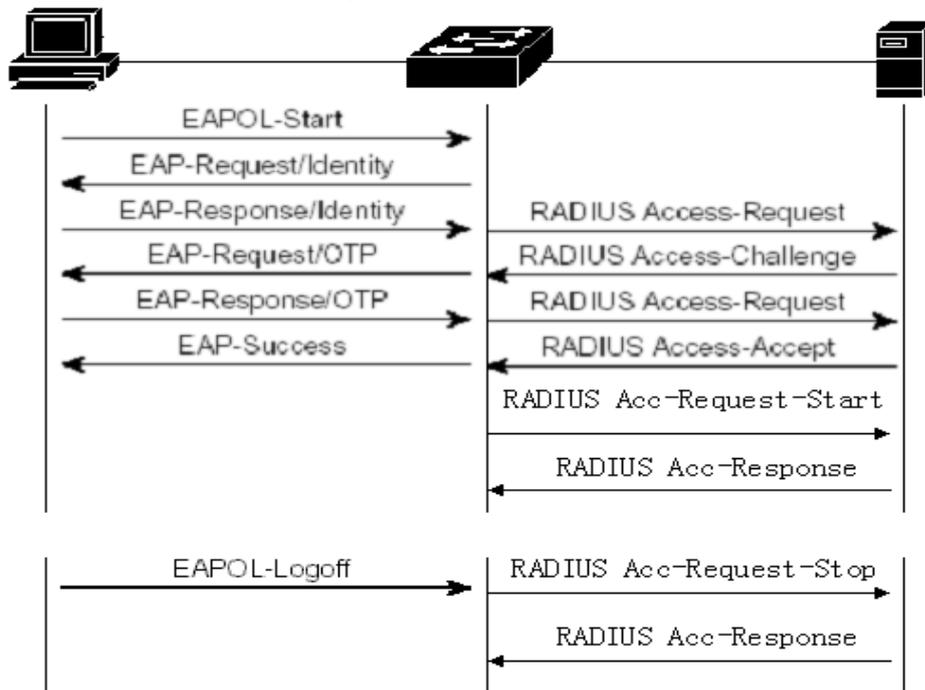
The Access-Challenge:Code - value is 11, from the authentication server to the response packet of the authentication system, which indicates that the authentication server needs further information of the user, such as passwords.

The Accounting-Request:Code - value is 4, and the billing request package from the authentication system is sent to the authentication server, including the start billing and the end billing package, and the billing information is encapsulated on the package.

The Accounting-Response:Code - value is 5, from the authentication server to the billing response package of the authentication system, which indicates that the billing information has been received.

11.2.2 Protocol flow interaction

When the user initiates authentication, the authentication system and the authentication server interact with each other through the RADIUS protocol. The authentication system does not send the protocol flow of the RADIUS billing package as shown in the diagram below. Generally, when the user authentication is successful or the user is offline, the authentication system needs to send the RADIUS billing package to the authentication server, and the protocol flow interaction is shown in the following picture.



Authenticate user - the user device sends a EAPOL start request to the switch, the switch request the user’s identity. This identity is sent to the RADIUS server for verification. The RADIUS server issues a challenge to the request to the switch. The switch requests a password form the user; the user then sends the password to the switch. The switch sends an access request to the RADIUS server which then accept as the request to the switch. The switch then sends a success response to the user and the user is granted access to the network.

The switch then sends an accounting start request to the RADIUS server which acknowledges the request.

When the user wants to leave the network an EAPOL logoff message is sent to the switch and the switch disables access by the user and sends an accounting stop request to the RADIUS server.

11.2.3 User authentication method

There are three kinds of user authentication methods for RADIUS :

- **PAP** (Password Authentication Protocol). The user passes the user name and his password to the switch in the form of plain text. The switch passes the user name and password to the RADIUS server through the RADIUS protocol package, and the RADIUS server looks in the database. If there is the user name and password, it indicates that the authentication is passed, otherwise it indicates that the authentication has not passed.
- **CHAP** (Challenge Handshake Authentication Protocol). When the user requests access the network, the switch generates a 16 byte random code to the user. The user encrypts the random code, password, and other domains to generate a response, passing the username and response to the switch. The switch passes the username, the response, and the original 16 byte random code to the RADIUS server. According to the RADIUS username in the switch, it searches its database, and end users use the same password encryption, (based on random code of 16 bytes,) and the results from the response comparison showed that if the same is verified, if not the same that validation failed.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

- **EAP (Extensible Authentication Protocol)** - With this verification method, the switch doesn't really participate in the verification, and only forwards authentication packets between the user and the RADIUS server.
When a user requests access the authentication request is sent to the switch which is sent as is to the RADIUS server. The RADIUS server generates a 16 byte random code to the user and stores the random code. The user generates a random code, response encryption password and other domain, the user name and the response to the switch. The switch forwards all this to the RADIUS server. According to the RADIUS username in the switch side search database, and end users use the same password encryption, and then encrypted according to random code stored 16 bytes, and the results from the response comparison showed that if the same is verified and access granted, if not the same then validation failed and access with denied..

The authentication and billing solution of network adopts the method of EAP user authentication.

11.3 Configuring 802.1x

This section gives a detailed description of the configuration of 802.1x, including the following :

- 802.1x default configuration
- Start and close 802.1x
- Configuring 802.1x port status
- Configuring 802.1x port authentication
- Configuring 802.1x port guest VLAN
- Configuration re authentication mechanism
- Maximum number of configuration port access host
- Configure interval times and resend times
- Configuration port is the transport port
- Configuring the 802.1x client version number
- Configure whether to check the client version number
- Configuration authentication method
- Configure whether to check the client's timing packet
- Display 802.1x information

11.3.1 802.1x default configuration

The switch 802.1x configuration defaults as follows :

- 802.1x is closed.
- The state of all ports is N/A.
- The authentication mechanism is closed, and the authentication interval is 3600 seconds.
- The maximum number of access hosts for all ports is 100.
- The timeout interval of EAP-Request retransmission is 30 seconds.
- The number of timeout retransmission EAP-Request is 3 times.
- The user authentication failed waiting for 60 seconds.
- The timeout interval of the server timeout is 10 seconds.

The switch provides a command in the global CONFIG mode to return all the configuration back to the default state. The commands are as follows:

Switch(config)#dot1x default

11.3.2 Start and close 802.1x

The first step in configuring 802.1x is to start 802.1x. In the global CONFIG mode, enter the following command to start 802.1x:

```
Switch(config)#dot1x
```

When the 802.1x is closed, all port States return to the N/A state. In global CONFIG mode, enter the following command to close 802.1x:

```
Switch(config)#no dot1x
```

11.3.3 Configuring 802.1x port status

You must start 802.1x before setting 802.1x port state. If all users under the port must be authenticated to access the network, the port must be set to the Auto state.

The following command sets port ge1/1 to Auto state in the interface configuration mode and enables anti ARP spoofing function:

```
Switch(config-ge1/1)dot1x control auto
```

If the configuration of anti ARP spoofing fails, it may be caused by the following reasons:

- 1、 System CFP resource exhaustion.
- 2、 The current interface is configured with the ACL filter function.
- 3、 The current interface enables the DHCP SNOOPING function.
- 4、 The configured interface is a three layer interface or a trunk interface.

The following command sets port ge1/1 to Force-authorized state in the interface configuration mode:

```
Switch(config-ge1/1)dot1x control force-authorized
```

The following command sets port ge1/1 to Force-unauthorized state in the interface configuration mode:

```
Switch(config-ge1/1)dot1x control force-unauthorized
```

The following command sets port ge1/1 to N/A state in the interface configuration mode:

```
Switch(config-ge1/1)no dot1x control
```

Note: if a port has bound the MAC address, then the port cannot be set to Auto, Force-authorized or Force-unauthorized state.

11.3.4 Configuring 802.1x port authentication

You must start 802.1x before you set up the 802.1x port authentication method. If the port is only connected to a user who needs authentication, the port is opened by authentication, and the port must be set to port base. If the authentication is based on the MAC address, it will be set to mac base. The default state is mac base.

The following command sets port ge1/1 to portbase state in the interface configuration mode:

```
Switch(config-ge1/1)dot1x method portbase
```

The following command sets port ge1/1 to macbase state in the interface configuration mode:

```
Switch(config-ge1/1)dot1x method macbase
```

11.3.5 Configuring 802.1x port guest VLAN

Before setting 802.1x port guest VLAN, you must start 802.1x, and configure ports for Auto state and portbase state. The guest VLAN can be accessed before the authentication of the user under the desired port. After the authentication, the configuration VLAN can be accessed, and then the port must be configured with guest VLAN.

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

It must be noted that guest VLAN only supports access mode, nor does it support trunk. Once the port is configured with guest VLAN, its mode cannot be modified, and guest VLAN cannot be configured in non-access mode. When configuring guest VLAN, you must ensure that the VLAN has been created. The following command sets the port guest VLAN to 2 in the interface configuration mode:

Switch(config-ge1/1)dot1x guest-vlan 2

11.3.6 Configuration re authentication mechanism

In order to prevent the client from being unaware of the switch and authentication server, the switch provides a re-authentication mechanism that initiates authentication once every other time interval. The following command starts the re authentication mechanism in the global CONFIG mode:

Switch(config)#dot1x reauthenticate

The following command closes the authentication mechanism in global CONFIG mode:

Switch(config)#no dot1x reauthenticate

The following command sets the time interval for re authentication in global CONFIG mode:

Switch(config)#dot1x timeout re-authperiod <interval>

Note: the interval between re authentication should not be too short, otherwise the network bandwidth and the CPU resource consumption of the switch will be too large.

11.3.7 Maximum number of configuration port access host

Each port of the switch can control the maximum number of access hosts. This function can restrict users to illegally access to the network by using multiple hosts. The maximum number of port access host defaults is 100, the maximum can be set to 100. If the maximum number of ports access host is set to 0, then the port rejects any user access.

The following command sets the maximum number of port ge1/1 access hosts in the interface configuration mode:

Switch(config-ge1/1)dot1x support-host <number>

11.3.8 Configure interval times and resend times

The 802.1x standard protocol states the time interval and the number of retransmissions. Switches using the standard time interval and the number of retransmissions. We suggest that users in the do not change the time interval and the number of retransmissions.

Tx-period - said the switch time interval repeat EAP-Request protocol package; max-req said the number of retransmission switch.

EAP-Request;- quiet-period represents the time interval of user authentication failure when waiting for re certification; server-timeout said the switch to the authentication server RADIUS packet retransmission time interval; supp-timeout said time interval of packet switches to the client EAP retransmission request.

The following command configures the interval and retransmission times in the global CONFIG mode:

Switch(config)#dot1x timeout tx-period <interval>

Switch(config)#dot1x max-req <number>

Switch(config)#dot1x timeout quiet-period <interval>

Switch(config)#dot1x timeout server-timeout <interval>

Switch(config)#dot1x timeout supp-timeout <interval>

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

11.3.9 Configuration port is the transport port

When the switch is not open to 802.1x authentication but in the network other switches are open to the 802.1x authentication the switch can be configured to forward 802.1x authentication requests to the authentication server. The switch can be configured to forward EAPo authentication packets between the client and the authentication of 802.1x switches. So as to enable the 802.1x authentication of other switches to the client.

The following command sets port ge1/1 as the transport port in the interface configuration mode :

Switch(config-ge1/1)dot1x transmit-port

The following command sets port ge1/1 as non-transport port in the interface configuration mode :

Switch(config-ge1/1)no dot1x transmit-port

11.3.10 Configuring the 802.1x client version number

Configure the version number of the 802.1x client. Only the client whose version is greater than the version number of the configuration can be authenticated, otherwise the authentication fails. The default client version number of the switch is 2.

The following command configures the client version number in global CONFIG mode :

Switch(config)# dot1x client-version <string>

11.3.11 Configure whether to check the client version number

Configure whether the switch should check the version number of the 802.1x client or not. If configured to check, the switch first checks the client version number when authenticating. The default is configured to check.

The following command configures the global CONFIG mode to open the check of the client version number :

Switch(config)# dot1x check-version open

11.3.12 Configuration authentication method

The authentication method of configuring the switch to 802.1x packet, (the client-initiated authentication method) is divided into universal authentication and extended authentication. The switch can be configured as the first as to which way authentication should occur. If the client-initiated authentication the method is inconsistent with the authentication method of the switch configuration, the client will initiate authentication after another failure of authentication.

The following command configures the authentication method of the switch in the global CONFIG mode to extend the authentication mode :

Switch(config)# dot1x extended

11.3.13 Configure whether to check the client's timing packet

Check whether the configuration of the client in the authentication succeeds, asks the client to regularly send 802.1x packets. Not all of the clients will regularly send 802.1x packets on certification through, this configuration through the command switch timing packet inspection of the client.

The following command is configured as a switch in the global CONFIG mode to check the client's timing packet :

Switch(config)# dot1x check-client

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

11.3.14 Display 802.1x information

The following command in the normal mode / privilege mode display 802.1x information, when the command is show dot1x, display 802.1x configuration information for all, including the configuration information for all ports; when the command is show dot1x interface, to display all the information user access port:

```
Switch#show dot1x
```

```
Switch#show dot1x interface
```

11.4 Configuration RADIUS

This section gives a detailed description of the configuration of RADIUS, including the following:

- RADIUS Default configuration
- Configuring the IP address of the authentication server
- Configuring shared keys
- Start and close billing
- Configuring RADIUS ports and attribute information
- Configuring RADIUS roaming function
- Display RADIUS information

11.4.1 RADIUS Default configuration

The RT series switch default RADIUS configuration is as follows:

- There is no IP address for the primary authentication server and the backup authentication server, that is, the IP address is 0.0.0.0.
- There is no configuration share key, that is, the shared key string is empty.
- Billing is initiated by default.
- RADIUS authentication UDP port is 1812, billing UDP port is 1813.
- The value of RADIUS attribute NASPort is 0xc353, the value of NASPortType is 0x0f, and the value of NASPortServer is 0x02.

11.4.2 Configuring the IP address of the authentication server

In order to communicate between the switch and the authentication server, the IP address of the authentication server needs to be configured on the switch. RADIUS. In practical applications, you can use an authentication server, you can also use two authentication servers, one as the main authentication server, one as backup authentication server. If the switch is configured with two authentication server IP addresses, when the switch and the main authentication server interrupt communication, you can switch to the backup authentication server communication.

The following command configures the IP address of the master authentication server in the global CONFIG mode:

```
Switch(config)#radius-server host <ip-address>
```

The following command configures the IP address of the backup authentication server in the global CONFIG mode:

```
Switch(config)#radius-server option-host <ip-address>
```

11.4.3 Configuring shared keys

Mutual authentication is needed between the switch and authentication server, and the same shared key is needed on the switch and authentication server. Note that the shared key on the

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

switch must be the same as the authentication server.

The following command configures the shared key of the switch in the global CONFIG mode:

Switch(config)#radius-server key <string>

11.4.4 Start and close billing

If the switch closes the billing, the switch will not send the RADIUS packet to the authentication server when the authentication is successful, or the user is offline. In general, billing is open in practical applications.

The following command initiates billing in global CONFIG mode:

Switch(config)#radius-server accounting

The following command closes billing in global CONFIG mode:

Switch(config)#no radius-server accounting

11.4.5 Configuring RADIUS ports and attribute information

It is recommended that users do not modify the RADIUS port and attribute information configuration.

The following command modifies the RADIUS authentication UDP port in the global CONFIG mode:

Switch(config)#radius-server udp-port <port-number>

The following command modifies the RADIUS attribute information in global CONFIG mode:

Switch(config)#radius-server attribute nas-portnum <number>

Switch(config)#radius-server attribute nas-porttype <number>

Switch(config)#radius-server attribute service-type <number>

11.4.6 Configuring RADIUS roaming function

When MAC, IP or VLAN binding is made to the client, when the client is moved to other places, the binding client cannot carry out 802.1x authentication because of the MAC address, IP address or VLAN change. Open the radius roaming function, will ignore the client's MAC, IP or VLAN binding, so as to continue to achieve 802.1x authentication.

The following command configures the RADIUS roaming function in the global CONFIG mode:

Switch(config)#radius-server roam

The following command closes the RADIUS roaming function in global CONFIG mode:

Switch(config)#no radius-server roam

11.4.7 Display RADIUS information

The following command displays RADIUS configuration information in normal mode / privilege mode:

Switch#show radius-server

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

11.5 Configuration example

Open the 802.1x protocol, configure the port ge1/1 is Auto state, configure the main authentication server is 198.168.80.111, configure the switch shared secret key is ABCDEF.

```
Switch#  
Switch# dot1x  
Switch#config t  
Switch(config)#radius-server host 198.168.80.111  
Switch(config)#radius-server key abcdef  
Switch(config)# interface ge1/1  
Switch(config-ge1/1)# dot1x control auto
```

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

12. GMRP Configuration

The main contents of this chapter are as follows :

- GMRP introduction
- GMRP configuration
- Examples of typical GMRP configurations

12.1 GMRP introduction

At present, GMRP (GARP Multicast Registration Protocol) is a multicast registration protocol based on GARP, which is used to maintain the multicast registration information in the switch. The GMRP switches can receive the multicast registration information from other switches, and dynamically update the local multicast registration information, but also to the local multicast registration information is spread to other switches. This information exchange mechanism ensures the consistency of multicast information maintained by all GMRP supported devices in the same switching network.

When a host wants to join a multicast group, it sends GMRP to join the message. The switch will receive the port of adding GMRP message to the multicast group and broadcast the GMRP into the message in the VLAN where the receiving port is located. The multicast source in VLAN can know the existence of multicast members. When the multicast source sends multicast packets to the multicast group, the switch only forwards the multicast packets to the ports connected to the multicast group members, thus realising the two layer multicast in the VLAN.

12.2 GMRP Configuration

The main configuration of GMRP includes :

- Open GMRP
- View GMRP

In configuration tasks, you must first open the global GMRP to open the port GMRP.

12.2.1 Open GMRP settings

Command	Description	Configuration mode
set gmrp enable disable	Enable / go global VLAN GMRP	Global configuration mode
set gmrp enable vlan <vlan-id>	Enabling globally specific VLAN GMRP	Global configuration mode
set gmrp registration {fixed forbidden normal} <if-name>	Configuring interface registration multicast mode	Global configuration mode
set gmrp timer {join leave nleaveall} <time-value>	The timing of configuring various timers	Global configuration mode
set port gmrp enable <if-name>	Enable port GMRP function	Global configuration mode
set port gmrp disable <if-name>	De enable port GMRP function	Global configuration mode

12.2.2 View GMRP information

After completing the above configuration, executing show command in any view can display the operation of GMRP after configuration, and verify the effect of configuration by checking the display information.

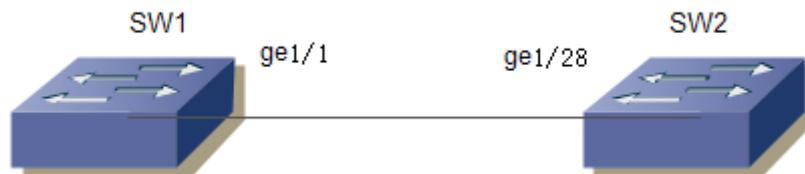
Command	Description	Configuration mode
show gmrp configuration	View GMRP configuration information	Privileged mode
show gmrp machine	View GMRP state machine information	Privileged mode
show gmrp statistics vlanid	See the GMRP statistics of specific vlanid	Privileged mode
show gmrp timer <ifname>	View timer information for specific ports	Privileged mode

12.3 Examples of typical GMRP configurations

1. Networking requirement

In order to realize dynamic registration and update of multicast information between switches, it is necessary to start GMRP on the switch

2. Network diagram



GMRP example network diagram

3. Configuration steps

Configuring SW1

Start global GMRP

Switch(config)# set gmrp enable

Start port GMRP on Gigabit Ethernet port ge1/1

Switch(config)# set port gmrp enable ge1/1

Switch(config)#

Configuring SW2

Start global GMRP

Switch(config)# set gmrp enable

Start port GMRP on Gigabit Ethernet port ge1/28

Switch(config)# set port gmrp enable ge1/28

Switch(config)#

13. SNOOPING configuration

A switch will, by default, flood multicast traffic to all the ports in a broadcast domain (or the VLAN equivalent). Multicast can cause an unnecessary load on host devices by requiring them to process packets they have not solicited. When purposefully exploited, this can form the basis of a denial-of-service attack. IGMP snooping is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. It provides switches with a mechanism to prune multicast traffic from links that do not contain a multicast listener (an IGMP client).

Essentially, IGMP snooping is a layer 2 optimisation for the layer 3 IGMP. IGMP snooping takes place internally on switches and is not a protocol feature.

IGMP snooping allows a switch to only forward multicast traffic to the links that have solicited them. Snooping is therefore especially useful for bandwidth-intensive IP multicast applications such as IPTV.

This chapter describes the concept and configuration of IGMP SNOOPING, including the following contents:

- IGMP SNOOPING introduction
- IGMP SNOOPING configuration
- IGMP SNOOPING configuration example

13.1 IGMP SNOOPING introduction

In a traditional network broadcast traffic packets can potentially cause excess network traffic leading to network congestion. When the switch is configured to use IGMP SNOOPING, IGMP SNOOPING can learn IP dynamic multicast MAC addresses to maintain the output port list IP multicast MAC address, this allows the multicast data flow only to the output port it is needed to send to and thus it can reduce the network traffic.

The main contents of this section are as follows:

- IGMP SNOOPING processing
- Second layer dynamic multicast
- Join a group
- Leave a group

13.1.1 IGMP SNOOPING processing

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic to control delivery of IP multicasts. Network switches with IGMP snooping listen in on the IGMP conversation between hosts and routers and maintain a map of which links need which IP multicast transmission. Multicasts may be filtered from the links which do not need them, conserving bandwidth on those links.

Multicast group information includes multicast group address, member port, VLAN ID, Age time.

The formation of an IGMP SNOOPING multicast group is a learning process. When one port of the switch receives the IGMP REPORT packet, IGMP SNOOPING generates a new multicast group and the port that receives the IGMP REPORT packet is added to the multicast group. When an IGMP QUERY packet is received by the switch, if the multicast group already exists in the switch, then the port received the IGMP QUERY is added to the multicast group, otherwise it will only forward the IGMP QUERY packet. Leave SNOOPING also supports the IGMP mechanism of IGMP V2 IGMP SNOOPING; if the configuration of the fast-leave ENABLE in IGMP V2, received leave packet when it receives port can leave the multicast group immediately; if the configuration of the fast-leave left the waiting time (fast-

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

leave-timeout), then the multicast group waiting for this time expires after leaving the multicast group.

There are two update mechanisms for IGMP SNOOPING. One is the leave mechanism described above. In most cases, IGMP SNOOPING deletes expired multicast groups through age time. When the multicast group joins the IGMP SNOOPING, the added time is recorded. When the multicast group has more than one configured age time in the switch, the exchange opportunity deletes the multicast group.

When a port to receive Leave packets, this port will immediately be removed from the multicast group to which it belongs, this situation may affect the continuity of the network data stream; because this network equipment port below may be connected to a HUB or no IGMP SNOOPING function, the equipment connected to receive the multicast data under many of the current equipment. A device sends Leave, which may affect other devices and cannot receive multicast data streams. Fast-leave-timeout mechanism can prevent the occurrence of this situation, through the Fast-leave-timeout configuration of a left waiting time, port leave packets received after waiting for Fast-leave-timeout long time and then removed from the multicast group to which it belongs, to guarantee the continuity of network multicast stream.

13.1.2 Second layer dynamic multicast

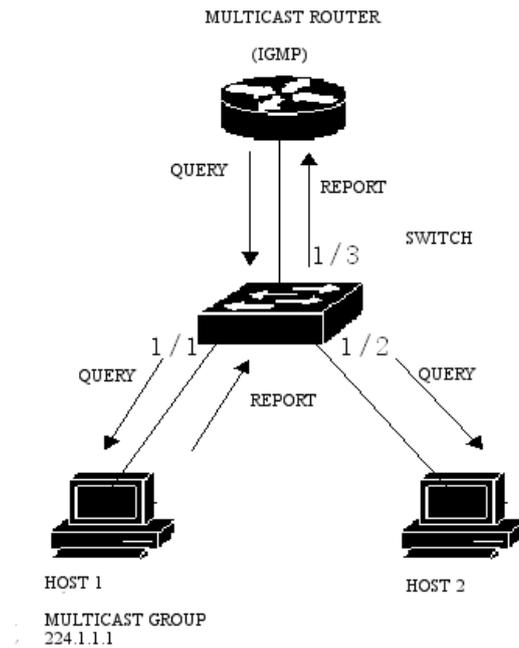
The multicast MAC address entries in the two layer hardware multicast forwarding table can be dynamically learned by IGMP SNOOPING. The IP multicast MAC address is dynamically learned through IGMP SNOOPING.

When IGMP SNOOPING is not enabled then multicast MAC addresses cannot be dynamically learned and the multicast stream is broadcast by the switch just like a standard unicast stream.

When IGMP is configured and in use, one device on the network is designated as the IGMP Querier, and it is responsible for asking devices what multicast groups they want to join on the network. The querier then tracks those responses and passes them to the switch or switches to add to their Multicast Forwarding Database. This database is a table of multicast IPv4 or multicast MAC addresses as well the switchports which should receive that traffic. When multicast traffic arrives at the switch, the switch checks the table and then passes the traffic to all ports which should receive it.

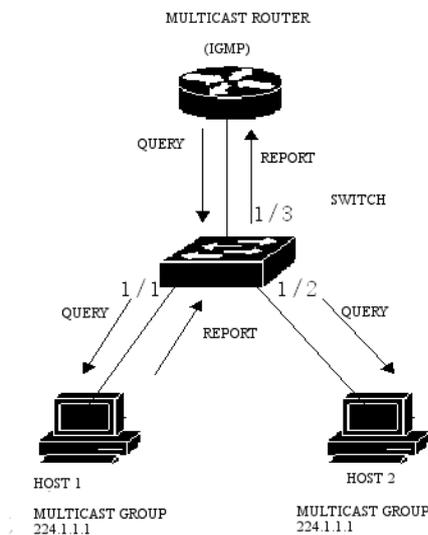
13.1.3 Join a group

When a host wants to join a multicast group, the host sends an IGMP REPORT packet, which specifies the multicast group to which the host is to join. When the switch receives an IGMP QUERY packet, the packet forwarding will switch to the same VLAN all other ports, when the IGMP QUERY packet is received under the port to join a multicast group after the host return an IGMP REPORT package. When an IGMP REPORT packet is received, a two layer multicast entry is established, and the port of the IGMP QUERY packet and the port of the IGMP REPORT packet are added to the two layer multicast item to become its output port.



If all the devices in the picture are in a subnet, suppose that the subnet VLAN is 2. Router runs IGMPv2 protocol and sends IGMP QUERY packets regularly. Host 1 wants to join multicast group 224.1.1.1. After receiving the IGMP QUERY packet from the 1/3 port, the switch will record the port and forward the packet to port 1/1 and 1/2. Host 1 sends an IGMP REPORT packet after receiving the IGMP QUERY packet, and host 2 does not send IGMP REPORT packet because it does not want to join the multicast group. After receiving the IGMP REPORT packet from the port 1/1, the switch forwards the packet from the query port 1/3 and creates a two layer multicast item (assuming that the item does not exist). The two layer multicast entry includes the following items:

Two layer multicast address	VLAN ID	Output port list
01:00:5e:01:01:01	2	1/1, 1/3



	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

As shown in Figure 1, host 1 has added multicast group 224.1.1.1, and now host 2 wants to join multicast group 224.1.1.1. When the host 2 received IGMP QUERY packet after sending back an IGMP REPORT packet switch IGMP REPORT received from the 1/2 port will put the package from the 1/3 query port forwarded and make port 1/2 was added to the two layer multicast entry, the entry into the two layer multicast:

Two layer multicast address	VLAN ID	Output port list
01:00:5e:01:01:01	2	1/1, 1/2, 1/3

13.1.4 Leave a group

In order to be able to form a stable multicast environment, IGMP devices (such as routers) send an IGMP QUERY packet to all hosts at regular intervals. The host that has joined the multicast group or who wants to join the multicast group returns an IGMP REPORT after receiving the IGMP QUERY.

If the host wants to leave a multicast group, there are two ways: the active leave and the passive leave. The active departure is the host sends an IGMP LEAVE packet to the router, and the passive departure is when the host receives the IGMP QUERY sent by the router and does not send back the IGMP REPORT.

When the host leaves the multicast group, there are two ways to switch off the two layer multicast from the switch: leave out of time and receive the IGMP LEAVE packet.

When the switch over a certain time from one port to receive a multicast group IGMP REPORT packet, the port should be removed from the two layer multicast entry corresponding, if the two layer multicast entries without port, delete two layer multicast entries.

When the switch fast-leave is configured as an ENABLE, if a port receives a multicast group IGMP LEAVE packet, clear the port from the two layer multicast entry corresponding, if the two layer multicast no entry port, then delete the layer two multicast entries.

Fast-leave is generally used by one host in a port under the circumstances; if a port under more than one host, you can configure the fast-leave-timeout waiting time, so as to ensure the continuity and reliability of multicast flow.

13.2 IGMP SNOOPING configuration

13.2.1 IGMP SNOOPING default configuration

The default IGMP SNOOPING is closed, and the two layer hardware multicast forwarding table is in the unregistered forwarding mode.

Fast-leave is closed by default.

Fast-leave-timeout time is 300 seconds.

The age time of multicast group REPORT port defaults to 400 seconds.

The age time of multicast group QUERY port defaults to 300 seconds.

13.2.2 Open and close IGMP SNOOPING

Open the IGMP SNOOPING protocol can be global open, you can also open part of the VLAN; only global open IGMP SNOOPING to open or close a VLAN IGMP SNOOPING.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Open global IGMP SNOOPING
Switch#configure terminal
Switch(config)#ip igmp snooping

Open a VLAN IGMP SNOOPING
Switch#configure terminal
Switch(config)#ip igmp snooping vlan <vlan-id>

Close global IGMP SNOOPING
Switch#configure terminal
Switch(config)#no ip igmp snooping

Close a VLAN IGMP SNOOPING
Switch#configure terminal
Switch(config)#no ip igmp snooping vlan <vlan-id>

13.2.3 Configuration survival time

Configuring the lifetime of multicast groups
Switch#configure terminal
Switch(config)#ip igmp snooping group-membership-timeout <interval> vlan <vlan-id>
The unit of Interval is milliseconds.

The lifetime of configuration query groups
Switch#configure terminal
Switch(config)#ip igmp snooping query-membership-timeout <interval> vlan <vlan-id>
The unit of Interval is milliseconds.

13.2.4 Configuration fast-leave

Start a VLAN fast-leave
Switch#configure terminal
Switch(config)#ip igmp snooping fast-leave vlan <vlan-id>

Close fast-leave
Switch#configure terminal
Switch(config)#no ip igmp snooping fast-leave vlan <vlan-id>

Configuring fast-leave wait time
Switch#configure terminal
Switch(config)# ip igmp snooping fast-leave-timeout <interval> vlan <vlan-id>

Recovery default fast-leave wait time
Switch#configure terminal
Switch(config)#no ip igmp snooping fast-leave-timeout vlan <vlan-id>

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

13.2.5 MROUTER configuration

Configuring a static query port

Switch#configure terminal

Switch#interface ge1/6

Switch(config-ge1/6)#ip igmp snooping mrouter vlan [vlan-id]

13.2.6 Display information

Display IGMP SNOOPING configuration information

Switch#show ip igmp snooping

Displays a configuration information for VLAN

Switch#show ip igmp snooping vlan <vlan-id>

Display aging information of REPORT multicast group

Switch#show ip igmp snooping age-table group-membership

Display the aging information of QUERY

Switch#show ip igmp snooping age-table query-membership

Display forwarding information of multicast group

Switch#show ip igmp snooping forwarding-table

Display MROUTER information

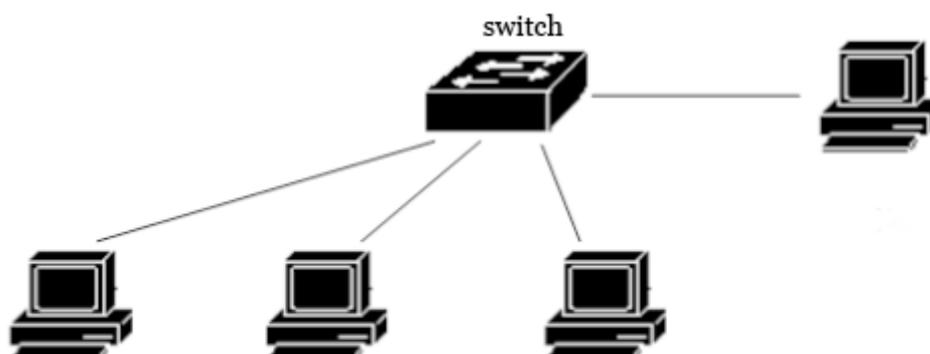
Switch#show ip igmp snooping mrouter

The display system is currently configured, including the configuration of IGMP SNOOPING

Switch#show running-config

13.3 The IGMP SNOOPING configuration example

The IGMP SNOOPING function is enabled on the switch. The user 1, the user 2, and the user 3 can be added to the particular multicast group.



	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

```

Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 200
Switch(config)#ip igmp snooping
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode access
Switch(config-ge1/1)#switchport access vlan 200
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 200
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 200
Switch(config)#ip igmp snooping group-membership-timeout 60000 vlan 200

```

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

14. MVR configuration

The main contents of this chapter are as follows:

- MVR profile
- MVR configuration
- MVR configuration example

14.1 MVR profile

Multicast VLAN registration (MVR) is applied to multicast streaming applications in service provider networks, such as Video On Demand. MVR allows users to subscribe to or cancel multicast flows within the multicast VLAN, allowing a multicast VLAN to share data streams with other VLAN. MVR has two purposes: (1) through simple configuration, it can effectively and securely transfer multicast flows between VLAN; (2) support multicast groups dynamically join and leave.

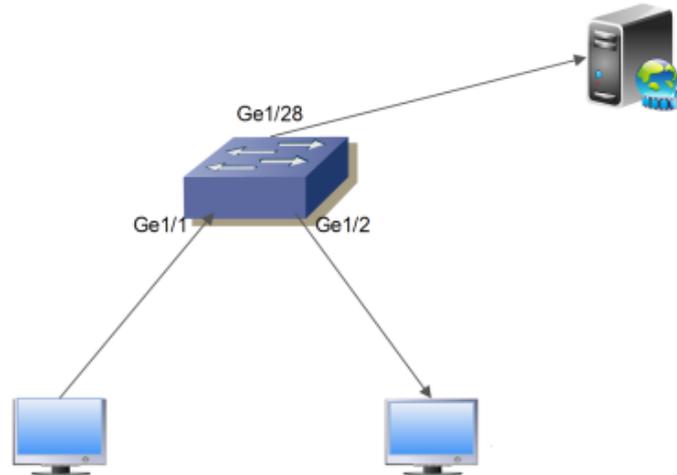
MVR is similar to IGMP snooping in that two functions can be started at the same time, MVR only handles the joining and leaving of configured multicast groups, and the other groups join and leave by IGMP snooping management. The difference between them is that multicast flows in IGMP snooping can only be forwarded within one VLAN, while MVR multicast streams can be forwarded in different VLAN.

14.2 MVR configuration

Command	Description	CLI mode
mvr (enable disable)	Start global MVR	Global configuration mode
no mvr	Clear all MVR configurations	Global configuration mode
mvr group A.B.C.D	Configuring IP multicast address	Global configuration mode
no mvr group A.B.C.D	Delete IP multicast address	Global configuration mode
mvr group A.B.C.D <1-256>	Configure the IP multicast address and configure a continuous MVR group address	Global configuration mode
mvr vlan <1-4094>	Specifies the VLAN to receive multicast data	Global configuration mode
no mvr vlan	Restore default VLAN1 for receiving multicast data	Global configuration mode
mvr-interface (enable disable)	Boot interface MVR	Interface configuration mode
show mvr	Display MVR configuration information	Privileged mode

14.3 MVR configuration example

Network topology as shown below, the user 1 and user 2 belong to vlan10 vlan20 respectively, user 1 and user 2 see the same program, program range 225.1.1.1~225.1.1.64, MVR VLAN is 100:



Configure VLAN, start global IGMP snooping, configure MVR VLAN, MVR program group range, global enable MVR:

```
Switch#configure terminal
Switch(config)#ip igmp snooping
Switch(config)# mvr enable
Switch(config)#mvr vlan 100
Switch(config)#mvr group 225.1.1.1 64
Switch#
```

Configure switch user port Ge1/1 Ge1/2, and uplink Ge1/28 :

```
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode hybrid
Switch(config-ge1/1)#switchport hybrid allowed vlan add 10 egress-tagged disable
Switch(config-ge1/1)#switchport hybrid allowed vlan add 100 egress-tagged disable
Switch(config-ge1/1)#mvr enable
Switch(config-ge1/1)#
```

```
Switch#configure terminal
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode hybrid
Switch(config-ge1/2)#switchport hybrid allowed vlan add 20 egress-tagged disable
Switch(config-ge1/2)#switchport hybrid allowed vlan add 100 egress-tagged disable
Switch(config-ge1/2)#mvr enable
Switch(config-ge1/2)#
```

```
Switch#configure terminal
Switch(config)#interface ge1/28
Switch(config-ge1/28)#switchport mode trunk
Switch(config-ge1/28)#switchport trunk allowed vlan add 100
Switch(config-ge1/28)#
```

15. DHCP SNOOPING configuration

In the dynamic access network environment, the host obtains the IP address and the network parameter through the DHCP server. DHCP SNOOPING is a kind of interception protocol for ARP attack. By listening to the DHCP message, dynamically binding the DHCP server to the client's IP address and the client's MAC address we can filter the ARP attack message on the switch.

The switches support DHCP SNOOPING and can effectively defend ARP attacks. DHCP SNOOPING listens to the DHCP message on the network and binds the port ARP information. You can configure four links to DHCP server physical ports, to some extent, to prevent unknown server interference networks.

When the switch undergoes a power off restart, the binding table will be lost and need to be re learned; the switch provides binding table uploading and downloading function, and the binding table can be stored in the TFTP server.

This chapter describes the concept and configuration of DHCP SNOOPING, including the following contents :

- DHCP SNOOPING introduction
- DHCP SNOOPING configuration
- DHCP SNOOPING configuration example
- DHCP SNOOPING configuration error

15.1 DHCP SNOOPING introduction

Because of the simple trust mechanism, the ARP protocol can potentially cause a loophole to the network security. When an ARP attack message carrying a false MAC message arrives at the host, it will override the local ARP cache table directly without restriction, allowing a normal data flow to the attacker. Therefore, the ARP information binding of ports can be implemented on the network two layer switch, which can effectively filter the ARP attack packets and make the attack packets unable to reach the attack host. If the network has not foreseen into the DHCP server, IP address distribution will lead to confusion, DHCP SNOOPING protocol provides a physical port binding link server, physical port cannot be non-specified by the DHCP server forwarding DHCP packets, can reduce the unknown server into the network the opportunity.

The main contents of this section are as follows :

- DHCP SNOOPING processing
- DHCP SNOOPING binding table
- DHCP SNOOPING specifies the physical port of the linked server
- DHCP SNOOPING binding list is uploaded and downloaded

15.1.1 DHCP SNOOPING processing

The DHCP SNOOPING protocol listens only to DHCPrequest, DHCPack, DHCPrelease three kinds of messages, does not receive other types of DHCP packets, and binds the mapping relationship between IP and MAC according to these messages.

The global DHCP SNOOPING switch is responsible for opening the switch to receive DHCP packets, i.e., UDP ports are 67 and 68 IP packets.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

15.1.2 DHCP SNOOPING binding table

The DHCP SNOOPING binding table entries are indexed by the MAC address, including item type, IP address, MAC address, interface information, delay timer, lease timer. The type of REQ and ACK in two, type REQ entry indicates that the DHCPrequest message is received, the DHCPack has not yet received the message, then start delay timer, the default time interval is 10 seconds, 10 seconds if it fails to receive an DHCPack message, the REQ type binding table entries are deleted; type ACK entry indicates that the DHCPack message is received and recorded the IP server address is assigned IP address, then start the lease timer, time interval is included in the DHCPack message DHCP server provides the lease contract value, the timer is restarted, the lease expires, the binding table entries are deleted. The interface information records the interface where the client is, that is, the interface between the IP address and the MAC address binding.

When the DHCPrequest message is received, the binding table entries are created, the entries type is REQ, the IP address, the MAC address, the interface information, and the 10 second delay timer are set up.

When the DHCPrequest message is received, the REQ type binding table entries already exist, the entries are updated, and the delay timers are restarted.

When the DHCPrequest message is received, the ACK type binding table entry already exists, then the interface information is recorded.

When receiving the DHCPack message, if there is a REQ type binding table entry, the IP address allocated by the server in the DHCPack message is recorded, the delay timer is closed, and the lease timer is started.

When receiving the DHCPack message, there is no REQ type binding table entry, and then the message is dropped.

When DHCPack packets are received, ACK type binding table entries already exist. If the interface has changed, the binding table entries of the original interface are deleted, and the entries are updated.

If the interface does not change, the IP address assigned by the server changes, deleting the binding table entries of the original interface and updating the entries.

If the interface does not change, the IP address has not changed, indicating that the renewal process, restart the lease timer can be.

When the timeout timer expires, the REQ type binding table entries are deleted.

When the lease timer timeout, the ACK type binding table entries are deleted.

15.1.3 DHCP SNOOPING specifies the physical port of the linked server

DHCP SNOOPING specifies the physical port of the linked server, and only the DHCP message can be received on the specified port. If there are multiple DHCP servers in the network, the OFFER provided by the server from the non-specified port will be filtered, and the IP address cannot be assigned to the client. Designated ports are conducive to the unified allocation of IP addresses in the network, to avoid the unknown server address pool is not in the IP planning, some clients cannot normally connect to the network. To some extent, it reduces the probability of network communication anomalies caused by unauthorized access to the server.

15.1.4 DHCP SNOOPING binding list is uploaded and downloaded

DHCP SNOOPING records the binding relationship between IP and MAC by monitoring the DHCP message and maintains its binding table. When the switch is switched off, restarted or a malfunction occurs then the binding table will be lost and the switch needs to relearn the binding table entries after a restart. In the network topology, it is difficult to identify the network

connection interruption and restart the DHCP discover process unless the host is directly connected and the switch will be difficult to relearn the binding information. For this reason, the binding table is saved on the TFTP server and the binding table is downloaded after the switch is restarted, which can solve the transient memory gap when the switch is restarted. The switch provides the binding table upload and download function, the administrator can be ordered through the manual upload or download the binding table, can automatically upload configuration commands, uploaded the binding table; the binding table command in the starting process from the TFTP server to download the backup file and the binding table has the binding table into the DHCP SNOOPING protocol module automatically restart the download.

15.2 DHCP SNOOPING configuration

15.2.1 DHCP SNOOPING default configuration

DHCP SNOOPING is disabled by default.

DHCP SNOOPING binding table type REQ entry delay timer default time interval is 10 seconds.

15.2.2 Global open and close DHCP SNOOPING

When the DHCP SNOOPING is opened globally, the DHCP SNOOPING of an interface can be turned on or off, and DHCP SNOOPING of all interfaces must be turned off before the global DHCP SNOOPING can be turned off.

Open global DHCP SNOOPING

Switch#configure terminal

Switch(config)#ip dhcp snooping [IF_LIST]

The parameter is the physical port list of the linked DHCP server that needs to be bound. A total of four ports can be specified, and the port list is separated by "", "ge1/1", "ge1/25", "ge1/26"

Close global DHCP SNOOPING

Switch#configure terminal

Switch(config)#no ip dhcp snooping

15.2.3 The interface opens and closes DHCP SNOOPING

Open an interface for DHCP SNOOPING

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#dhcp snooping

DHCP SNOOPING that closes an interface

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#no dhcp snooping

15.2.4 DHCP SNOOPING binding list is uploaded and downloaded

Upload the DHCP SNOOPING binding table to the TFTP server

Switch#configure terminal

Switch(config)#dhcp snooping upload A.B.C.D FILE_NAME

Parameters: the IP address of A.B.C.D TFTP server; the name of the binding table file that is saved on the TFTP server by FILE_NAME.

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Download the DHCP SNOOPING binding table from the TFTP server

```
Switch#configure terminal
Switch(config)#dhcp snooping download A.B.C.D FILE_NAME
```

Configure timed upload DHCP SNOOPING binding table to TFTP server

```
Switch#configure terminal
Switch(config)#dhcp snooping auto-upload A.B.C.D FILE_NAME interval
```

Parameters: interval upload interval time, ranging from 1 minutes to one day.

Cancel the configuration of DHCP SNOOPING binding table to TFTP server regularly

```
Switch#configure terminal
Switch(config)#no dhcp snooping auto-upload
```

Automatically download the DHCP SNOOPING binding table from the TFTP server when configuration restarts

```
Switch#configure terminal
Switch(config)#dhcp snooping reset-download A.B.C.D FILE_NAME
```

Automatically configure the configuration of the DHCP SNOOPING binding table from the TFTP server when the restart is cancelled

```
Switch#configure terminal
Switch(config)#no dhcp snooping reset-download
```

15.2.5 Display information

Display DHCP SNOOPING configuration information

```
Switch#show dhcp snooping
```

Display DHCP SNOOPING binding table information

```
Switch#show dhcp snooping binding-table
```

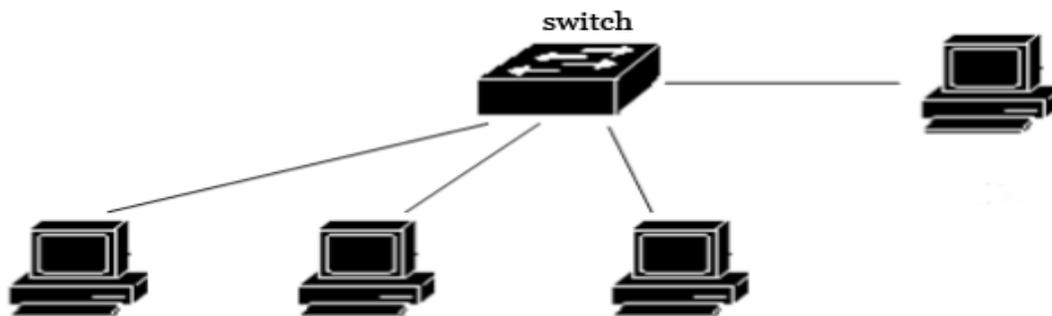
The display system is currently configured, including the DHCP SNOOPING configuration.

```
Switch#show running-config
```

15.3 DHCP SNOOPING configuration example

15.3.1 DHCP SNOOPING configuration

The DHCP SNOOPING function is enabled on the two layer switch, and the user 1, the user 2 and the user 3 obtain the IP address and network parameters dynamically through the DHCP server. User 1, user 2, user 3 interfaces start the DHCP SNOOPING function, dynamically binding ARP information in the interface.



```

Switch#configure terminal
Switch(config)#ip dhcp snooping ge1/9
Switch(config)#interface ge1/1
Switch(config-ge1/1)#dhcp snooping
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#dhcp snooping
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#dhcp snooping
Switch(config-ge1/3)#end
Switch#show dhcp snooping
DHCP Snooping is enabled globally
DHCP Server interface: ge1/9
Enable interface: ge1/1 ge1/2 ge1/3
Switch#show dhcp snooping binding-table

IP                MAC                FLAG PORT LEASE
192.168.1.100    00:11:5b:34:42:ad  ACK ge1/1  23:59:58
192.168.1.101    00:11:64:52:13:5d  ACK ge1/2  23:50:01
192.168.1.102    00:11:80:4d:a2:46  ACK ge1/3  20:34:45
Switch#show running-config
!
ip dhcp snooping ge1/9
!
spanning-tree mst configuration
!
interface vlan1
Ip address 192.168.0.1/24
!
interface ge1/1
dhcp snooping
!
interface 1/2
dhcp snooping
!
interface 1/3
dhcp snooping
!
line vty
!
End
Switch#

```

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

15.4 DHCP SNOOPING configuration error

If the DHCP snooping configuration fails, it may be caused by one of the following reasons:

1. System CFP resource exhaustion.
2. If the interface is configured, the ACL filtering function fails to open the DHCP SNOOPING globally
3. When the interface is configured with IP binding to MAC, the global open DHCP SNOOPING fails
4. The current interface is configured with the ACL filter function.
5. The current interface enables 802.1x anti ARP spoofing.
6. The configured interface is a three layer interface or a trunk interface.

16. MLD SNOOPING configuration

In a traditional network broadcast traffic packets can potentially cause excess network traffic leading to network congestion. Because of unicast packets being used then each packet will need to be copied to each receiver. As the number of receivers increases the more packets will need to be copied potentially resulting in a network bandwidth increase and efficiency being affected. With the increasing demand for multipoint video conferencing, video on demand and group communication applications, multicast has become the most popular mode of communication in order to improve resource utilization.

The switch implements the MLD SNOOPING function for multicast application service. MLD SNOOPING monitors MLD packets on the network to realize dynamic learning of IPV6 multicast MAC addresses.

This chapter describes the concept and configuration of MLD SNOOPING, including the following contents:

- MLD SNOOPING introduction
- MLD SNOOPING configuration
- MLD SNOOPING configuration example

16.1 MLD SNOOPING introduction

In a traditional network using subnet multicast packets as broadcast processing it possible to create excess network traffic which could cause network congestion. When the switch has MLD SNOOPING enabled then this can learn IPV6 dynamic multicast MAC addresses, to maintain the output port list IPV6 multicast MAC address and allow the multicast data to flow only to the output ports to send and so reduce the network traffic.

The main contents of this section are as follows:

- MLD SNOOPING processing
- Second layer dynamic multicast
- Join a group
- Leave a group

16.1.1 MLD SNOOPING processing

MLD SNOOPING is a two layer network protocol, the MLD protocol packets through the switch monitoring, according to the receiving port these MLD protocol package, VLAN ID and multicast address to maintain a multicast group, and then forwarded these MLD protocol. Only multicast ports can be added to receive multicast data streams; thus, the network traffic is reduced and the network bandwidth is saved.

Multicast group includes multicast group address, member port, VLAN ID, Age time.

The formation of MLD SNOOPING multicast group is a learning process. When one port of the switch receives the MLD REPORT packet, MLD SNOOPING generates a new multicast group, and the port that receives the MLD REPORT packet is added to the multicast group. When a MLD QUERY packet is received by the switch, if the multicast group already exists in the switch, then the port received the MLD QUERY is added to the multicast group, otherwise it will only forward the MLD QUERY packet. Done SNOOPING also supports the MLD mechanism of MLD V2 MLD SNOOPING; if the configuration of the fast-leave ENABLE in MLD V2, received Done packet when it receives port can leave the multicast group immediately; if the configuration of the fast-leave left the waiting time (fast-leave-timeout), then the multicast group waiting for this time expires after leaving the multicast group.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

There are two update mechanisms for MLD SNOOPING. One is the Done mechanism described above. In most cases, MLD SNOOPING deletes expired multicast groups through age time. When the multicast group joins the MLD SNOOPING, the added time is recorded. When the multicast group has more than one configured age time in the switch, the exchange opportunity deletes the multicast group.

When a port to receive Done packets, this port will immediately be removed from the multicast group to which it belongs, this situation may affect the continuity of the network data stream; because this network equipment port below may be connected to a HUB or no MLD SNOOPING function, the equipment connected to receive the multicast data under many of the current equipment. A device sends Done, which may affect other devices and cannot receive multicast data streams. Fast-leave-timeout mechanism can prevent the occurrence of this situation, through the Fast-leave-timeout configuration of a left waiting time, port leave packets received after waiting for Fast-leave-timeout long time and then removed from the multicast group to which it belongs, to guarantee the continuity of network multicast stream.

16.1.2 Second layer dynamic multicast

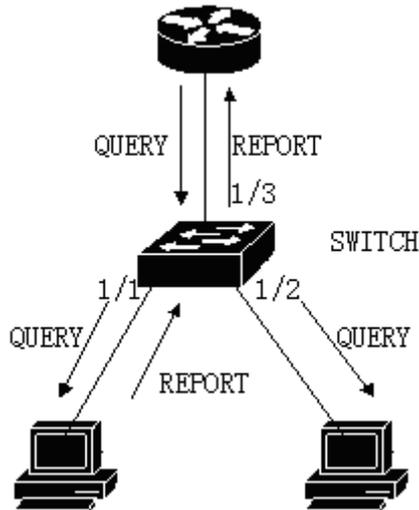
The multicast MAC address entries in the two layer hardware multicast forwarding table can be dynamically learned by MLD SNOOPING. The IPV6 multicast MAC address is dynamically learned through MLD SNOOPING.

When the switch off MLD SNOOPING, the two layer hardware multicast forwarding table in unregistered forwarding mode, multicast MAC address cannot be dynamically learned that two layer hardware multicast forwarding table no entries, two layer multicast data stream as all broadcast processing.

When the network multicast environment, in order to effectively control the multicast traffic network, the switch can open the MLD SNOOPING, the two layer hardware multicast forwarding table in register forwarding mode, the switch can learn to multicast MAC address through the monitoring network on the MLD protocol, and the two layer hardware multicast forwarding entries in the table, the two layer multicast to be able to flow forward.

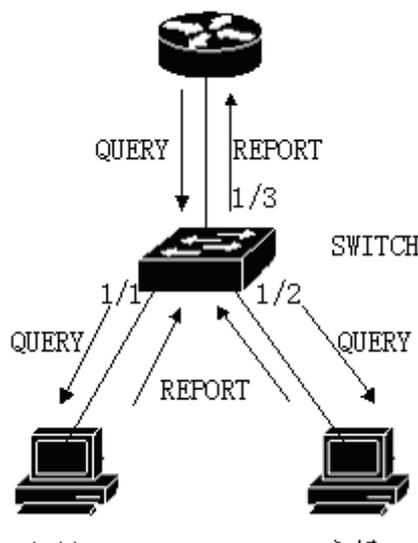
16.1.3 Join a group

When a host wants to join a multicast group, the host sends a MLD REPORT packet, which specifies the multicast group to which the host is to join. When the switch receives a MLD QUERY packet, the packet forwarding will switch to the same VLAN all other ports, when the MLD QUERY packet is received under the port to join a multicast group after the host return a MLD REPORT package. When a MLD REPORT packet is received, a two layer multicast entry is established, and the port of the MLD QUERY packet and the port of the MLD REPORT packet are added to the two layer multicast item to become its output port.



If all the devices in the picture are in a subnet, suppose that the subnet VLAN is 2. Router runs MLDv2 protocol and sends MLD QUERY packets regularly. Host 1 wants to join multicast group ff15::1. After receiving the MLD QUERY packet from the 1/3 port, the switch will record the port and forward the packet to port 1/1 and 1/2. Host 1 sends a MLD REPORT packet after receiving the MLD QUERY packet, and host 2 does not send MLD REPORT packets because it does not want to join the multicast group. After receiving the MLD REPORT packet from the port 1/1, the switch forwards the packet from the query port 1/3 and creates a two layer multicast item (assuming that the item does not exist). The two layer multicast entry includes the following items:

Two layer multicast address	VLAN ID	Output port list
33:33:00:00:00:01	2	1/1, 1/3



As shown in Figure 1, host 1 has added multicast group ff15:: 1, and now host 2 wants to join multicast group ff15::1. When the host 2 received MLD QUERY packet after sending back a MLD REPORT packet switch MLD REPORT received from the 1/2 port will put the package

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

from the 1/3 port and forwarded the query packet port 1/2 was added to the two layer multicast entry, the entry into the two layer multicast:

Two layer multicast address	VLAN ID	Output port list
33:33:5e:00:00:01	2	1/1, 1/2, 1/3

16.1.4 Leave a group

In order to be able to form a stable multicast environment, MLD devices (such as routers) send a MLD QUERY packet to all hosts at regular intervals. The host that has joined the multicast group or who wants to join the multicast group returns a MLD REPORT after receiving the MLD QUERY.

If the host wants to leave a multicast group, there are two ways: the active leave and the passive leave. The active departure is the host sends a MLD LEAVE packet to the router, and the passive departure is when the host receives the MLD QUERY sent by the router and does not send back the MLD REPORT.

When the host leaves the multicast group, there are two ways to switch off the two layer multicast from the switch: leave out of time and receive the MLD DONE packet.

When the switch over a certain time from one port to receive a multicast group MLD REPORT packet, the port should be removed from the two layer multicast entry corresponding, if the two layer multicast entries without port, delete two layer multicast entries.

When the switch fast-leave is configured as an ENABLE, if a port receives a multicast group MLD LEAVE packet, clear the port from the two layer multicast entry corresponding, if the two layer multicast no entry port, then delete the layer two multicast entries.

Fast-leave is generally used by one host in a port under the circumstances; if a port under more than one host, you can configure the fast-leave-timeout waiting time, so as to ensure the continuity and reliability of multicast flow.

16.2 MLD SNOOPING configuration

16.2.1 MLD SNOOPING default configuration

By default MLD SNOOPING is disabled, and the two layer hardware multicast forwarding table is in the unregistered forwarding mode.

Fast-leave is disabled by default.

Fast-leave-timeout time is 300 seconds.

The age time of multicast group REPORT port defaults to 400 seconds.

The age time of multicast group QUERY port defaults to 300 seconds.

16.2.2 Open and close MLD SNOOPING

Open the MLD SNOOPING protocol can be global open, you can also open part of the VLAN; only global open MLD SNOOPING to open or close a VLAN MLD SNOOPING.

Open global MLD SNOOPING

Switch#configure terminal

Switch(config)#ipv6 mld snooping

Open a VLAN MLD SNOOPING

Switch#configure terminal

Switch(config)#ipv6 mld snooping vlan <vlan-id>

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Close global MLD SNOOPING

```
Switch#configure terminal
Switch(config)#no ipv6 mld snooping
```

Close a VLAN MLD SNOOPING

```
Switch#configure terminal
Switch(config)#no ipv6 mld snooping vlan <vlan-id>
```

16.2.3 Configuration survival time

Configuring the lifetime of multicast groups

```
Switch#configure terminal
Switch(config)#ipv6 mld snooping group-membership-timeout <interval> vlan <vlan-id>
```

The unit of Interval is milliseconds.

The lifetime of configuration query groups

```
Switch#configure terminal
Switch(config)#ipv6 mld snooping query-membership-timeout <interval> vlan <vlan-id>
```

The unit of Interval is milliseconds.

16.2.4 Configuration of fast-leave

Start a VLAN fast-leave

```
Switch#configure terminal
Switch(config)#ipv6 mld snooping fast-leave vlan <vlan-id>
```

Close fast-leave

```
Switch#configure terminal
Switch(config)#no ipv6 mld snooping fast-leave vlan <vlan-id>
```

Configuring fast-leave wait time

```
Switch#configure terminal
Switch(config)# ipv6 mld snooping fast-leave-timeout <interval> vlan <vlan-id>
```

Recovery default fast-leave wait time

```
Switch#configure terminal
Switch(config)#no ipv6 mld snooping fast-leave-timeout vlan <vlan-id>
```

16.2.5 MROUTER configuration

Configuring a static query port

```
Switch#configure terminal
Switch#interface ge1/6
Switch(config-ge1/6)#ipv6 mld snooping mrouter vlan [vlan-id]
```

16.2.6 Display information

Display MLD SNOOPING configuration information

```
Switch#show ipv6 mld snooping
```

Displays a configuration information for VLAN

```
Switch#show ipv6 mld snooping vlan <vlan-id>
```

Display aging information of REPORT multicast group

```
Switch#show ipv6 mld snooping age-table group-membership
```

Display the aging information of QUERY

```
Switch#show ipv6 mld snooping age-table query-membership
```

Display forwarding information of multicast group

```
Switch#show ipv6 mld snooping forwarding-table
```

Display MROUTER information

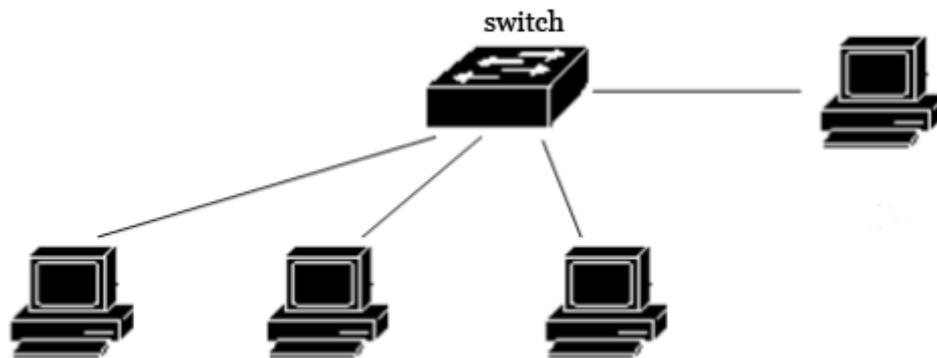
```
Switch#show ipv6 mld snooping mrouter
```

The display system is currently configured, including the configuration of MLD SNOOPING

```
Switch#show running-config
```

16.3 MLD SNOOPING configuration example

The MLD SNOOPING function is enabled on the switch. The user 1, the user 2, and the user 3 can be added to the particular multicast group.



```

Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 200
Switch(config)#ipv6 mld snooping
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode access
Switch(config-ge1/1)#switchport access vlan 200
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 200
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 200
Switch(config)#ipv6 mld snooping group-membership-timeout 60000 vlan 200
  
```

17. ACL configuration

In the actual network, the access security of the network is the concern of the administrator. The RT range of switches support ACL filtering to provide access security for the network. By configuring the ACL rules, the switches filter the input data stream according to these rules to realize the access security of the network.

This chapter describes how to configure ACL, including the following:

- Introduction of ACL resource library
- ACL filtering introduction
- ACL repository configuration
- ACL based on time interval
- ACL filter configuration
- ACL configuration example
- ACL configuration debugging

17.1 Introduction of ACL resource library

ACL (Access Control List) resource library is a set of multi group access rules. ACL resource library does not control the function of data forwarding, but only a set of rules sorted by conflict. When the ACL resource library is referenced, these applications control the forwarding of data according to the rules provided by the ACL resources. ACL can be applied to port access filtering, service access filtering and QoS, and so on.

The ACL resource group (group number 1 standard rules of IP ~ 991300 ~ 1999), IP group (group number 100 expansion rules ~ 1992000 ~ 2699), IP group MAC group ARP group (700~799> <, group 1100~1199); Each group of rules is automatically prioritized by conflicting rules. When the user configured an ACL rule, the system inserts the rule into the corresponding location according to the collation.

In the application, when a data packet through a port, the switch will all fields corresponding to each rule in the field and in the data packet are compared; when appear at the same time a complete matching rules, a rule, the first fully effective; by this matching rule to determine data the package is forwarded or discarded. The so-called perfect match is that the value of the field in the rule is exactly equal to the value of the corresponding field in the packet. Only when a rule is fully matched with ACL, the rule can do the corresponding deny or permit operations.

In switches, the rules within the same group are automatically sorted. The automatic sorting of rules is relatively complicated. In the sorting process, a large range of rules is behind, and a small range is in front. The scope of the rule is determined by the constraint condition of the rule; the less the constraint condition of the rule is, the larger the range of the rule matching is; the more the rule constraints are, the smaller the range of the rule matching is. Constraint rules are mainly embodied in the number of wildcard addresses and some non-address field. Wildcard is a bit string. The IP address is four bytes, and the MAC address is six bytes. Bits' 1 'means no matching, and bits' 0 ' means matching. Non address fields refer to protocol types, IP protocol types, protocol ports, and these fields also hide a wildcard. Their length is the byte length of the corresponding field, so the same field length is uniform, just counting the number of fields. The more bit the Wildcard is ' 0 ', the more constraints.

Taking port access filtering as an example, the necessity of rule ranking and the advantages of automatic sorting are illustrated. If the user needs to reject the source address for the 192.168.0.0/16 segment address forwarding, allowing the source address for the 192.168.1.0/24 network address forwarding, you can configure the following two rules:

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

```
access-list 1 permit 192.168.1.0 0.0.0.255 — Rule 1
access-list 1 deny 192.168.0.0 0.0.255.255 — Rule 2
```

Rule 1 and rule 2 are hereafter referred to as rule 2.

The two rules are conflicting; the address of rule 1 is contained in the address of rule 2, and one is deny and one is permit; according to the filtering principle of ACL, different orders have different results. If you want to achieve the above requirements, the order of the two rules above must be: Rule 1 is in front, rule 2 is behind. The switch automatically implements the above sorting function, regardless of the order in which the user configures the above rules, and the final order is the rule 1, which is in front of rule 2. When a source address is the 192.168.1.1 address of the packet forwarding up, first compare the first rule, then compare second rules, two rules are matched, in front of the force (forward); if the source address is 192.168.0.1, only the first match, then discarded (not forwarding).

If no sorting is done, the user may configure rule 2 first, then configure rule 1, rule 1 behind, rule 2 in front.

```
access-list 1 deny 192.168.0.0 0.0.255.255 — Rule 2
access-list 1 permit 192.168.1.0 0.0.0.255 — Rule 1
```

Because rule 2 contains the following rule 1, which may lead to the fact that the packets that match rule 1 completely match rule 2, rule 2 will be effective every time, and cannot meet the application requirements.

In the switch, '0.0.255.255' is wildcard bits, bits '1' means no matching, bits '0' means to match. It can be seen wildcard bits rule 2 for '0.0.255.255', need to match two bytes (16 bits); wildcard bits in rule 1 as the '0 0.0.255', need to match three bytes (24 bits); so rule 2 of the rules' "bigger, so after the row in the face. In extended IP, sorting needs to consider more rule fields, such as IP protocol type, communication port and so on. Their ordering rules are the same, that is, the more the configuration limit, the smaller the scope of the rule, and the larger the scope. The ordering of the rules is implemented in the background, and the user commands can only be displayed in the order of user configuration.

The filter fields supported by ACL include source IP, destination IP, IP protocol type (such as: TCP, UDP, OSPF), source port (such as 161), destination port. Users can configure different rules to access control according to different needs.

In a switch, a set of rules can be used by multiple applications; for example, a set of rules are filtered by port access and service access filtering and referenced by or accessed by ports of the two ports.

17.2 ACL filtering introduction

ACL filtering is carried out at the input port of the switch, and the port is filtered by the rule matching of the data stream entering the port. The ACL filter is handled by the line speed of the switch and does not affect the forwarding efficiency of the data stream.

When a port of a switch does not configure ACL filtering, all data flow through the port will not match the rules and can be forwarded through the port. When a switch port configuration of the ACL filter, all the input data through the port flow rule matching, the matching rules of action if it is permit, the data flow allows the forwarding, if it is deny, the data stream is not allowed to discard forwarding.

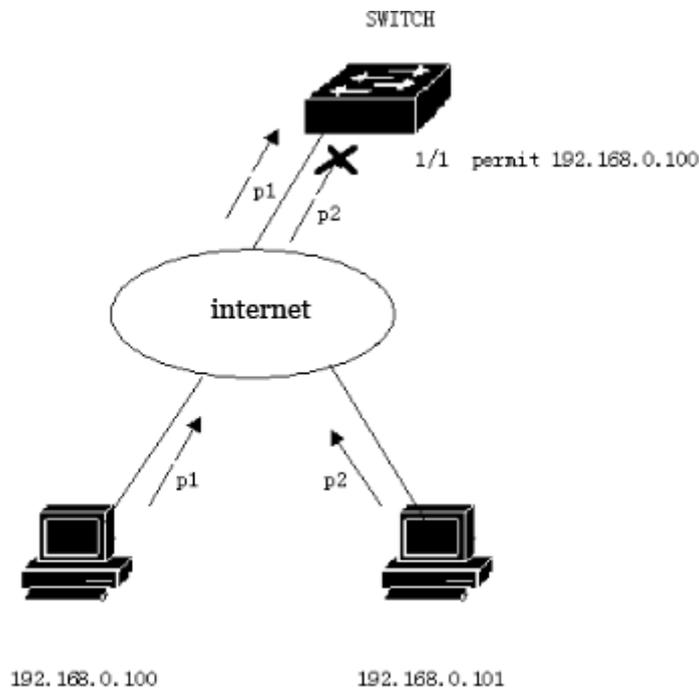
In the ACL filter configuration port, a port can select multiple ACL rules CFP group, the group rules into port selection, if not to deny or allow all the IP protocol. The rules set of rules in writing, CFP will add a rejection of all the rules of the IP agreement. When the rules of the ACL repository change, the rules written into the CFP automatically change.

For example, there is only one rule in a set of rules: access-list 1 permit 192.168.1.0 0.0.0.255,

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

which defaults to a rule that rejects all IP protocol packets, and actually there are two rules imported into the port's CFP. When data flows through filters, only data flows from 192.168.1.0 to 192.168.1.255 can be forwarded through this port, and all other data streams are filtered out. For example, there are two rules in a set of rules: access-list 1, deny 192.168.1.0 0.0.0.255, and access-list 1 permit any. At this point there is a rule that allows all IP protocol packages, and there are no hidden rules, and actually there are two rules imported into the port's CFP. When data flows through filters, only data streams with source addresses from 192.168.1.0 to 192.168.1.255 are filtered out, and all other data streams can be forwarded.

As shown below, an example of ACL filtering is given. The port 1/1 of the switch selects an ACL rule group 1. There is only one rule access-list 1 permit 192.168.0.100 in this set of rules. In the switch port 1/1, there are two users want to access the network from this port, the user's 1 IP address is 192.168.0.100, the user's 2 IP address is 192.168.0.101. Only the user 1 can access the network through the port 1/1 of the switch, and the user 2 cannot access the network through the port 1/1 of the switch. The data stream P1 sent by the user can be forwarded through the port 1/1 of the switch, while the data stream P2 sent by the user 1 is discarded at the port 1/1 of the switch.



When multiple ports are used for ACL filtering, the same ACL rule group can be used, and the same filtering rules are used.

Whether a set of rules or multi group rules are referenced by a port, they are automatically sorted, even if the order between the two sets of rules is crossed.

When a user refers to a set of rules, if the rules change, then the ports that refer to this set of rules will automatically respond to the user's configuration; there is no need to reconfigure the reference of this port.

17.3 ACL repository configuration

By default, the switch has no rules configured.

The resource library in the switch supports four types of ACL rules: Standard IP rules, extended IP rules, IP MAC groups, and ARP groups. Here are four rules to introduce the configuration of ACL.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Standard IP rule: the standard IP rule is to control the forwarding of data packets through the source IP address.

Command form: `access-list <groupId> {deny | permit} <source>`

Parameter description:

groupId: The access control list number, standard IP ACL support from 1 to 99 or 1300 to 1999.

deny/permit: If the match is complete, the packet is rejected or allowed to be forwarded.

source: Source IP has three input modes:

- 1) A.B.C.D wildcard You can control the IP address from a network segment;
- 2) any Amount to A.B.C.D 255.255.255.255
- 3) host A.B.C.D Amount to A.B.C.D 0.0.0.0

wildcard: Determine which bits needs to match, '0' indicates the need for matching, and '1' indicates no need for matching.

Extended IP rule: extending the IP rule is an extension of the standard IP rule. The packet forwarding can be controlled by source IP, destination IP, IP protocol type and service port.

Command form: `access-list <groupId> {deny | permit} <protocol> <source> [eq <srcPort>] <destination> [destPort] <tcp-flag>`

Parameter description:

groupId: The access control list number, the extended IP ACL support from 100 to 199 or 2000 to 2699.

deny/permit: If the match is complete, the packet is rejected or allowed to be forwarded.

protocol: The protocol types over the IP layer, such as TCP, UDP, and so on, can also input the corresponding number 6 (TCP). If you don't need to control these protocols, you can enter IP or 0.

source: Source IP has three input modes:

- 1) A.B.C.D wildcard You can control the IP address from a network segment;
- 2) any Amount to A.B.C.D 255.255.255.255
- 3) host A.B.C.D Amount to A.B.C.D 0.0.0.0

srcPort: For the case of protocol TCP or UDP, you can control the source port of the packet, the input mode can be some familiar port service name, such as: www can also be digital, such as 80.

destination: Objective IP has three input modes:

- 1) A.B.C.D wildcard You can control the IP address from a network segment;
- 2) any Amount to A.B.C.D 255.255.255.255
- 3) host A.B.C.D Amount to A.B.C.D 0.0.0.0

destPort: For the case that protocol is TCP or UDP, the destination port of the packet can be controlled, and the input mode is the same as that of srcPort.

tcp-flag: For the case that protocol is tcp. The TCP field matching of data packets can be controlled, and the optional parameters are ACK, fin, PSH, RST, syn, urg.

IP MAC rule: The IP MAC group can control the source destination MAC address and the source destination IP address of the IP packet.

Command form: `access-list <groupid> {deny | permit} <src-mac> vid <vlan-id|any> ip <src-ip> <dst-ip>`

Parameter description:

groupId: The access control list number, the extended IP ACL support group from 700 to 799.

deny/permit: If the match is complete, the packet is rejected or allowed to be forwarded.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

src-mac: source mac address.

The MAC address has three input modes:

- 1) HHHH.HHHH.HHHH wildcard You can control the MAC address from a segment;
- 2) any Amount to HHHH.HHHH.HHHH FFFF.FFFF.FFFF.
- 3) host A.B.C.D Amount to HHHH.HHHH.HHHH 0000.0000.0000

Vid: The outer vid can be either a vlan-id, or any any vlan-id

src-ip: Source IP address.

dst-ip: Destination IP address.

The IP address has three input modes:

- 1) A.B.C.D wildcard You can control the IP address from a network segment;
- 2) any Amount to A.B.C.D 255.255.255.255
- 3) host A.B.C.D Amount to A.B.C.D 0.0.0.0

ARP rule: The ARP group can control the type of operation of the ARP packet, the sender MAC and the sender IP.

Command form: access-list <groupid> {deny | permit} arp <sender-mac> <sender-ip>

Parameter description:

groupId: The access control list number, the extended IP ACL support group from 1100 to 1199.

deny/permit: If the match is complete, the packet is rejected or allowed to be forwarded.

sender-mac: The MAC address of the sender of the ARP packet.

The MAC address has three input modes:

- 1) HHHH.HHHH.HHHH wildcard You can control the MAC address from a segment;
- 2) any Amount to HHHH.HHHH.HHHH FFFF.FFFF.FFFF
- 3) host A.B.C.D Amount to HHHH.HHHH.HHHH 0000.0000.0000

sender-ip: Sender IP address of ARP packet.

The IP address has three input modes:

- 1) A.B.C.D wildcard You can control the IP address from a network segment;
- 2) any Amount to A.B.C.D 255.255.255.255
- 3) host A.B.C.D Amount to A.B.C.D 0.0.0.0

Other commands list:

show access-list [groupId]

Displays a list of rules configured in the current ACL. If groupId is entered, the list of rules for the current group is shown; otherwise, all the list of rules are displayed.

no access-list <groupId>

Deletes the specified rule list. All rules of group groupId.

17.4 ACL based on time interval

The time section is used to describe a particular time range. Users may have the need to have some ACL rules be effective within a certain period of time and do not use packet filtering during other time periods. At this time, the user can first configure one or more time periods, give this time period a name that is used in the corresponding rule. This rule is effective only in the time period specified.

If the time rule reference is not configured then the system will give a message and allow such rules to be created successfully but the rule will not take effect until the time reference has been configured and the system time in the specified period of time within the scope of the ACL rules to take effect.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

There are two situations for configuring the time section:

- (1) Configure the relative time section: use one day at a time to a certain point in the form of a point.
- (2) Configuration of absolute time: the use of a year, a month, a day, a part of a year, a month, a day, a part of the form.

Configuring ACL based on the time period:

Command	Description	CLI mode
time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59>	Assign a relative time segment that contains time only to the time section	Global configuration mode
time-range WORD cycle-time days from <0-6> to <0-6>	Configure a relative period of time only for weeks	Global configuration mode
time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59> days from <0-6> to <0-6>	Configure a time interval between time and week	Global configuration mode
time-range WORD utter-time from <2000-2100> <1-12> <1-31> <0-23> <0-59> to <2000-2100> <1-12> <1-31> <0-23> <0-59>	Assign an absolute time period to the date section	Global configuration mode
no time-range WORD cycle-time	Delete all the relative time periods of a certain time period	Global configuration mode
no time-range WORD utter-time	Delete all absolute time periods of a certain time period	Global configuration mode
no time-range WORD	Delete a period of time (including deleting all the relative time and absolute time periods)	Global configuration mode
no time-range	Delete all the time periods	Global configuration mode
show time-range WORD cycle-time	Displays all the relative time periods of a given period of time	Privileged mode
show time-range WORD utter-time	Displays all absolute time periods of a certain time period	Privileged mode
show time-range WORD	Display a certain period of time (including all absolute and absolute time periods)	Privileged mode
show time-range	Show all the time periods	Privileged mode
acl (<1-99> <100-199> <1300-1999> <2000-2699> <700-799> <1100-1199>) time-range WORD	The so and so ACL rule applies a certain period of time and plays a role when ACL is applied to the interface	Global configuration mode
no acl (<1-99> <100-199> <1300-1999> <2000-	Cancel a certain ACL rule and apply a certain period of time or all time	Global configuration

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

2699> <700-799> <1100-1199>) time-range (WORD)	periods	mode
show acl (<1-99> <100-199> <1300-1999> <2000-2699> <700-799> <1100-1199>) time-range	Displays all the time periods of the application of a certain ACL rule	Privileged mode
show all acl time-range	Displays the time periods for all ACL rules to be applied	Privileged mode

It's important to note that:

- (1) The time interval is configured with a number of relative time periods, the relationship between the relative time interval, the system time in any relative period of time, the time period is activated.
- (2) There are several absolute time periods for a certain time period, and the absolute time period is the relationship. The system time is in any absolute time period, and the time period is in the active state.
- (3) If to a certain time while the configuration of the relative time and absolute time, relative time and absolute time and system time relationship, at the same time only in the relative time and absolute time, the time period is active.
- (4) Define up to 256 time periods; a maximum period of time can be configured 256 relative time and absolute time; an ACL rule can be used up to 256 time periods; in the period of ACL association rules applied to the interface when the time comes into play.

17.5 ACL filter configuration

By default the switch has all ports configured to not do ACL filtering.

Command list:

access-group <groupId>

Mode: two layer interface configuration mode

parameter:

groupId: The binding of ACL and port number

Function: configure ACL port filter.

Note: if the above command configuration fails or fails, there may be the following reason:

Too many rules in the ACL group or the hardware resources are exhausted or occupied by other applications.

Display ACL port filter configuration

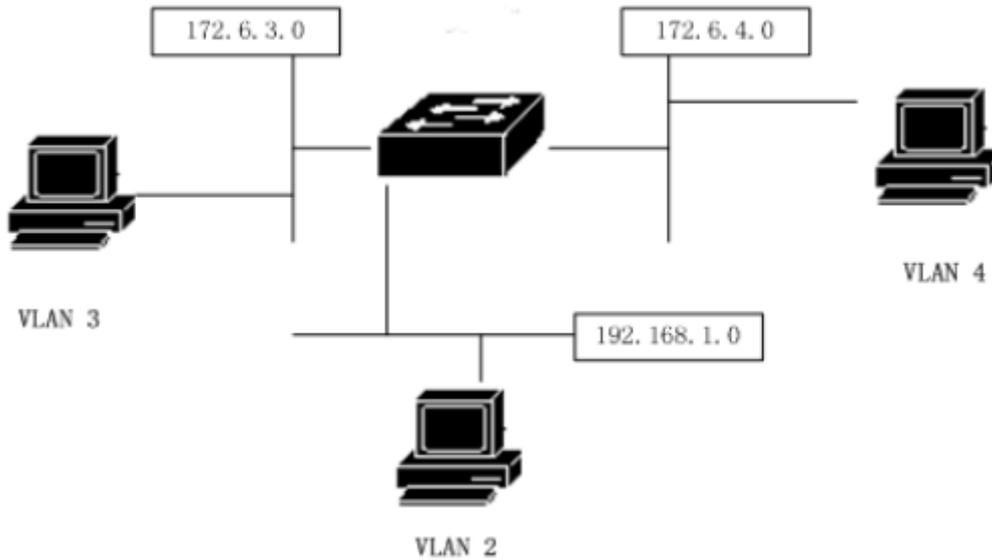
show access-group

Removes the current port and ACL port filter configuration

no acl- group <groupId>

17.6 ACL configuration example

A switch connects three subnets, ACL is configured to block any source address in the 192.168.1.0 network address. The other network addresses are allowed to pass. The 192.168.1.0 segment connects to the 1/1 port of the switch.



The switches are configured as follows:

```

Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config)#interface ge1/1
Switch(config-ge1/1)# switchport mode access
Switch(config-ge1/1)#switchport access vlan 2
Switch(config)#interface vlan2
Switch(config-vlan2)#ip add 192.168.1.1/24
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 3
Switch(config)#interface vlan3
Switch(config-vlan2)#ip add 172.16.3.1/24
Switch(config)#access-list 10 deny 192.168.1.0 0.0.0.255
Switch(config)#access-list 10 permit any
Switch(config)#interface ge1/1
Switch(config-ge1/1)#access-group 10
Switch(config)#interface ge1/2
Switch(config-ge1/2)#access-group 10

```

Note: according to the specific needs of the configuration of the time period, the time section associated with ACL rules, refer to the configuration as follows:

```

Switch(config)#time-range test cycle-time from 8 30 to 17 30 days from 1 to 5
Switch(config)#acl 1 time-range test
Switch(config)#interface ge1/20
Switch(config-ge1/20)#access-group 1

```

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

17.7 ACL configuration debugging

If the ACL configuration fails, the cause may be one of the following reasons:

- Before configuring the access control list, make sure that all IP are connected and then add access control lists. This access control list blocks the IP data stream whose source address is 192.168.1.0 segment through the switch. Note the subnet complement method. Use the show access-list command to list access control lists for viewing and be sure to pay attention to the source address and destination address. Don't write back. Then view the access control list. And the default access control list finally has an implicit deny any statement, if you want to let the other through, you need to add a permit any statement, otherwise it cannot pass.
- The system is configured with a static IP MAC binding.
- The current interface enables the DHCP SNOOPING protocol.
- System CFP resource exhaustion.

18. TCP/IP basic configuration

For a two layer switch with network management function, it is necessary to provide the basic network configuration for TCP/IP protocol.

The main contents of this chapter are as follows:

- Configuring the VLAN interface
- Configuring ARP
- Configuring static routing
- TCP/IP basic configuration example

18.1 Configuring the VLAN interface

On the switch, each three layer interface is attached to a certain VLAN, so the three layer interface is also called VLAN interface. The creation and deletion of the VLAN interface is accomplished manually. The RT range of switches can have a maximum of 4094 VLANs, but a maximum of 32 subnets can be configured. The creation of a subnet interface can be created according to the needs of the users; the subnet interface can be deleted manually by users and can be deleted with the deletion of the VLAN in which the subnet is located.

Each VLAN interface has a name. The name of the VLAN interface is the string "VLAN", followed by the VLAN ID number, such as the name of the three layer interface of VLAN 1 is "vlan1", and the name of the three layer interface of VLAN 4094 is "vlan4094".

Like ports, the VLAN interface also has management status and link states. At present, the switch does not provide the configuration of the management state of the VLAN interface. As long as the VLAN interface is established, the management state of the VLAN interface is always UP. Link state VLAN interface is corresponding to the interface of the VLAN contained in the port, as long as the link state of a port in VLAN is RUNNING, then the link state of the VLAN interface is RUNNING, if VLAN in all ports are not RUNNING, then the link state of the VLAN interface is not RUNNING.

On the VLAN interface, you can configure the IP address and indicate the network prefix of the network segment connected to the interface (converted to network mask). Currently, switches only support one IP address on one VLAN interface. Before configuring the IP address, users need to create the VLAN first and add the related ports to the VLAN. By default, the switch has the interface of VLAN1, and the IP address 192.168.0.1/24 is set on this interface, and the user can also modify the IP address of the VLAN1 interface. The VLAN interface other than VLAN1 defaults not to set the IP address.

The commands for configuring the IP address of the VLAN interface are as follows:

Command	Description	CLI mode
Ip interface vlan <2-4094>	Create a VLAN interface	Global configuration mode
No Ip interface vlan <2-4094>	Deleting a VLAN interface	Global configuration mode
ip address <ip-prefix>	Set the IP address on the VLAN interface. Parameters include the IP address of the interface and the	Interface configuration mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

	network prefix of the connected segment. If the VLAN interface originally exists the IP address, first delete the original IP address, and then set the specified IP address. The format of the parameter is A.B.C.D/M.	
no ip address [ip-prefix]	Deleting the IP address of the VLAN interface. If the parameter is specified, the parameter must be the same as the parameter given at the time of the setting, otherwise the command is invalid. The format of the parameter is A.B.C.D/M.	Interface configuration mode

See the command of the VLAN interface as follows:

Command	Description	CLI mode
show interface [if-name]	View the information of the VLAN interface, including the IP address, MAC address, management state, link state, etc. of the interface. The parameter is the interface name of the VLAN interface. If no parameters are specified, all ports and VLAN interfaces are checked.	Normal mode, privileged mode
show running-config	Viewing the current configuration of the system, you can see the configuration of the VLAN interface.	privileged mode

Example:

The subnet 193.1.1.0 is configured on the VLAN3 interface, the subnet prefix is 24 (i.e. the subnet mask is 255.255.255.0) and the IP address of the interface is 193.1.1.1

The settings used for VLAN3 are then shown using the following commands:

```

switch(config)#interface vlan3
switch(config-vlan3)#ip address 193.1.1.1/24
switch(config-vlan3)#end
switch#show interface vlan3

```

18.2 Configuring ARP

ARP (Address Resolution Protocol) protocol is a mapping protocol used to map an IP address to its corresponding MAC address. ARP is a simple message format containing one address resolution request or response. The packets are carried at the data link layer of the underlying network as raw payload. The size of the ARP message depends on the link layer and network layer address sizes. The message header specifies the types of network in use at each layer as well as the

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

size of addresses of each. The message header is completed with the operation code for request and reply. The payload of the packet consists of four addresses, the hardware and protocol address of the sender and receiver hosts.

Suppose that the two adjacent segment of the host A and B communicate through the switch, the host A to host B before sending data to the first and the host A directly connected to the switch interface to send the ARP request message, get the ARP response to send data packets to the interface. After receiving the data packet, the switch first broadcasts an ARP request message to the host B, then receives the ARP response message from the host B, and then sends the data packet to the host B.

There is an ARP cache on the switch, called the ARP table, which stores the mapping records of the IP address to the MAC address in the directly connected network. Each item in the ARP table has a lifetime, the default is 20 minutes. When the switch does not receive the ARP request or reply message of the IP address during the lifetime, the ARP table entry corresponding to the IP address will be deleted.

This section includes the following contents:

- Configuring static ARP
- Configuring ARP bindings
- Configuring ARP aging time
- View ARP information

18.2.1 Configuring static ARP

There are two different ARP table entries in ARP table, one is static ARP, and the other is dynamic ARP. Static ARP is the ARP table entry that is configured by the user, the system will not automatically refresh and delete this entry and user input is required to manually enter, update or delete it. Dynamic ARP is the system for automatically learning ARP according to the received ARP request or response package. The system automatically creates and deletes, updates and maintains in real time dynamic ARP entries, without user intervention, but the user can manually delete the dynamic ARP entries.

The switch does not configure a static ARP table item by default. It is important to note that when a VLAN interface is deleted or the subnet segment IP of the interface changes, the static and dynamic ARP table entries in the original subnet segment are deleted.

Configure the static ARP command as follows:

Command	Description	CLI mode
arp <ip-address> <mac-address> [if-name]	Configuring static ARP table entries. The first parameter is the IP address, and the IP address must be within a subnet segment. The second parameter is the MAC address, the MAC address must be unicast MAC address, and the MAC address format is HHHH.HHHH.HHHH, such as 0010.5cb1.7825. The third parameter is the two - level interface name, optionally, which indicates that the static ARP table	Global configuration mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

	entry is associated with a specific two - layer interface.	
no arp {<ip-address> <ip-prefix> all dynamic static }	Delete ARP table entries. It includes deleting an ARP table item of IP, deleting an ARP table item of a network segment, deleting all ARP table items, deleting all dynamic ARP table items, deleting all static ARP items.	Global configuration mode
arp static {<ip-prefix> all}	Modify all or all of the dynamic ARP items in a network segment to a static ARP table item.	Global configuration mode
arp aging <time>	Configuring ARP aging time only takes effect on dynamic learning ARP	Global configuration mode

18.2.2 View ARP information

The commands for viewing ARP information are listed below :

Command	Description	CLI mode
show arp [<ip-prefix> dynamic static]	Look at the ARP table item information in the ARP table, including all the ARP table entries, the ARP table entries of a segment, the dynamic ARP table entries and the static ARP table entries.	Normal mode, privileged mode
show running-config	Viewing the current configuration of the system, you can see the configuration of ARP.	privileged mode

18.3 Configuring static routing

A static route is defined by the user and is a route that can send packets from the source address to the destination address through the specified path. By configuring a static route as the default route, the packets that cannot be routed are sent to the default gateway.

Static routing is manually configured by administrators. It is suitable for the network with a simpler network structure. The administrator can configure the static route to make the switch work normally. Static routing does not take advantage of network bandwidth because it does not have routing updates.

Default routing is also a static route. In brief, the default route is the route that is used only when no matching routing item is found. That is, the default route is used only when there is no proper routing. In the routing table, the default route appears in the form of network 0.0.0.0/0 (mask 0.0.0.0). If the destination of the message is not in the routing table and there is no default route in the routing table, the message will be discarded and a ICMP message from the source will be returned to indicate the destination address or unreachable information of the network. Default

routing is very useful in the network. If a typical network consists of hundreds of switches, running dynamic routing protocols may consume more bandwidth resources, but by using the default routing can save time bandwidth resources, so you can meet a large number of users in a certain extent and communication needs.

A switch can configure multiple static routes to the same destination, but only one of the routes is activated for actual data forwarding. The switch does not have static routing enabled by default. Configure the static routing command as follows:

Command	Description	CLI mode
ip route <ip-prefix> <nexthop-address>	Set static routing. The first parameter specifies the length of the network segment IP and the network prefix, and the second parameter specifies the next hop IP address.	Global configuration mode
ip route <ip-address> <mask-address> <nexthop-address>	The function is the same as the previous command. The first parameter specifies the IP address of the network segment, the second parameter specifies the mask of the network segment, and the third parameter specifies the next hop IP address.	Global configuration mode
no ip route <ip-prefix> [nexthop-address]	Delete static routing. The first parameter specifies the length of the network segment IP and the network prefix, and the second parameter specifies the next hop IP address. If there are no second parameters, delete all the routes that match the specified segment. If you have second parameters, delete the routing that matches the specified segment and the next hop.	Global configuration mode
no ip route <ip-address> <mask-address> [nexthop-address]	The function is the same as the previous command. The first parameter specifies the IP address of the network segment, the second parameter specifies the mask of the network segment, and the third parameter specifies the next hop IP address. If there are no third parameters, delete all the routes that match the specified segment. If you have third parameters, delete the routing that matches the specified segment and the next hop.	Global configuration mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

See the routing command as follows:

Command	Description	CLI mode
show ip route [<ip-address> <ip-prefix>]	View the active routing information, you can choose to see all the routing, a route, a network segment of the routing, static routing.	Normal mode, privileged mode
show ip route database	View all the routing information (including active and inactive routes), and you can choose to view all the routes.	Normal mode, privileged mode
show running-config	Viewing the current configuration of the system, you can see the configuration of the static route.	privileged mode

Example:

The destination network is 200.1.1.0, subnet mask is 255.255.255.0, and the next hop is 10.1.1.2.

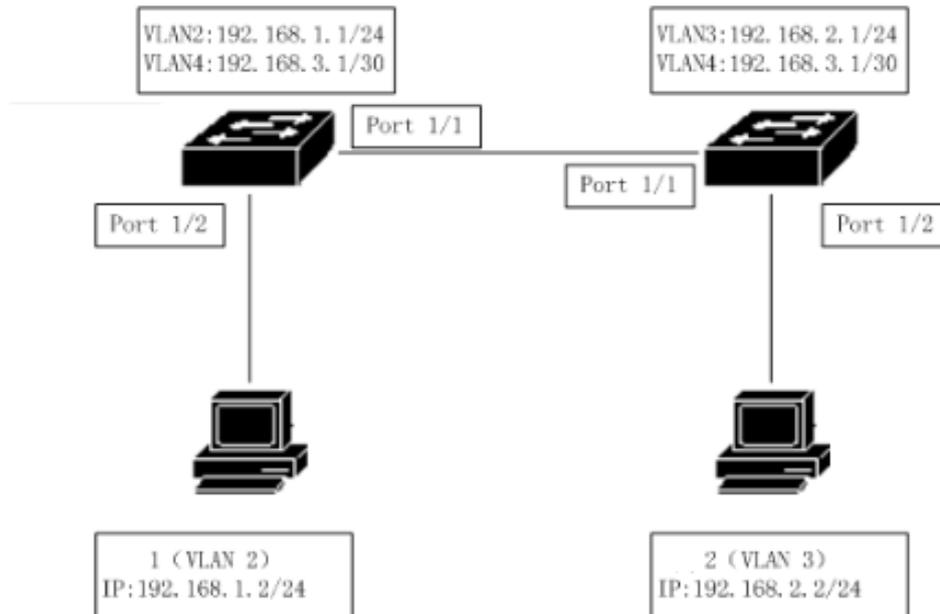
Configure command as:

Switch(config)#ip route 200.1.1.0 255.255.255.0 10.1.1.2
or **Switch(config)#ip route 200.1.1.0/24 10.1.1.2**

Delete the destination IP address is 200.1.1.0, subnet mask is 255.255.255.0, the next hop is 10.1.1.2 static routing. Configure command as:

Switch(config)#no ip route 200.1.1.0/24
or **Switch(config)#no ip route 200.1.1.0/24 10.1.1.2**
or **Switch(config)#no ip route 200.1.1.0 255.255.255.0**
or **Switch(config)#no ip route 200.1.1.0 255.255.255.0 10.1.1.2**

18.4 TCP/IP basic configuration example



In the diagram, switch 1 is a two layer switch, and switch 2 is a three layer switch.

18.4.1 Three layer interface

On switch 1, configure the corresponding three layer interface of VLAN2, and assign an IP address 192.168.1.1/24 to the interface.

Configuration is as follows:

```
Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switch access vlan 2
Switch(config)#interface vlan 2
Switch(config-vlan2)#ip add 192.168.1.1/24
```

Verification: user 1 is able to access the three layer interface IP address of VLAN2, e.g. by pinging IP address 192.168.1.1

18.4.2 Static routing

User 2 must be able to access switch 1 and must access the switch 1 through the routing function of switch 2.

Switch 1 is configured as follows:

```
Switch#configure terminal
Switch(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2
```

Switch 2 is configured as follows:

```
Switch#configure terminal
Switch(config)#ip route 192.168.1.0/24 192.168.3.1
```

Verification: User 2 can ping switch 1 using IP address 192.168.1.1

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

18.4.3 ARP

Configure 1 of the user's static ARP, allowing only 1 specific user to access from VLAN2.
Assume that the user's MAC address is 00:00:00:00:00:01

Switch 1 is configured as follows:

Switch#configure terminal

Switch(config)#arp 192.168.1.2 0000.0000.0001

Verification: user 1 is able to access the three layer interface IP address of VLAN2, e.g. by pinging IP address 192.168.1.1 but only from equipment with MAC address 00:00:00:00:00:01

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

19. SNMP configuration

The RT range of switches can be configured to allow SNMP remote management of the switch. This chapter describes how to configure SNMP, including the following:

The main contents of this chapter are as follows:

- SNMP introduction
- SNMP configuration
- SNMP configuration example

19.1 SNMP introduction

SNMP is a simple network management protocol and is the most widely used network management protocol. SNMP has five major functions: fault management, billing management, configuration management, performance management and security management. SNMP provides an information format for communication between network management application software and network management agent (agent).

SNMP network management protocol has four main elements: management of workstations, management of agents, management of information base and network management protocol. The management agent is the server of the management workstation accessing the switch. The information of the management workstation accessing the network management agent is organized in the form of MIB, and the management information base is formed.

SNMP has three big operations: GET operation, SET operation and TRAP operation. The GET operation enables the management workstation to obtain the value of the object in the proxy. The SET operation enables the management workstation to set the value of the object in the proxy. The TRAP operation enables the agent to notify the event of the management workstation.

The TRAP message is sent to the management workstation automatically when the event occurs. These messages include cold start, hot start, port link up, link down, shared name authentication failure, STP state switching, etc.

At present, SNMP has three versions: SNMPV1, SNMPV2, SNMPV3 and the latter version is the upgraded version in the previous version with enhanced functionality and improved security. The switch supports all three SNMP versions and can parse all three versions of the SNMP protocol package. When you send TRAP messages, you can use any version of SNMPV1, SNMPV2 or SNMPV3.

The RT range of switches support RFC, BRIDGE, and private MIB objects, and can fully manage switches through SNMP. Some MIB:RFC 1213, RFC 1493, RFC 1724, RFC 1850, RFC 1907, RFC 2233, RFC 2571, RFC 2572, RFC 2575, RFC 2573, RFC 2574, RFC 2674 and other common MIB.

19.2 SNMP configuration

The SNMP configuration includes the community configuration of the switch, the configuration of the TRAP workstation, the information of the SNMP system and the configuration of group engine, ID, user and snmpV3. The switch has a read-only SNMP set by default and the share name is public. The switch can have up to 8 shares configured. The switch does not have any TRAP workstations configured by default. The switch has a default local engine ID, and the switch can modify the local engine ID. The switch has a default user name:initialnone which belongs to a non-identified unencrypted user name. The switch can configure multiple

different levels of user names. The switch has a default group name:initial and switches can configure different group name according to different user names.

The commands of SNMP are as follows:

Command	Description	CLI mode
snmp community <community-name> {ro rw }	Configure the name of the shared object that accesses the network management, which is an interactive command. When configuring, the user can input the created name of the shared body and read / write permission according to the prompt.	Global configuration mode
no snmp community <community-name>	Deletes the specified SNMP share name.	Global configuration mode
snmp trap <notify-name> host <ipaddress> version {1 2c 3 }	Add or modify the sending target of SNMP trap. This is an interactive command. Notify name is unique, and if you modify the existing name, you can modify the trap to send the target item. Host is the destination address to send trap; version is sent in snmpV1, snmpV2c or snmpV3 mode. This command defaults to the target port of 162.	Global configuration mode
no snmp trap <notify-name>	Delete the specified SNMP trap.	Global configuration mode
snmp system information <contact location name> <information-string>	Configure system information, configurable system information include: contact, location and name.	Global configuration mode
no snmp system information <contact location name >	Delete a system configuration information.	Global configuration mode
snmp engine-id local <engine-id-octet-string>	Configure engine ID for version 3 of SNMP. The ID is a 24 bit sixteen decimal number; when the input is less than 24 bits, it is automatically padded with 0.	Global configuration mode
snmp user <user-name> <group-name> v3 [auth {md5 sha} <auth-key>]	The SNMP user command is to set a user name corresponding to the local engine ID of the snmpv3. And the group name corresponding to the user name. If the user name supports authentication, the authentication	Global configuration mode

	protocol (MD5 or Sha) and the corresponding identification password need to be set.	
no snmp user <user-name> <group-name> v3	Delete a user name corresponding to the local engine ID of SNMPv3.	Global configuration mode
snmp group <group-name> v3 {auth noauth} [notify <notify view name> write <write view name> read <read view name>]	The SNMP group command is a set of group names that the security level is (auth or noauth), and the notification, writable, or readable view specified by the security model (V3).	Global configuration mode
no snmp group <group-name> v3 {auth noauth}	Delete a group name, the security level is (auth or noauth), the security model (V3) specified view.	Global configuration mode
show snmp community	Show all the current public name and the corresponding read and write permissions information.	Normal mode, privileged mode
show snmp trap	Display all the trap names and the corresponding trap sent target IP address and version information.	Normal mode, privileged mode
show snmp system information	Display system information set by SNMP	Normal mode, privileged mode
show snmp engine-id	Display SNMPV3 local engine-id.	Normal mode, privileged mode
show snmp user [specify name of user]	Displays a user name information corresponding to the local engine ID of snmpv3. Include the group name corresponding to the user name and the authentication and encryption information supported by the user name.	Normal mode, privileged mode
show snmp group	Displays all group names, security levels (auth or noauth), notification specified by the security model (V3), writable or readable view information.	Normal mode, privileged mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

19.3 SNMP configuration example

Configure a share called private and configure it to have read and write permissions.

Configure a SNMP trap called test and set the destination IP to 192.168.0.10; use the version 1 of SNMP.

The specific content of the configuration system is contact: E-mail:user@user.com

The specific content of the configuration system is location: UserLocation

Set a user name initialmd5 that supports MD5 authentication, the group name is initial and the authentication password is 047b473f93211a17813ce5fff290066b.

Set the group name initial, the security level is (auth), the notification specified by the security model (V3), writable or readable view names are Internet, Internet, Internet.

The configuration of the switch is as follows:

Switch#configure terminal

Switch(config)#snmp community private rw

Switch(config)#snmp system information contact E-mail: user@user.com

Switch(config)#snmp system information location UserLocation

Switch(config)# snmp user initialmd5 initial v3 auth md5 17813ce5fff290066b

Switch(config)# snmp group initial v3 auth read internet write internet notify internet

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

20. RMON configuration

The main contents of this chapter are as follows:

- RMON introduction
- RMON configuration
- RMON configuration example

20.1 RMON introduction

RMON (Remote Monitoring) is a standard monitoring specification. It is mainly used to monitor data flow in a network segment and even in the whole network. It is one of the widely used network management standards. The RMON specification is extended by SNMP MIB, so it is also a MIB, which is the most important enhancement of the MIB II standard. RMON makes SNMP more effective and proactive in monitoring remote devices.

RMON monitoring system consists of two parts: detector (proxy or monitor) and management station. RMON agents store network information in RMON MIB, which are directly implanted into network devices (such as routers, switches, etc.). Management station uses SNMP to obtain RMON data information.

This device supports the 4 most commonly used groups in RMON:

- (1) Statistical group (Statistics): provide statistical data for each interface, where most of the objects are counters, recording the information collected by the monitor from the interface.
- (2) Historical group (History): data stored at a fixed time interval to a specified interface.
- (3) Alarm group (alarm): sampling the specified data of all interfaces at a fixed time interval, comparing with the set threshold, and triggering the corresponding event when the condition is satisfied.
- (4) Event group (event): setting events, you can choose to log records or send Trap.

20.2 RMON configuration

The RMON command consists of 4 groups of configurations to view configuration and view data:

Command	Description	CLI mode
rmon statistics <1-100> (owner WORD)	A group configuration that specifies the specified number of ports for this port. This is an interactive command. The configuration is that the user can enter the number and owner according to the prompt, and the owner is optional. The serial number is the configuration number of the statistical group, and the value ranges from 1 to 100.	Port configuration mode
no rmon statistics <1-100>	Statistical group configuration to cancel specified number.	Port configuration mode
rmon history <1-100> buckets <1-100> interval <1-3600> (owner WORD)	The historical group parameter that specifies the ordinal number for this port, which is an interactive command. The configuration user can enter the serial number, the number of requesting	Port configuration mode

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

	<p>buckets, the time interval and the owner according to the prompt. The serial number is the number of the historical group configuration, the value range is from 1 to 100; the number of bucket requests is the maximum number of the saved data, the value range is 1 to 100; the sampling interval is in seconds, and the value range is from 1 to 3600.</p>	
no rmon history <1-100>	The history group configuration to cancel the specified number.	Port configuration mode
<p>rmon alarm <1-60> WORD <1-3600> (absolute delta) rising-threshold <1-2147483647> <1-60> falling-threshold <1-2147483647> <1-60> (owner WORD)</p>	<p>Configuring an alarm group parameter with a specified ordinal number, which is an interactive command. Configuration user can input serial number, monitor object, time interval, contrast mode, upper limit value, upper limit event sequence number, lower limit value, lower limit time sequence number and owner. The serial number is the number of alarm configuration, the 1 to 60 range; the monitoring object is a MIB node OID, the sampling time interval in seconds, the 1 to 3600 range of contrast; you can select absolute or delta, said the absolute value (the value of each sample respectively) and relative value (increment relative to the last sampling sampling); range limit threshold is 1 to 2147483647; the event must advance configuration, 1 to 60 is the range of numbers.</p>	Global configuration mode
no rmon alarm <1-60>	Alarm group configuration to cancel specified number.	Global configuration mode
<p>rmon event <1-60> (log log-trap WORD none trap WORD) (description WORD) (owner WORD)</p>	<p>Configuring the event group parameter of the specified ordinal number, which is an interactive command. The configuration user can enter the serial number, event type, shared name, description and owner according to the prompt. The serial number is event group configuration number, 1 to 60 range; event types can choose log (log), log-trap (log and a Trap) and none (no action) and trap (a Trap), when the choice of log-trap or</p>	Global configuration mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

	trap, you must also specify the name of the equipment (in the common body the body name configuration is ignored).	
no rmon event <1-60>	Event group configuration to cancel the specified number.	Global configuration mode
show rmon (statistics history-control alarm event) config	View the RMON configuration information, which is an interactive command. Configuration users can input and view objects according to the prompts.	Global configuration mode
show rmon statistics-data interface IFNAME	View the RMON statistics group data, configure the user to input the interface name.	Global configuration mode
show rmon history-data interface IFNAME	View the RMON history group data, configure the user to enter the interface name.	Global configuration mode

20.3 RMON configuration example

Enable port group configuration for ge1/1, the ordinal number is 10, and the owner is user.

Enable the port ge1/8 history group data acquisition, the serial number is 2, the maximum preservation of 80 data, sampling interval is 1 minutes, no owner.

Configure events with a serial number of 1, log, no owner.

Configure an event with a number of 3, send Trap, share the name of public, no owner.

An alarm group with a serial number of 5 is used to monitor the number of bytes received per port. The Trap alarm is issued when the number of bytes per half is greater than 1000, and the log is less than 10. No owner.

The switch is configured as follows:

```

Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#rmon statistics 10 owner user
Switch(config-ge1/1)#exit
Switch(config)#interface ge1/8
Switch(config-ge1/8)#rmon history 2 buckets 80 interval 60
Switch(config-ge1/8)#exit
Switch(config)#rmon event 1 log
Switch(config)#rmon event 3 trap public
Switch(config)#rmon alarm 5 1.3.6.1.2.1.2.1.10 30 delta rising-threshold 1000 3 falling-
threshold 10 1

```

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

21. Cluster configuration

The RT range of switches provide a cluster management function that enables a single device to manage a set of network devices. This chapter describes how to configure cluster management, including the following :

- Introduction of cluster management
- Brief introduction of cluster configuration
- Configuration management equipment
- Configuration member device
- Configuring access cluster members
- Cluster management display and maintenance
- Example of cluster management typical configuration

21.1 Introduction of cluster management

21.1.1 Cluster definition

A cluster is a set of network devices that can be managed as a single device.

The purpose of cluster management: to solve the centralized management of a large number of scattered network devices.

Cluster advantages: save public network IP address and to simplify configuration management tasks. Network managers only need to configure the public network IP address on a switch in the cluster, so that the management and maintenance of other switches in the cluster can be achieved. Switches that have a public network IP address configured and perform management functions are command switches and other managed switches are member switches. Command switches and member switches that form a cluster.

The cluster configures and manages the switches within the cluster by using the following three protocols.

- NDP (Neighbour Discovery Protocol)
- NTDP (Neighbour Topology Discovery Protocol)
- Cluster (Cluster Management Protocol)

The working process of the cluster and the cluster topology collection including the establishment and maintenance, and maintenance of the cluster topology collection process is relatively independent, topology collection process begins to start up in the cluster before the establishment of the working principle is as follows :

- All devices acquire the information of neighbour devices through NDP, including the software version, host name, MAC address and port name of neighbour devices.
- The management device collects the device information and the connection information of each device through the NTDP and determines the cluster candidate devices from the collected topology information.
- The management device completes the operation of adding candidate devices to cluster and member devices leaving the cluster according to the candidate device information collected by NTDP.

The cluster message is two layer Ethernet message, the specific format and interactive process refer to the national standard "YDT 1692-2007 Ethernet switch cluster management technical requirements.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

21.1.2 Cluster role

According to the position and function of the devices in the cluster, different roles are formed. The user can specify roles by configuration, and all the roles are as follows:

1) Command Switch:

In a cluster, the only switch that can configure and manage the entire cluster is also the only switch in the cluster with the public network IP address.

- Command switches create clusters.
- Command switches discover and determine candidate switches by collecting information from NDP and NTDP.
- Command switches control cluster maintenance by adding candidate switches to clusters or deleting member switches from clusters.
- After the cluster is established, the command switch provides a management channel for the cluster.

2) Member switch

- Managed switches in a cluster.
- A member switch is a candidate switch before joining the cluster.
- Member switch does not have public network IP address.
- The management of the member switch is performed by the command exchange agent.

3) Candidate switch

A switch that has the ability to join clusters but has not yet joined any cluster.

The switch must first be a candidate switch, and then it can become a member switch.

4) Independent exchange

Switch without cluster function.

Various roles can be converted according to certain rules:

- When a user creates a cluster on a candidate device, the current candidate device is designated as a cluster management device. Each cluster must specify one (and only one) management device. After the management device is assigned, the management device discovers and identifies the candidate devices by collecting relevant information. The user can join the candidate device into the cluster through the appropriate configuration.

- When a candidate device joins a cluster, it becomes a member device.
- When a member device in the cluster is deleted, it will revert to a candidate device.
- Management devices can only be restored to candidate devices only when the cluster is removed.

21.1.3 NDP profile

NDP is used to obtain the information of directly connected neighbour equipment, including connection port, device name, software version and other information. The working principle is as follows:

- The NDP enabled device periodically transmits the NDP message to the neighbours, including NDP information in the NDP message (name of equipment, including the current version of the software, equipment port and other information) and NDP information on the receiving device aging time. It also receives and does not forward the NDP message sent by neighbour devices.

- The NDP enabled device stores and maintains the NDP neighbour information table and creates a table item for each neighbour device in the NDP neighbour information table. If a neighbour is discovered for the first time it sends the received NDP message, NDP will be in the neighbour information table to add a table; if different from neighbours received NDP information and old information, update the NDP table in the corresponding data item, if the same, only updated

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

if the aging time. Over ageing time has not received the neighbours send NDP information will automatically delete the corresponding neighbour table entry.

21.1.4 NTDP profile

NTDP is used to collect the information of each device and the connection information between devices in a certain network range. NTDP provides device information for management devices that can join the cluster and collects topological information of the devices within the specified hop count.

NDP provides adjacency list information for NTDP, NTDP sends and forwards NTDP topology collection request according to adjacency information, collects NDP information of each device in a certain network range and its connection information with all neighbours. After collecting the information, the management equipment or network management can use the information according to the need to complete the required functions. When a member device NDP neighbour discovery has changed, the handshake message will notify neighbour management equipment change, management of equipment can start NTDP for the specified topology collection, so that the NTDP can reflect the change of network topology.

The management device can periodically collect topology in the network, and the user can initiate a topology collection by manually configuring commands. Management equipment collects topological information process as follows:

- The management device sends the NTDP topology to collect the request packets from the ports that enable the NTDP function.
- Receive the request message immediately send response message to the topology of equipment management equipment and has the function of NTDP in the port of a copy of the request message and sends it to the adjacent equipment; the response message contains the topological equipment basic information and all adjacent equipment information NDP.
- The neighbour device receives the request message and executes the same operation until the topology collects the request packets to all devices within the specified hop range.

When the topology collection request message diffusion within the network, a large number of network equipment also received the request and send topology collection response message, in order to avoid network congestion and task management device is busy, you can take the following measures to control the topology collection request message diffusion speed:

- After receiving the topology collection request, the device does not immediately forward the topology collection request packet, but delays waiting for a certain time, and then begins to forward the topology collection request packet at the port enabling the NTDP function.
- On the same device, except for the first port, each port enabled the NTDP function to send the topology collection request message at the previous port, and then it will delay a certain period of time before forwarding the topology collection request packet.

21.1.5 Cluster management maintenance

1) Candidate devices join clusters

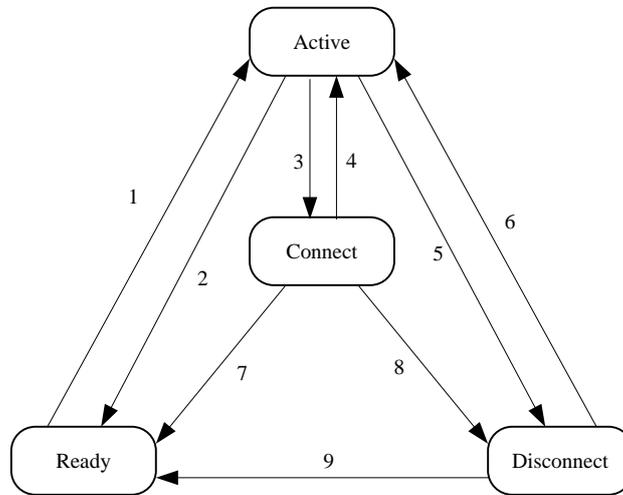
The user should first specify the management of equipment in the establishment of the cluster, management of equipment through the NDP and NTDP protocol to discover and identify the candidate equipment, the candidate equipment automatically join the cluster, can also manually configure the candidate device to join the cluster.

After the candidate device is successfully added into the cluster, the cluster member sequence number and cluster management of the management device allocated to it are obtained

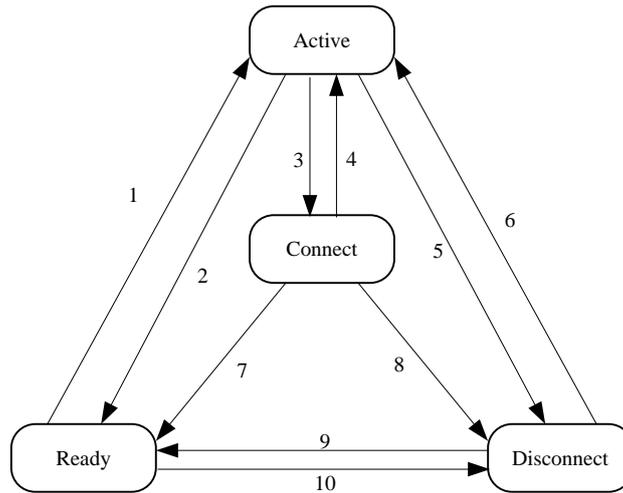
Private IP addresses used, etc.

2) Trunking communication

In the cluster, the management device and the member device communicate with each other through handshake message to maintain the connection state between them and manage the connection state of the equipment and member equipment as shown in the following picture.



State transition diagram of command switch



Member switch state transition graph

The command switch collects the basic information of the device, identifies a device as a candidate switch, and begins with the Ready state.

The deletion of member operations in any state migrates the state of the member switch back to the Ready state and identifies it as a candidate switch.

- The cluster is established successfully, the candidate to become a member of the equipment into the equipment cluster, management of equipment status information is saved to the local members of equipment, and the member state is identified as Active, a member of equipment will also be saved to the local state information itself, and its status is identified as Active.

- Management device and member device send handshake message regularly. After receiving the handshake message of the member equipment, the management equipment does not respond, keeps the member equipment as Active state, and the member equipment does not respond, and keeps the state of itself as Active.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

- If the management of equipment to send handshake message member device at three times handshake message transmission time interval is not received within the handshake message sending members of equipment, will be saved in the local members of the state of the device by Active migration to Connect; similarly, if a member of equipment to management did not receive a handshake message sending management equipment three times handshake message transmission time interval by transmitting handshake message, its status will migrate from Active to Connect.

- If the management of equipment received in the Connect state member of the device to send in effective reservation time handshake message or message management, the member state of the device transfer back to Active, otherwise the migration is Disconnect, in which management equipment that the member is disconnected; in the Connect state member of the equipment if the retention time received the sending equipment management handshake message or message management, its state will migrate to Active, otherwise it will migrate to Disconnect.

- When the restoration of communications equipment and management of equipment members interrupted when the device is in the Disconnect state members will rejoin the cluster join after the success of members in the management of equipment and the local state will return to Active.

If topology changes are found, member devices also pass the change information to the management device through handshake messages.

21.1.6 Managing VLAN

Managing VLAN limits the scope of cluster management. By configuring VLAN, the following functions can be implemented:

- The management message of cluster (including NDP, NTDP message and handshake message) will be limited in the management of VLAN, isolated from other messages, which increases the security.

- Managing devices and member devices to implement internal communications by managing VLAN.

Cluster management requirements management equipment and members / candidate device port, including cascade port (when the candidate device is connected by another candidate equipment and management of equipment, equipment connected to each candidate between ports are called cascade port) allows management through VLAN, so:

- If the port does not allow VLAN to pass through, the device connected to the port cannot join the cluster, so the cluster should be connected with the management device before the cluster, including the cascade port, allowing the management of the VLAN to pass.

- Only when the management of equipment and equipment connected to the member / candidate port and port default VLAN ID cascade is the management of VLAN, the message will allow the configuration management of VLAN with no label through, otherwise the message management must be labelled by VLAN.

For VLAN, see Chapter sixth configuring VLAN.

21.2 Brief introduction of cluster configuration

Before the user configures the cluster, it is necessary to define the roles and functions of each device in the cluster and configure the related functions to do the planning work for the communication with the internal equipment of the cluster.

Configuration task	Detailed configuration	
Configuration management equipment	NDP function of enable system and port	15.3.1
	Configuring NDP parameters	15.3.2
	NTDP function of enable system and port	15.3.3
	Configuring NTDP parameters	15.3.4
	Configure manual collection of NTDP information	15.3.5
	Enable cluster function	15.3.6
	Build clusters	15.3.7
	Configuring internal member interactions in clusters	15.3.8
	Configuring cluster member management	15.3.9
Configuration member device	NDP function of enable system and port	15.4.1
	NTDP function of enable system and port	15.4.2
	Configure manual collection of NTDP information	15.4.3
	Enable cluster function	15.4.4
Configuring cluster members to access each other		15.5

Note:

After the cluster is established, the cluster will not dissolve when the NDP or NTDP function is closed on the management device and member device, but it will affect the normal operation of the cluster that has been established.

21.3 Configuration management equipment

21.3.1 Enable system and port NDP capabilities

Command	Description	CLI mode
ndp global enable	Enabling global NDP functionality. Global shutdown by default.	Configuration mode
ndp enable	The NDP function of enable ports. All ports are closed by default NDP	Interface configuration mode

Note:

- The NDP function of both the global port and the port must be enabled, and the NDP can run normally.
- NDP function does not support aggregated ports.
- In order to avoid the topology information of the devices that are not required to join the cluster during topology collection and add it to the cluster, it is recommended that the NDP function be closed on the ports that do not need to join the cluster device.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

21.3.2 Configuring NDP parameters

Command	Description	CLI mode
ndp aging-timer <aging-time>	Configure the aging time of the NDP message sent by the device on the receiving device. Default 180 seconds.	Configuration mode
ndp hello-timer <hello-time>	Configuring the time interval for NDP packets to be sent. Default 60 seconds.	Configuration mode

Note

The aging time of NDP message on the receiving device cannot be less than the NDP transmission time interval, otherwise it will cause the instability of the NDP port neighbour information table.

21.3.3 Enable system and interface NTDP capabilities

Command	Description	CLI mode
ntdp global enable	Enabling global NTDP functionality. Global shutdown by default.	Configuration mode
ntdp enable	The NTDP function of enabled ports. All ports are closed by default NDP	Interface configuration mode

Note:

- The NTDP function of both the global port and the port must be enabled, and the NTDP can run normally.
- NTDP function does not support aggregated ports.
- In order to avoid the topology information of the devices that are not required to join the cluster during topology collection and add it to the cluster, it is recommended that the NTDP function be closed on the ports that do not need to join the cluster device.

21.3.4 Configuring NTDP parameters

Command	Description	CLI mode
ntdp hop <hop-value>	The range of configuration topology collection. By default, the maximum number of hops from the topology collection device is 3 in the topology collected.	Configuration mode
ntdp timer <interval-time>	Time interval for configuring timing topology collection. Default 1 minutes.	Configuration mode
ntdp timer hop-delay <time>	Configuring the collected device before the first port forwards the topology to collect the waiting time before the request message.	Configuration mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

	Default 200 milliseconds.	
ntdp timer port-delay <time>	Configure port delay time for current device forwarding topology to collect requests. Default 20 milliseconds.	Configuration mode

21.3.5 Configure manual collection of NTDP information

After the cluster is established, the management equipment collects the topology information periodically. In addition, users can manually collect NTDP information manually (regardless of whether the cluster is established), and initiate a collection process of NTDP information, so as to effectively manage and monitor the equipment more effectively.

Command	Description	CLI mode
ntdp explore	Topology information is collected manually.	Common mode, privileged mode

21.3.6 Enable cluster function

Command	Description	CLI mode
cluster enable	Enable cluster function. The default cluster function is closed.	Configuration mode

21.3.7 Build clusters

Managing VLAN limits the scope of cluster management. By configuring VLAN, the following functions can be implemented:

- The management message of cluster (including NDP, NTDP message and handshake message) will be limited in the management of VLAN, isolated from other messages, which increases the security.
- Managing devices and member devices to implement internal communications by managing VLAN.

Command	Description	CLI mode
cluster management-vlan <vlan-id>	Designated management VLAN. The default management VLAN is VLAN1.	Configuration mode

Note:

If the current device is in the cluster, it is not allowed to modify the management VLAN.

The situation is not in the cluster:

- 1) Check whether the VLAN exists, no direct failure exists, and move on to the next step
- 2) Re check all the interfaces, if the interface where VLAN and management VLAN is not the same VLAN, then open the global switch of NDP and ntdp are closed, and do the corresponding closed empty operation, and then re-opened.
- 3) Find the three layer interface that you want to configure VLAN. If you don't find it, create a new three level interface to the VLAN. If the new build fails, you can manage VLAN

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

configuration successfully, you can NDP and ntdp, but you can't join the cluster.

- 4) The MAC of the three layer interface is set to dev_id. If the VLAN is set up successfully and the new three layer interface fails, then the vlan1 of MAC is used as dev_id

If the configuration management of VLAN, but the user directly in the VLAN database to remove the VLAN, it will automatically manage the VLAN set to vlan1, NDP, ntdp and global switch will open and clusters are closed and the corresponding empty closed operation.

In the establishment of the cluster, the user must first set the members of equipment used in the cluster private IP address range, when the candidate device is added, the distribution of private IP address can be used in a cluster within the scope of the dynamic management of equipment and given to the candidate for the communications equipment within the cluster, in order to achieve the management of equipment management members and maintenance.

note :

Command	Description	CLI mode
cluster ip-pool <IP/MASK>	Configure the private IP address range used by the member devices in the cluster on the device that you want to set up to manage the device.	Configuration mode

- The IP address and cluster address pool of the VLAN interface for managing device and member devices cannot be configured on the same network segment, otherwise the cluster will not work properly.
- Only when the device is not in the cluster can it be configured.
- Use management VLAN to find whether there is a corresponding three layer port, if there is no three layer, the direct return failure. (this device cannot be a cluster command exchange). If there are three levels of interface, the base address of the IP-POOL is configured to the three port, and if the configuration fails, IP-POOL is configured to fail.

By default, the device is not managed by the device, and the cluster is established:

Command	Description	CLI mode
cluster build <name>	Manually build clusters, configure the current device to manage the device, and assign a cluster name.	Configuration mode
cluster auto-build <name>	Auto build cluster. The automatic cluster function automatically adds all the candidate devices found within the specified hop count to the created cluster.	Configuration mode
cluster delete <name>	Delete cluster.	Configuration mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

cluster stop auto-add member	Automatically set up cluster configuration, stop automatically adding member switches. This operation can only stop adding new devices, and the devices that have been added to the cluster will remain in the cluster.	Configuration mode
------------------------------	---	--------------------

Note:

- The user can only specify the management VLAN before the cluster is established. After the device has joined the cluster, the user cannot modify the management VLAN. If you need to change the management VLAN after the cluster is established, you need to delete the cluster on the management device, reassign the management VLAN, and finally re build the cluster.
- For security reasons, it is recommended that management VLAN should not be configured to manage the connection ports between devices and member devices, and the default VLAN ID of cascading ports.
- Only when connected to the equipment and management of equipment and all members of the port cascade port default VLAN ID is the management of VLAN, the message cannot allow management of the VLAN tag through, otherwise must be connected to configuration management equipment, equipment and all members of the port cascade allowed VLAN management message with label through, please refer to "VLAN specific configuration".
- The configuration of the private IP address range of the member devices in the cluster can only be configured when the cluster has not been established and can only be configured on the management device. If the cluster has been established, the system does not allow to modify the IP address range.

21.3.8 Configure the cluster's internal members to interact

In the cluster, management equipment and equipment for real-time communication by members to maintain the handshake message, the connection state between them, we can effectively keep the time allocation handshake message sent in the management of equipment on time interval and equipment, the configuration will also effect the cluster members of all equipment.

Command	Description	CLI mode
cluster timer <interval-time>	Configuring the time interval for handshake packets to be sent. Default 10 seconds.	Configuration mode
cluster holdtime <hold-time>	Effective retention time of configuration device. Default 60 seconds	Configuration mode

21.3.9 Configuring cluster member management

The user can manually specify the candidate devices to join in the cluster, or manually delete the specified member devices in the cluster. The join / delete operations of cluster members must be carried out on the management device, otherwise the error prompt message will be returned.

Command	Description	CLI mode
cluster add member mac-address <mac-address>	Adding candidate devices to clusters.	Configuration mode
cluster delete member mac-address <mac-address>	Deleting member devices from a cluster.	Configuration mode

21.4 Configuration member device

21.4.1 Enable system and port NDP capabilities

See the 18.3.1 enabled system and port's NDP function

21.4.2 Enable system and port NTDP capabilities

See the 18.3.3 enabled system and port's NTDP function

21.4.3 Configure manual collection of NTDP information

See 18.3.5 configuration for manually collecting NTDP information

21.4.4 Enable cluster function

See 18.3.6 enable cluster functionality

21.5 Configuring access cluster members

After the NDP, NTDP and cluster functions are properly configured, the members of the cluster can be configured, managed and monitored by the management device. You can configure the member device configuration on the management device to switch to the specified member device operating interface.

Command	Description	CLI mode
cluster switch-to member <member-number>	Switch from management device operation interface to member device operation interface.	Normal mode, privileged mode

Note:

The connection between cluster management equipment and member equipment is connected by Telnet, so it is necessary to pay attention to switch:

- Before switching, the end device needs to execute the "telnet server enable" command to enable the telnet function, otherwise it will result in the handover failure.
- From the management device to the member device, if the member number n does not exist, an error message will be displayed. If the device Telnet user logged on is full, the handover failure will result.

21.6 Cluster management display and maintenance

Command	Description	CLI mode
show ndp[interface <ifname>]	Display NDP configuration information	Normal mode, privileged mode
reset ndp statistics [interface <ifname>]	Clear NDP statistics	Configuration view
show ntdp	Display system NTDP information	Normal mode, privileged mode
show ntdp device-list	Display device information collected by NTDP	Normal mode, privileged mode
show ntdp single-device mac-address <mac-address>	Displays the NTDP details of the specified device	Normal mode, privileged mode
show cluster	The status and statistical information of the cluster to which the device belongs	Normal mode, privileged mode
show cluster topology	Display cluster topology information	Normal mode, privileged mode
show cluster candidates [mac-address <mac-address>]	Display candidate device information	Normal mode, privileged mode
show cluster members [<member-number>]	Display cluster member information.	Normal mode, privileged mode

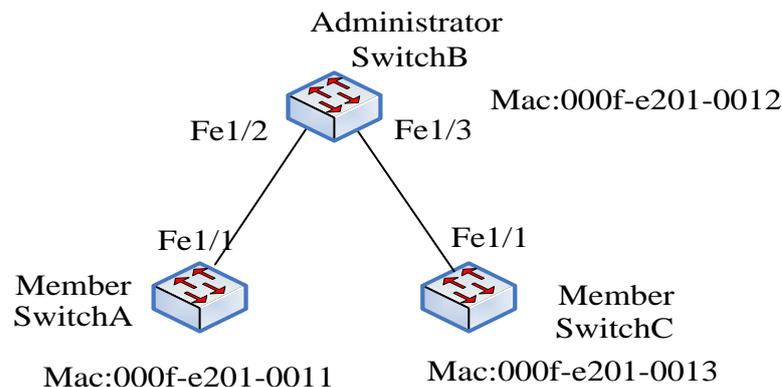
21.7 Example of cluster management typical configuration

1. Networking requirement:

The network ABC consists of three switches and the management VLAN is VLAN 10. Among them, Switch B is management equipment (Administrator); Switch A and Switch C are member devices (Member).

The base address IP of the cluster address pool is 10.0.0.1, supporting 8 devices.

2. Network diagram:



Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

3. Configuration steps:

Configuring member device SwitchA

Configuration management VLAN.

[SwitchA] cluster management-vlan 10

[SwitchA] interface ge1/1

[SwitchA-ge1/1] switch trunk vlan 10

Enabling global NDP functionality and NDP functionality on port ge1/1.

[SwitchA] ndp enable

[SwitchA] interface ge1/1

[SwitchA-ge1/1] ndp enable

Enabling global NTDP functionality and NTDP functionality on port Ethernet1/0/1.

[SwitchA] ntdp enable

[SwitchA] interface ge1/1

[SwitchA-ge1/1] ntdp enable

Enable cluster function.

[SwitchA] cluster enable

Configuring member device SwitchC

Because the configuration of the member devices is the same, the configuration on Switch C is similar to that of Switch A.

Configuration management device SwitchB

Configuration management VLAN.

[SwitchB] cluster management-vlan 10

[SwitchB] interface ge1/2

[SwitchB-ge1/2] switch trunk vlan 10

[SwitchB] interface ge1/3

[SwitchB-ge1/3] switch trunk vlan 10

Enabling global NDP and NTDP functions and enabling ports ge1/2 and ge1/3 on the NDP, NTDP functions.

[SwitchB] ndp enable

[SwitchB] ntdp enable

[SwitchB] interface ge1/1

[SwitchB-ge1/2] ndp enable

[SwitchB-ge1/2] ntdp enable

[SwitchB] interface ge1/3

[SwitchB-ge1/3] ndp enable

[SwitchB-ge1/3] ntdp enable

The aging time of the NDP message sent by the device is 200 seconds on the receiving device.

[SwitchB] ndp timer aging 200

The time interval for configuring the NDP message is 70 seconds.

[SwitchB] ndp timer hello 70

The maximum number of hops collected by the configuration topology is 2 hops.

[SwitchB] ntdp hop 2

Configuring the first port of the collected device to forward the topology, the delay time of collecting the request packets is 150ms.

[SwitchB] ntdp timer hop-delay 150

The delay time of collecting request packets of other ports forwarding topology is 15ms.

[SwitchB] ntdp timer port-delay 15

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

The configuration topology collects intervals of 3 minutes.

[SwitchB] ntdp timer 3

Enable cluster function.

[SwitchB] cluster enable

The private IP address of the configured member device ranges from 10.0.0.1 to 10.0.0.9.

[SwitchB] cluster ip-pool 10.0.0.1 8

Configure the current device to manage the device, and build a cluster called ABC, members automatically join the cluster.

[SwitchB] cluster autobuild abc

When you add all the switches you want to add, you can turn off and automatically join the cluster function

[SwitchB]cluster stop auto-add member

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

22. System log configuration

The main contents of this chapter are as follows:

- System log introduction
- System log configuration
- configuration SYSLOG

22.1 System log introduction

The system log module is an important part of the switch, it is used to record the operation of the whole system, operation behaviour and abnormal behaviour of users, to help administrators understand and monitor the switch. The system log module management system all comes from the log information of the running modules, collects, sorts, stores and displays the output of the log information.

There is also an important debugging function in the log system. System log with debugging can help administrators or other technical personnel to monitor the operation of the network, debug and diagnose the fault in the network. Administrators can easily select the content that needs debugging, and by observing the log information of debugging output to locate and solve the fault of equipment or network.

The main contents of this section are as follows:

- Format of log information
- Log storage
- Log display
- Debugging tools

22.1.1 Format of log information

The format of log information is as follows:

Timestamp priority: module name: log content

There is a space between the timestamp and the priority. There is a colon and a space between the priority and the module name. There is a colon and a space between the module name and the content of the log.

An example of the format of log information is as follows:

```
2006/05/20 13:56:34 Warning: MSTP: Port up notification received for port ge1/2
```

In this log message, the timestamp is 2006/05/20 13:56:34; the priority is Warning; the module name is MSTP; the log content is Port up notification received for port ge1/2.

1) Time stamp

Timestamp format: year / month / day hours: Minutes: seconds.

The hours are 24 hours, from 0 to 23.

The timestamp records the time that the log information was generated, and the system time of the switch was used. System time has been set up in the switch factory, administrators can also modify the system after power failure, the system is still able to run.

2) Priority

Priority records the importance of the log information. According to the importance of the log information, the log information is divided into four levels. The order of priority is from high to low: Critical, Warning, Informational and Debugging. The description of priority is as follows:

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Priority	Description
Critical	Serious mistake
Warning	Common mistakes, warnings, very important tips
Informational	Important hints, general tips, diagnostic information
Debugging	debug information

3) Module name

The module name records the module generated by the log message, and the following table lists some of the main modules that generate log information:

Module name	Description
CLI	Command line interface module
MSTP	Multi instance spanning tree protocol module
VLAN	VLAN function module
ARP	ARP protocol module
IP	IP protocol module
ICMP	ICMP protocol module
UDP	UDP protocol module
TCP	TCP protocol module

4) Log content

Log content is a phrase or sentence, which represents the content of the log message. The administrator can know what happened in the system by reading the log content.

22.1.2 Log storage

There are three ways to store logs:

- The log is stored in memory.
- Log storage to NVM.
- Log storage to server.

There are four priority according to the log table in memory, each table log information stored a priority, which is based on the priority of the log is divided into four categories, there is a separate log table for each log. Each log table has 1K entries, which can store 1K log information. When the log table is full, the log information with the longest coverage is behind the log. This storage method has a problem, when the system restarts, the log information is gone, the administrator cannot see the log information when the system crashes, cannot locate the problem.

For important log information, such as log information of priority Critical and Warning, these log information can be stored in the NVM of the system. In this way, the log information in NVM can be retained after the system is restarted, so that the administrator can locate the problem when the system crashes. But there is a problem with this storage method because of the limited capacity of NVM, and the log information entries stored in NVM are very limited.

There is a better way is to store your log messages to the server, using the SYSLOG protocol can achieve real-time, log information can be sent to the server, the server to save the log information and displayed on an interface. This storage mode is not only convenient for users to view log information, but also has huge capacity. It can store a large amount of log information on the server.

At present, the system only supports the storage of log information into memory and does not support the storage of log information into NVM or server.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

22.1.3 Log display

There are two ways to display logs: manual display and real-time display. Manual display is that the user displays the log information by inputting the command, and the real-time display is when the log information is generated, the log information is directly output to the terminal, and the user can see it in time.

For manual display, the user can view all the log information, or view a priority log information. The display order of the log information is the last log information, so that the user can first see the latest running state of the switch.

For real-time display, the user must open the terminal real-time display switch. If the switch is open, the log information is not only written into the log table, but also the log information is exported to the terminal. If the switch is closed, the log information will not be displayed on the terminal in real time. The system can only log information real-time output to the Console terminal, does not support the log information output to the Telnet terminal.

22.1.4 Debugging tools

Debugging is a useful diagnostic tool for network device, system and module of data packet transceiver module, state machine change tracking process allows administrators to understand and monitor systems and modules, or if the network equipment appeared abnormal situation, through the debugging tracking tool.

Debugging tools provide rich switches, and by controlling these switches, administrators can track what they're interested in. When the device or network is out of order, the administrator can open the debugging switch associated with this exception and find the problem by tracking the execution of the system and the module.

When a debugging switch is turned on, the system generates log information that will be written to the corresponding log table. In general, the priority of log information generated by debugging is Informational. When the terminal real-time display switch is opened, the log information will be output to the terminal in real time. When the debugging switch is turned off, the system does not generate log information.

22.2 System log configuration

The system log configuration includes the following :

- Configuring terminal real time display switch
- View log information
- Configure debugging switch
- View debugging information

22.2.1 Configuring terminal real time display switch

By default, the terminal real-time display switch is closed, and the log information generated by the system is written into the log table, but it will not be displayed on the terminal in real time.

There are also some log information in the system that are not limited by this switch. These log messages are always output to the Console terminal in real time.

The terminal display switch is corresponding to the priority and the system log, if a priority terminal real-time display switch is turned on, the log information of the priority will be displayed on the terminal in real time, if the terminal display switch does not turn a priority, the priority of the log information is not displayed in real time on the terminal.

The switch can only display the log information on the Console terminal in real time and cannot display the log information on the Telnet terminal in real time.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

When the user uses the write command to the system configuration stored in the configuration file, real-time display terminal switch configuration will be stored into the system files, when the system restarts the configuration will be lost, need to re configure.

Configure the terminal real-time display switch command as follows:

Command	Description	CLI mode
log display [critical warning informational debugging]	Open terminal real time display switch. If you do not input parameters, open all priority terminal real-time display switch, if you enter one of the parameters, open the specified priority terminal real-time display switch.	Privileged mode
no log display [critical warning informational debugging]	Close the terminal real time display switch. If you do not input parameters, turn off all priority terminal real-time display switches, if you enter one of the parameters, close the specified priority terminal real-time display switch.	Privileged mode

22.2.2 View log information

The commands for viewing log information are listed below:

Command	Description	CLI mode
show log display	Real time display switch configuration for displaying all priority terminals.	Normal mode, privileged mode
show log [critical warning informational debugging]	Display log information in log table. If you don't input parameters, display all log table log information, if you enter one of the parameters, display the log information of the specified priority log table.	Normal mode, privileged mode

22.2.3 Configure debugging switch

The switch provides a rich debugging capability, involving multiple modules which only lists the commands of each module and the complete format of the commands. See the command manual. When the user uses the write command to the system configuration stored in the configuration file, debugging switch configuration will be stored into the system files, when the system restarts the configuration will be lost, need to re configure.

The schematic command for configuring the debugging switch is as follows:

Command	Description	CLI mode
debug ip ...	Open system to send and receive IP packet related debugging switch.	privileged mode
no debug ip ...	Close debugging switches for sending and receiving IP packets.	privileged mode
debug ip icmp ...	Open system to send and receive ICMP packet related debugging switch.	privileged mode
no debug ip icmp ...	Close debugging switches for sending and receiving ICMP packets.	privileged mode
debug ip arp ...	Open system to send and receive ARP packet related debugging switch.	privileged mode
no debug ip arp ...	Close debugging switches for sending and receiving ARP packets.	privileged mode
debug ip udp ...	Open system to send and receive UDP packet related debugging switch.	privileged mode
no debug ip udp ...	Close debugging switches for sending and receiving UDP packets.	privileged mode
debug ip tcp ...	Open system to send and receive TCP packet related debugging switch.	privileged mode
no debug ip tcp ...	Close debugging switches for sending and receiving TCP packets.	privileged mode
debug mstp ...	Open the debugging switch related to MSTP protocol diagnostics.	privileged mode
no debug mstp ...	Close debugging switches related to MSTP protocol diagnostics.	privileged mode
debug igmp snooping ...	Open IGMP SNOOPING function diagnostic related debugging switch.	privileged mode
no debug igmp snooping ...	Close IGMP SNOOPING function diagnostic related debugging switches.	privileged mode
debug dhcp snooping ...	Open DHCP SNOOPIN protocol for diagnosis of related debugging switches	privileged mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

no debug dhcp snooping ...	Close the DHCP SNOOPIN protocol diagnostic debugging switch	privileged mode
no debug all	Turn off all debugging switches in the system.	privileged mode

22.2.4 View debugging information

The commands for viewing the debugging information are as follows:

Command	Description	CLI mode
show debugging [ip mstp igmp snooping dhcp snooping]	See the debugging switch configuration. If you don't have input parameters, look at the debugging switch configuration of all modules. If you only input one of these parameters, you only look at the debugging switch configuration of a module. If the input parameter is IP, the debugging switch configuration of the IP, ICMP, ARP, UDP, and TCP modules will be checked.	Normal mode, privileged mode

22.3 SYSLOG configuration

SYSLOG includes the following:

- SYSLOG introduce
- SYSLOG configuration
- SYSLOG configuration example

22.3.1 SYSLOG introduction

SYSLOG is a standard protocol for the management of equipment log information, which has been greatly applied because of its simplicity of design. In the SYSLOG system, it is divided into three parts. One is to define each sub module to distinguish the log information produced by different modules; define different log information levels to observe the running status of the device. All kinds of log information of the equipment are collected according to this agreement. The second is the configuration file, how to deal with the custom log information collected, can be stored in local, can be sent to the network server specified, can be sent to the specified user login log information and so on; by the configuration file to decide how to save the equipment. The third is to send SYSLOG protocol message according to the message format defined by RFC. As you can see, in our switch system, the whole SYSLOG work convention is the system log module. The first part of the SYSLOG protocol is completed by each function sub module of the switch and sends the log information of each level to the system log module. Maintaining four levels of log tables in the system log module. The second part of the SYSLOG protocol by the system log module to uniform distribution of log information, one is through the terminal display switch or real-time display in the serial port terminal two is stored manually; log table four levels in memory; three is to save the log information of high level on the NVM log records in order to avoid the loss of important power failure; the four is the log is sent to the remote server storage,

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

collecting and sorting through the SYSLOG message. The SYSLOG sub module in the system log module only implements third parts and transmits the system log to the server.

22.3.2 SYSLOG configuration

The SYSLOG configuration command contains :

- Open syslog protocol
- Closing the syslog protocol
- Set syslog send level
- Restore syslog send level to default value

Command	Description	CLI mode
syslog open <server-ip> [udp-port]	Open the syslog protocol; server-ip parameters for the server IP address is required; udp-port parameters for the destination port number, protocol message optional, if not set to the default value of 514; if the server configuration and set to be consistent.	Global configuration mode
syslog close	Closing the syslog protocol	Global configuration mode
syslog level <critical warning informational debugging>	Set the sending level of the log, such as set to debugging level, all the logs will be sent to the server.	Global configuration mode
no syslog level	Restore the send level to the default value debugging	Global configuration mode

22.3.3 SYSLOG configuration example

(1) Configuration

Configure the syslog server IP address for the 192.168.2.201 server configuration software receives the syslog message UDP to port 200; the ge1/3 port is connected to the server; the server saves only a maximum of two levels of logging.

The switch is configured as follows:

```

Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config-vlan)#exit
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport access vlan 2
Switch(config-ge1/3)#interface ge1/4
Switch(config-ge1/4)#switchport access vlan 2
Switch(config-ge1/4)#interface ge1/5
Switch(config-ge1/5)#switchport access vlan 3
Switch(config-ge1/5)#interface ge1/6
Switch(config-ge1/6)#switchport access vlan 3
Switch(config-ge1/6)#interface vlan2
Switch(config-vlan2)#ip address 192.168.2.1/24

```

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

```
Switch(config-vlan2)#exit
Switch(config)#syslog open 192.168.2.201 200
Switch(config)#syslog level warning
```

(2) Verification

```
Switch#show running-config
!
syslog open 192.168.2.201 200
syslog level warning
!
.....
!
line vty
!
end
```

```
Switch#show syslog
Syslog is opened!
server ip address: 192.168.2.201
udp destination port: 200
severity level: warning
```

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

23. Port loop

The main contents of this chapter are as follows:

- profile
- Protocol principle
- Configuration introduction

23.1 Profile

When the loop appears a port switch condition, will cause the broadcast storm this port, and all radio package source MAC address to the learning loop port forwarding will cause the equipment cannot be normal.

23.2 Protocol principle

Ethernet Loop Detection Protocol (Ethernet Loopback Detection, referred to as ELD) can detect loops through the interaction of packets and the port ELD protocol that blocks the loops is a protocol based on port calculations and can only detect the loops that occur on this port.

23.2.1 Detection process

When a port is enabled with the ELD protocol, this will enable a timer and until the timer expires it will send loop detection packets. If during the timer duration their own loop protection packet is received then it is assumed that there is a loop and the switch will execute the loop execution port blocking operation and empty this port FDB.

If a port is a port member of multiple VLANs, then this port automatically sends loop detection packets to all VLANs. That is to say, this port automatically detects whether all VLAN loops belong to it.

23.2.2 Recovery mode

When a port loop appears, the port will be blocked. The ELD protocol has two types of recovery patterns that users can configure: automatic recovery and manual recovery.

Automatic recovery is when a port is blocked after the receipt of its loop protection packets, ELD protocol enabled a recovery timer and when the timer expires the switch will perform a blocking loop reverse operation, and in the port loop detection timer is enabled again and loop protection packets are sent again.

Manual recovery is the port is blocked and the user must enter their commands to re-enable the port and recover from the port loop..

23.2.3 Protocol security

The ELD protocol in the network could potentially be attacked.

The ELD protocol uses strategies to prevent such attacks and minimize errors.

For example, the ELD protocol is a protocol without interaction, that is it does not rely on other devices and so the packet itself can be simply encrypted. Our operation here is to send the ELD protocol package with a key and the user cannot disguise the protocol packet without the key.

23.3 Configuration introduction

The ELD protocol is implemented based on ports, and there is no unified enable command.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

23.3.1 Global configuration

Global configuration is the uniform attribute of configuration protocol.

Command	Description	CLI mode
loop-detection detection-time <1-65535>	Configure the loop detection time, this time must be less than 2 times the recovery time, the default is 5 seconds.	Global configuration mode
loop-detection resume-time <10-65535>	The automatic recovery time must be greater than 2 of the loop check time. If the automatic recovery is enabled, this configuration will take effect. The default recovery time is 600 seconds.	Global configuration mode
loop-detection protocol-safety	Enable protocol security check, default is closed.	Global configuration mode
loop-detection respond-packets	Configure the number of packets that must be received within a certain period of time. If the protocol security check is enabled, this configuration will take effect, with the default value of 10	Global configuration mode

23.3.2 Interface configuration

The interface configuration is configured for each port.

Command	Description	CLI mode
Loop-detection enable	Enable ELD protocol on a port.	Interface configuration mode
Loop-detection resume	Manual recovery, restart loop check.	Interface configuration mode
loop-detection resume-mode {automation manual}	Configure recovery mode, select manual recovery or automatic recovery, default is automatic recovery.	Interface configuration mode
loopback-detection shutdown-mode {no-shutdown shutdown}	The command configures whether the port is shutdown when the loop is present.	Interface configuration mode

23.3.3 Display configuration

Show loop-detection [ifname]

Display all the configuration of the protocol and the configuration of an interface.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

24. SNTP configuration

The main contents of this chapter are as follows:

- SNTP introduction
- SNTP configuration
- SNTP information display

24.1 SNTP introduction

NTP is the most widely used communication protocol to monitor and set network time synchronization. NTP (Network Time Protocol Network Time Protocol) is a protocol that is a simplified version of the NTP protocol, namely SNTP (Simple Network Time Protocol simple network time protocol).

The NTP protocol can span a variety of platforms and operating systems, with a very sophisticated algorithm, so the effect of delay and jitter is almost not affected by the network and can provide 1-50ms accuracy. Using the NTP authentication mechanism, the security level is very high.

SNTP (Simple Network Time Protocol) is a simplified version of NTP, in the implementation of the calculation time using a simple algorithm, the performance is high, and the accuracy can generally reach about 1 second, but also basically meet the needs of most occasions.

Because the packets used by both SNTP and NTP message are completely identical, the SNTP Client implemented by this switch can be fully compatible with a NTP Server

24.2 SNTP configuration

24.2.1 Default SNTP settings

Project	Default value
SNTP state	Disable closes SNTP services
NTP Server	There are three NTP Server defaults 211.115.194.21 203.109.252.5 192.43.244.18
The synchronization time interval of SNTP	1800 second
local time zone	+8, East eight district

Open and close SNTP

Configuration is as follows:

Switch# configure terminal

Enter global configuration mode

Switch(config)# sntp enable

Open SNTP

Switch(config)# sntp disable

Close SNTP

24.2.2 Configuring SNTP Server address

Because SNTP's packets and NTP are exactly the same, so SNTP Client can use the existing the NTP Server network.

A specific NTP server address can be found on <http://www.time.edu.cn/> or <http://www.ntp.org/>

For example: 192.43.244.18 (time.nist.gov)

Document Title	Related to
RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

This switch has three default Server addresses, 211.115.194.21, 203.109.252.5 and 192.43.244.18 respectively, the switch uses the first Server address listed to the synchronization time, if synchronization fails then uses the second Server addresses, and so on. In general, users do not need to configure the Server address and an use the default Server address as it is configured by default. If you need to configure the Server address in a special case, you need to delete the default Server address first and then add a new Server address.

Add a Server address configuration as follows:

Switch# configure terminal

Enter global configuration mode

Switch(config)# sntp server 210.72.145.44

Add SNTP server IP, if the switch already has three Server addresses configured, it will cause a failure if you add a fourth. You need to delete an address and then add the new address.

The deletion of a specific Server address is as follows:

Delete all Server addresses

Switch(config)# no sntp server

Delete the Server address 210.72.145.44

Switch(config)# no sntp server 210.72.145.44

To configure the default SNTP server address use the following command:

Switch(config)# sntp server default

The Server address is reset to the default addresses.

24.2.3 Configure the SNTP sync clock interval

SNTP Client requires a timer to monitor the set NTP servers and correct and incorrect clock setting.

Configuration is as follows:

Switch# configure terminal

Switch(config)# sntp interval 60

Set the timing synchronization clock interval, the unit is seconds, the range is 60 seconds -65535 seconds. The default value is 1800 seconds, this command set it to 60 seconds

Switch(config)# no sntp interval

The timing synchronization clock interval is restored to the default 1800 seconds

24.2.4 Configuring the local time zone

The SNTP protocol includes time zones. This is configured so that the time is shows to the correct local time even if the NTP server used is not in the same time zone.

Configuration is as follows:

Switch# configure terminal

Switch(config)# sntp time-zone -0

Set the local time zone to GMT

Switch(config)# no sntp time-zone

The local time zone is restored to the default value -8

24.3 SNTP information display

Configuration is as follows:

Switch# show sntp

Switch# show running-config

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

25. OAM configuration

The main contents of this chapter are as follows:

- OAM introduction
- OAM configuration
- Typical configuration examples of OAM

25.1 OAM introduction

Ethernet OAM (Operations, Administration and Maintenance) is a tool to monitor network problems. It works at the data link layer and uses OAMPDU Protocol Data Units (OAM) to report the state of the network, so that the network administrator can manage the network more effectively.

At present, Ethernet OAM mainly solves the common link problem of "last mile" in Ethernet access. By enabling the Ethernet OAM function on two point to point devices, the link state between two devices can be monitored.

This section mainly introduces the main functions of Ethernet OAM, including the main functions of Ethernet :

- Link performance monitoring: it can detect link failures.
- Fault detection and warning: notify the network administrator in time when the link fails.
- Loop test: detecting link failures by returning non OAMPDU loops.

25.1.1 Link performance monitoring

Link monitoring is used to detect and detect link layer failures in various environments.

Ethernet OAM uses the interaction of Event Notification OAMPDU to monitor the link. When the link failure occurs, after the local link monitors the fault, the Event Notification OAMPDU is sent to the Ethernet OAM entity to notify the general link event. Administrators can observe the log information dynamically to grasp the status of the network.

Event type	Meaning	Description
Errored Symbol Event	Error signal event	In unit time, the number of false signals exceeds the threshold
Errored Frame Event	Error frame event	In unit time, the number of error frames exceeds the threshold
Errored Frame Period Event	Wrong frame periodic events	The number of error frames exceeds the threshold when the specified number of frames is received
Errored Frame Seconds Summary Event	Wrong frame seconds total event	Within the specified time, the number of frames per second exceeds the threshold

25.1.2 Remote fault detection

Ethernet fault detection is very difficult, especially when the network physical communication is not interrupted and the network performance drops slowly.

OAMPDU defines a flag (Flag domain) that allows Ethernet OAM entities to pass the fault information to the opposite end. The flag can represent the following emergency link events :

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Table 5 emergency link events

Event type	Meaning	Description	OAMPDU Sending frequency
Link Fault	Link fault	Loss of end-to-end link signal	Send once every second
Dying Gasp	Fatal fault	Unexpected local failures, such as power outages	Uninterrupted transmission
Critical Event	Emergency	Unclear emergency events, such as link single pass	Uninterrupted transmission

Ethernet OAM connection process is constantly sending Information OAMPDU, the end of the OAM entity can be the end of the emergency link event information through the Information OAMPDU to tell the remote OAM entity. In this way, the administrator can dynamically understand the state of the link, and deal with the corresponding errors in a timely manner.

25.1.3 Distal loopback

Yuan Duan loopback function refers to the active mode of the OAM entity to the end (Yuan Duan) send all other messages except OAMPDU, the end of the receipt of the message is directly returned to the end. It can be used to locate link failures and detect link quality: network administrators can judge the link performance (including packet loss rate, delay, jitter, etc.) by observing the return of non OAMPDU packets.

25.2 OAM configuration

Command	Description	CLI mode
oam errored-frame period <1-60>	Configuring Ethernet ports for periodic values of error frame event detection. The period of the default frame event is 1s.	Privileged mode
no oam errored-frame period	Reset Ethernet ports for periodic values of error frame event detection. The period of the default frame event is 1s.	Privileged mode
oam errored-frame threshold <0-4294967295>	Configuring thresholds for error frame event detection. The default error frame event threshold is 1.	Privileged mode
no oam errored-frame threshold	Reset threshold for error frame event detection. The default error frame event threshold is 1.	Privileged mode
oam errored-frame-period period <100-6000>	Configuring Ethernet ports to detect periodic values of false frame periodic event detection. The period of the default frame cycle event is 1000 milliseconds.	Privileged mode
no oam errored-frame-period period	Reset Ethernet ports for periodic values of false frame periodic event detection. The period of the default frame cycle event is 1000 milliseconds.	Privileged mode

oam errored-frame-period threshold <0-4294967295>	Configuring threshold values for periodic event detection in error frames. The default error frame event threshold is 1.	Privileged mode
no oam errored-frame-period threshold	Reset the threshold of periodic event detection for error frames. The default error frame event threshold is 1.	Privileged mode
oam errored-frame-seconds period <10-90>	Configuring Ethernet ports for periodic values of error frame seconds event detection. The period of the default frame event is 60s.	Privileged mode
no oam errored-frame-seconds period	Reset Ethernet port for periodic values of error frame seconds event detection. The period of the default frame event is 60s.	Privileged mode
oam errored-frame-seconds threshold <0-900>	Configuring thresholds for error frame seconds event detection. The default error frame seconds event threshold is 1.	Privileged mode
no oam errored-frame-seconds threshold	Reset error frame seconds threshold for event detection. The default error frame seconds event threshold is 1.	Privileged mode
oam mode (active passive)	Configure Ethernet OAM mode, default Ethernet OAM link mode as active mode.	Interface configuration mode
oam enable	Open Ethernet OAM function, default Ethernet OAM function is closed.	Interface configuration mode
oam loopback	Enable Ethernet OAM loopback function. Default Ethernet OAM loopback function shutdown.	Interface configuration mode
no oam loopback	Turn off Ethernet OAM loopback function. Default Ethernet OAM loopback function shutdown.	Interface configuration mode
show oam configuration	Displays the window and threshold of general link events.	Privileged mode
show oam local-state (IFNAME)	View OAM local information	Privileged mode
show oam remote-state (IFNAME)	View OAM peer to peer information	Privileged mode
show oam link-event (IFNAME)	View OAM link event information	Privileged mode
show oam-loopback IFNAME	Display loopback information of a port.	Privileged mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

25.3 Typical configuration examples of OAM

1 Networking requirement

By configuring the Ethernet OAM protocol on Device A and Device B, the data link layer is managed;
(Device A port: fe1/1, Device B port: fe1/1)

(1) Configuration Device A :

```
Switch>enable
Switch#configure terminal
Switch(config)# interface fe1/1
```

On port Ethernet1/0/1, configure its Ethernet OAM connection mode as passive mode and enable Ethernet OAM function.

```
Switch(config-fe1/1)#oam mode passive
Switch(config-fe1/1)#oam enable
```

(2) Configuration Device B:

```
Switch>enable
Switch#configure terminal
Switch(config)# interface fe1/1
```

The Ethernet OAM working mode of configuring port Ethernet1/0/1 is default mode active and can make Ethernet OAM function.

```
Switch(config-fe1/1)#oam enable
```

(3) Checking configuration effect on (Device A):

```
Switch>enable
Switch#show oam fe1/1
```

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

26. CFM configuration

The RT series of switches provides a CFM function, which is mainly used to detect link connectivity in a two layer network, confirm the fault and determine the location of the fault, including the following contents:

- CFM profile
- Brief introduction of CFM configuration task
- CFM base configuration
- Configure various functions of CFM
- CFM display and maintenance
- Typical configuration examples

26.1 CFM profile

CFM is the abbreviation of Connectivity Fault Management (connected error management). The CFM of this switch mainly refers to connected error detection, which follows the CFM protocol defined by IEEE 802.1ag. It is a two layer link based on end to end OAM VLAN (Operations Administration, and Maintenance, operation, management and maintenance) mechanism, mainly used in the two layer of the network detection link connectivity, confirm the fault and determine the fault position.

26.1.1 Basic concepts of CFM

1 Maintenance domain

The Maintenance Domain (MD) points out the network covered by the connectivity error detection, whose boundaries are defined by a series of maintenance endpoints configured on the port. The maintenance domain is marked by "domain name maintenance".

In order to locate the fault point accurately, the concept of level (hierarchy) is introduced into the maintenance domain. Maintenance domain is divided into eight levels, represented by integer 0~7, the larger the number, the higher the level, the greater the scope of the maintenance domain. Different maintenance domains can be adjacent or nested, but cannot cross, and nested can only be embedded by high-level maintenance domain to low-level maintenance domain, that is to say, low level maintenance domain must be included in the high-level maintenance domain. The CFM PDU of the low-level maintenance domain will be discarded after entering the high-level maintenance domain; the CFM PDU of the high-level maintenance domain can cross the low level maintenance domain; the CFM PDU of the same level maintenance domain cannot cross each other.

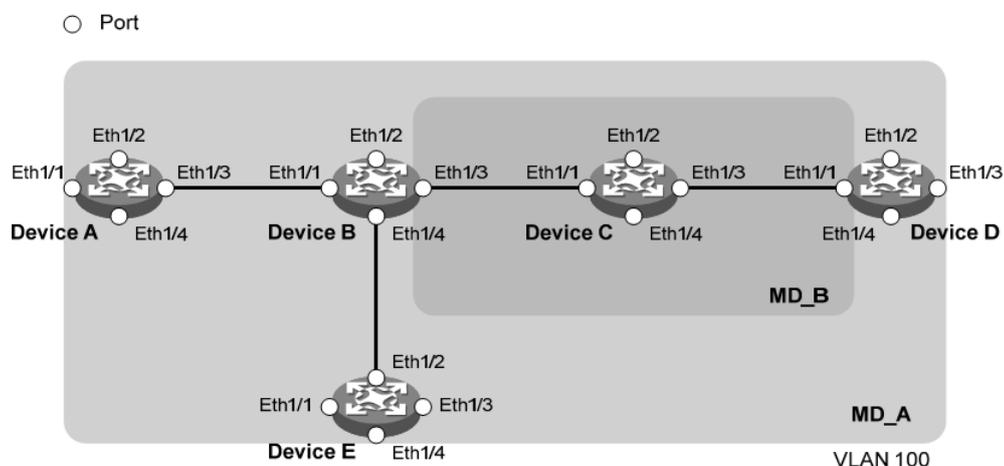


Figure 1-1

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

In practical application, to rational planning of maintenance domain: as shown in Figure 1-1, MD_B nested in the maintenance domain maintenance domain MD_A, to connectivity detection in MD_A, MD_A CFM PDU is required to cross the MD_B, it needs to be MD_A better than MD_B high level configuration. In this way, MD_A CFM PDU can pass through MD_B, so as to achieve the whole MD_A connectivity fault management, and the MD_B CFM PDU will not spread to MD_A.

Maintenance domain classification makes fault location more convenient and accurate, as shown in Figure 1-1, MD_B embedded in the maintenance domain maintenance domain MD_A, if it is found that the link is on the border of MD_A indicates that the domain of equipment malfunction, failure may occur in Device A ~ Device E five device. At this time, if not found in the MD_B link on the boundary of the fault range is reduced to Device B to Device D of the three sets of equipment; on the other hand, if the MD_B equipment is working properly, it can at least determine the Device C there is no fault.

2 Maintenance set

In the maintenance domain, Maintenance Association (MA) can be configured according to the requirements. Each maintenance set is a collection of maintenance points in the domain. The maintenance set is marked by "maintenance domain name + maintenance set name".

The maintenance set serves a VLAN, and the message sent by the maintenance point of the maintenance has the tag of the VLAN. Meanwhile, the centralized maintenance point can receive the message sent by the other maintenance points in the maintenance set.

3 Maintenance point

The maintenance point (Maintenance Point, MP) in port configuration, belong to a set of maintenance, maintenance can be divided into endpoint (Maintenance Association End Point, MEP) and the maintenance of the middle point (Maintenance Association Intermediate Point, MIP) two.

1) Maintenance endpoint

The maintenance endpoint is identified by an integer called MEP ID, which determines the scope and boundary of the maintenance domain. The maintenance set and maintenance domain belonging to the maintenance endpoint determine the VLAN attribute and level of the message sent by the maintenance endpoint.

The level of the endpoint determines the level of the message that it can handle, and the level of the message that maintains the endpoint is the level of the endpoint of the maintenance. When the maintenance endpoint receives a message above their level, not processed, but according to its original path forwarding; and when the message received is less than or equal to their maintenance endpoint level will no longer maintain the forwarding endpoint for the corresponding processing, to ensure a low level maintenance domain message will not spread to the high level maintenance domain.

Maintenance endpoints have directionality, which can be divided into two types: extroverted MEP and inward MEP. The direction of the endpoint maintenance indicates the location of the maintenance domain relative to the port.

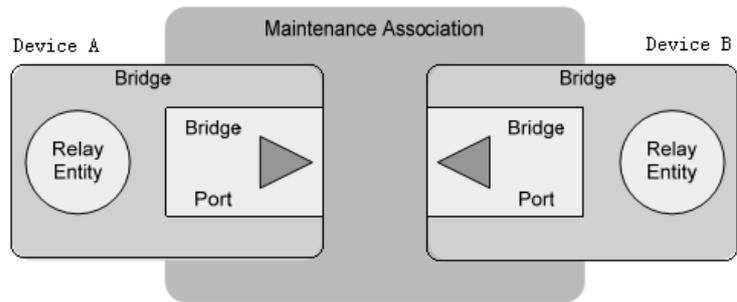


Fig. 1-2 schematic diagram of outgoing MEP

As shown in Figure 1-2, the outgoing maintenance endpoint sends the message outward through its port.

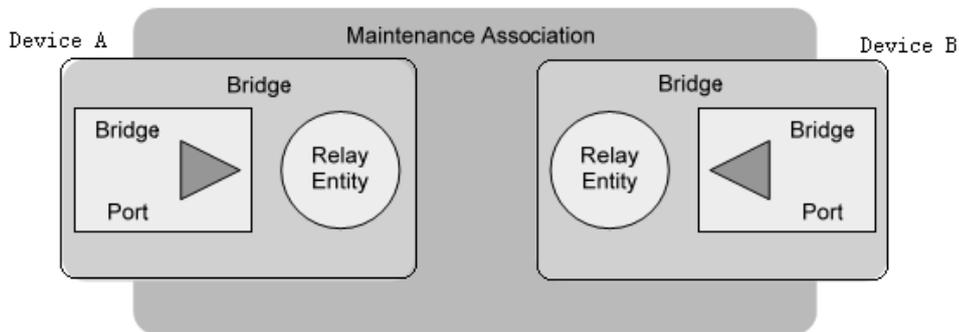


图 1-3

As shown in Fig. 1-3, the inward maintenance endpoint does not send messages outward through its ports but sends messages outward from other ports on the device.

2) Maintenance intermediate point

The maintenance intermediate point is located in the maintenance domain, and cannot send CFM protocol message actively, but it can process and respond to CFM protocol message. Maintaining the maintenance set and maintenance domain of the intermediate point determines the VLAN attribute and level of the received message of the maintenance intermediate point. Maintaining the intermediate point can be used with the maintenance endpoint to accomplish functions similar to Ping and tracert. Similar maintenance endpoints, while maintaining the middle point of message received above their level, not processed, but according to its original path forward; and when the message received is less than or equal to their own point maintenance intermediate level, will be processed.

As shown in Figure 1-4, is a hierarchical configuration of CFM, assuming that all six devices are only two ports, and the allocation of maintenance endpoints and maintenance intermediate points in some ports, such as the Device B port 1 configuration maintenance points are as follows: Level 5, level for the maintenance of intermediate point 3 within the maintenance endpoint, level 2 to level 0 maintenance endpoints and outgoing maintenance endpoint. There are four levels of maintenance domains in the graph. The maintenance area of the identification number is higher and the control range is wide; the maintenance area of the identification number is smaller and the control range is small.

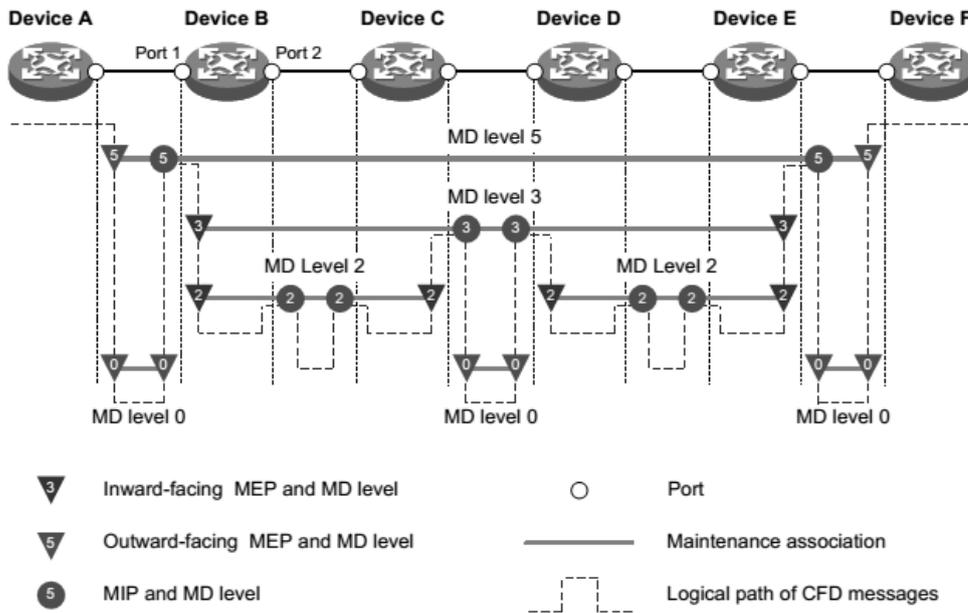


Figure 1-4 hierarchical configuration of maintenance points

4 Maintain endpoint list

The list is the same maintenance endpoint allows configuration within the set of local maintenance endpoints and the need to monitor the remote maintenance endpoint set, which defines a range of maintenance endpoint set: different devices on the same maintenance within the set of all maintenance endpoints should be included in this list, MEP and ID do not repeat. If the maintenance endpoint receives the CCM (Continuity Check Message, continuity check message) message from the remote device and the maintenance endpoint is not in the maintenance endpoint list of the same maintenance set, then the message is discarded.

5 Service instance

A service instance is represented by an integer that represents a maintenance set within a maintenance domain. The maintenance domain and maintenance set determine the level attribute and VLAN attribute of the message processed by the maintenance point in the service instance.

26.1.2 Various functions of CFM

The effective application of connectivity error detection is based on reasonable network deployment and configuration. Its function is implemented between the configured maintenance points, including :

- Continuous testing function (Continuity Check, CC)
- Loopback function (Loopback, LB)
- Link tracking function (Linktrace, LT)

1. Continuous testing function

The continuity detection function is used to detect the connectivity between the maintenance endpoints. Connectivity failures may be caused by device failures or configuration errors. The realization of this function is that the CCM message is periodically sent from the maintenance endpoint, which is multicast message, and the other maintenance endpoints of the same maintenance set receive the message, and the remote state is obtained. If the maintenance endpoint does not receive the CCM message from the remote maintenance endpoint during the 3.5 CCM packet transmission cycles, the link will be problematic and the log report will be output. When maintaining multiple maintenance endpoints in the domain to send CCM packets, the link detection between multipoint and multipoint is realized.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

2. Loopback function

The loopback function, similar to the ping function of the IP layer, is used to verify the connection state between the local device and the remote device. The realization function is: the maintenance of endpoint (Loopback Message, LBM sends the message to the remote maintenance loop), and according to the end can receive feedback LBR (Loopback Reply, loopback reply message) to test the link state. Both LBM and LBR are unicast messages.

3. Link tracking function

Link tracking function is used to determine the source to the target endpoint maintenance path, this is sent by the source: LTM (Linktrace Message, linktrace message) to the target endpoint maintenance, maintenance and maintenance after the endpoint LTM intermediate point received the message, will send LTR (Linktrace Reply, link tracking response message) to the source side, the source is based on the received LTR to determine the path to the target endpoint maintenance. LTM is multicast message, and LTR is unicast message.

26.2 Brief introduction of CFM configuration tasks

Before configuring the CFM function, plan the network as follows :

- The maintenance domain of the whole network is graded to determine the boundary of each level maintenance domain.
- Determine the name of each maintenance domain, and the same maintenance domain has the same name on different devices.
- According to the VLAN that needs to be monitored, the maintenance set in each maintenance domain is determined.
- Determine the name of each maintenance set, and the same maintenance set in the same maintenance domain has the same name on different devices.
- The maintenance endpoint should be planned on the boundary port of maintenance domain and maintenance set, and the maintenance intermediate point can be planned on non-boundary equipment or port.
- A list of remote maintenance endpoints to determine maintenance endpoints.

After completing the network planning, please configure the following.

Configuration task		Detailed configuration
CFM base configuration	Enable CFM function	Error! Reference source not found.
	Configuration service instance	Error! Reference source not found.
	Configuration maintenance endpoint	Error! Reference source not found.
	Configuration maintenance intermediate point	Error! Reference source not found.
Configure various functions of CFM	Configuration continuity detection function	Error! Reference source not found.
	Configuration loopback function	Error! Reference source not found.
	Configuring link tracking function	Error! Reference source not found.

Note :

The port blocked by the STP protocol cannot receive, send and respond to the CFM protocol packet; but if

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

the port is configured to be outgoing MEP, then even if the port has been blocked by the STP protocol, it will still receive and send CCM message.

Only Ethernet ports support configuring CFM functions.

26.3 CFM base configuration

26.3.1 Enable CFM function

Command	Description	CLI mode
cfm enable	Enable CFM function. Default shutdown.	Configuration mode

26.3.2 Configuration service instance

Before configuring the maintenance endpoint and maintaining the intermediate point, the service instance must be configured first. A service instance is represented by an integer that represents a maintenance set within a maintenance domain. The maintenance domain and maintenance set determine the level attribute and VLAN attribute of the message processed by the maintenance point in the service instance.

Create maintenance domains, maintenance sets and service instances in strict accordance with the following order.

Command	Description	CLI mode
cfm md <md-name> level <level-value>	Create maintenance domain. There is no maintenance domain by default.	Configuration mode
cfm ma <ma-name> md <md-name> vlan <vlan-id>	Create maintenance set. The maintenance set has not been created by default	Configuration mode
cfm service-instance <instance-id> md <md-name> ma <ma-name>	Creating service instances. The default does not create a service instance	Configuration mode

26.3.3 Configuration maintenance endpoint

The maintenance endpoint is a functional entity in the service instance, and the CFM function is mainly embodied in the operation of the maintenance endpoint. It implements the functions of CC, LB and LT, and alerts the false CCM message and cross connection. Because the maintenance endpoint is configured on the service instance, the maintenance domain level and the VLAN attribute represented by the service instance naturally become the attributes of maintaining the endpoint. After creating the maintenance endpoint, you need to configure the remote maintenance endpoint list of the specified maintenance endpoint, and the remote maintenance endpoint list is a collection of remote maintenance endpoints that need to be monitored in the same maintenance set.

Command	Description	CLI mode
cfm mep <mep-id> service- instance <instance-id> {inbound outbound}	Create maintenance endpoints. There is no maintenance endpoint on	Interface mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

	the default port.	
<pre>cfm remote-meplist <mep-list> service-instance <instance-id> mep <mep-id></pre>	A list of remote maintenance endpoints configured with specified maintenance endpoints. There is no maintenance endpoint list for the default port.	Interface mode
<pre>cfm mep service-instance <instance-id> mep <mep-id> enable</pre>	Enable endpoint maintenance. The default maintenance endpoint is closed.	Interface mode

Note :

After the endpoint is enabled, the maintenance endpoint processes the received CCM packets.

26.3.4 Configuration maintenance intermediate point

A maintenance intermediate point is a functional entity in a service instance that responds to LBM and LTM messages.

The maintenance of the middle point is the system in accordance with the rules in each port created automatically, the creation rules are as follows: if the middle point of no maintenance port, then in accordance with the level from low to high order check each maintenance set domain, as shown in Figure 1-5 and in accordance with the process to decide whether to create a maintenance (intermediate point in the same VLAN).

Figure 1-5 maintaining the creation process of the intermediate point

Please configure and maintain the creation rules of the intermediate points according to the network planning.

Command	Description	CLI mode
<pre>cfm mip-rule {explicit default} service-instance <instance-id></pre>	Creation rules for intermediate points of configuration maintenance. By default, there are no maintenance rules for creating intermediate points, and there is no creation maintenance intermediate point.	Configuration mode

Note :

After configuring the creation rules for maintaining intermediate points, any of the following conditions can trigger the creation or deletion of the maintenance intermediate point :

- Enable CFM function.
- Creating or deleting maintenance endpoints on a port.
- The VLAN property of the port changes.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

- The creation rules for maintaining intermediate points change.

26.4 Configure various functions of CFM

Before configuring the various functions of CFM, the basic configuration of CFM needs to be completed.

26.4.1 Configuration continuity detection function

By configuring the continuity detection function, the CCM messages can be sent between the maintenance endpoints to detect the connectivity status between the maintenance endpoints, so as to realize the management of link connectivity.

Command	Description	CLI mode
<code>cfm cc interval <interval-value> service-instance <instance-id></code>	The value of the time interval in the CCM message sent by the configuration maintenance endpoint. By default, the value of the time domain in the CCM message sent by the maintenance endpoint is 4.	Configuration mode
<code>cfm cc service-instance <instance-id> mep <mep-id> enable</code>	CCM message sending function that can maintain endpoint. By default, the CCM message sending function for maintaining endpoints is closed.	Interface mode

The relationship between the value of the time domain (Interval domain) in the CCM message sent by the endpoint maintenance and the CCM sending time interval and the remote MEP timeout time is shown in Table 1-1.

Table 1-1 the relationship between the time interval value and the CCM sending time interval and the MEP timeout time

Note :

- The endpoint of the CCM message must be the same at the maintenance endpoint of the same maintenance domain and maintenance set on different devices.
- If the value of the time domain of sending the CCM message to the maintenance endpoint is 3, it is suggested that more maintenance endpoints should not be configured in the same maintenance domain and maintenance set, otherwise the performance of the whole machine will be affected.

26.4.2 Configuration loopback function

By configuring loopback function, the link state can be checked so as to verify the link connectivity.

Command	Description	CLI mode
<code>cfm loopback service-instance <instance-id> mep <mep-id> { target-mep <target-mep-id> target-mac <mac-address> } [number <number>]</code>	Enable loopback function to check link status.	Privileged mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

26.4.3 Configuring link tracking function

By configuring the link tracking function, the path between the specified maintenance endpoint and the destination maintenance endpoint can be found, thus the link failure can be realized

Location. It includes the following two functions :

- Find the path from the specified maintenance endpoint to the destination maintenance endpoint: by sending the LTM message from the designated maintenance endpoint to the destination maintenance endpoint and detecting the LTR message of the response to determine the path between the devices.
- Automatic transmission link tracking message: enable this function, while maintaining at the end of 3.5 CCM packet sending period has not received the message sent to the remote maintenance of CCM endpoint, which determine the same remote maintenance error connecting terminals, will send the LTM message LTM message (target for remote maintenance endpoints, TTL field of LTM message for a maximum of 255), through the LTR message response to locate fault detection.

Command	Description	CLI mode
cfm linktrace service-instance <instance-id> mep <mep-id> {target-mep <target-mep-id> target-mac <mac-address> } [ttl <ttl-value>] [hw-only]	Find the path from the specified maintenance endpoint to the destination maintenance endpoint.	Privileged mode
cfm linktrace auto-detection [size <size-value>]	Enable automatically send link tracking message function. By default, the automatic send link tracking message function is closed.	Configuration mode

26.3 CFM display and maintenance

After completing the above configuration, executing show command in any view can display the operation of CFM after configuration, and verify the effect of configuration by checking the display information.

Command	Description	CLI mode
show cfm status	Displays the enabling state of CFM.	Privileged mode
show cfm md	Display configuration information of maintenance domain	Privileged mode
show cfm ma [[<ma-name>] md <md-name>]	Display configuration information of maintenance set	Privileged mode
show cfm service-instance [<instance-id>]	Display configuration information for service instances	Privileged mode
show cfm mp [interface <interface-name>]	Display maintenance point information	Privileged mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

show cfm mep <mep-id> service-instance <instance-id>	Displays the attributes and running information of the maintenance endpoint	Privileged mode
show cfm linktrace-reply [service-instance <instance-id> [mep <mep-id>]]	LTR message information obtained from the display maintenance endpoint	Privileged mode
show cfm remote-mep service-instance <instance-id> mep <mep-id>	Displays information about remote maintenance endpoints	Privileged mode
show cfm linktrace-reply auto-detection [size <size-value>]	Display the content of LTR message received automatically by sending LTM message	Privileged mode

26.4 Typical configuration examples

Networking requirement :

Consists of five sets of equipment network is divided into MD_A and MD_B two maintenance domain, its level were 5 and 3, port Ethernet1/0/1 to each device of the Ethernet1/0/4 are VLAN 100, and the maintenance domain maintenance serves the VLAN.

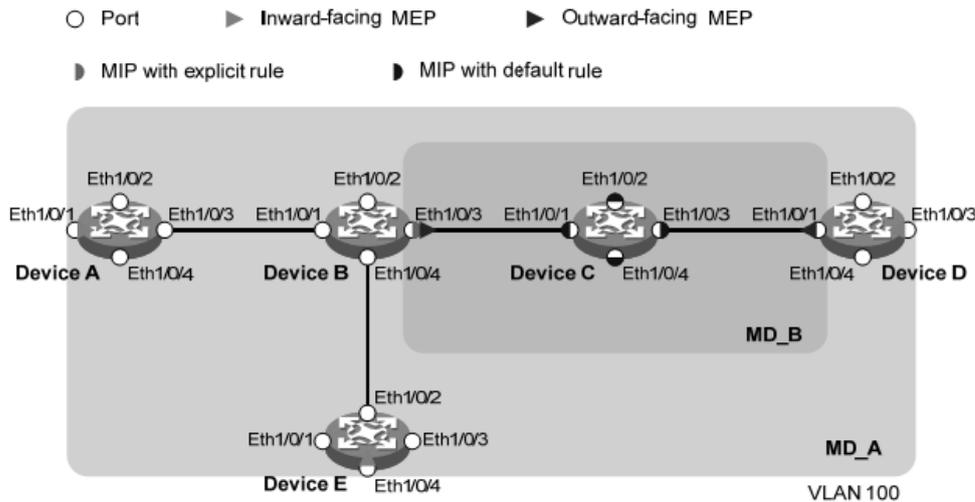
Ethernet1/0/4 Device A Ethernet1/0/1 Device, D Ethernet1/0/3 and Device E MD_A of the boundary ports, and in these ports are configured to maintain the endpoint; the boundary of the MD_B port for Device B Ethernet1/0/3 and Device D Ethernet1/0/1, and in the port configuration maintenance outgoing endpoint.

It is required to plan the MD_A maintenance intermediate point on Device B and configure it only on the port with low-level maintenance endpoints. According to this plan, the maintenance point of MD_A is configured on Device B due to the configuration of MD_B maintenance endpoint on the Device B Ethernet1/0/3, and the rule is created as Explicit rule.

It is required to plan the maintenance intermediate point of MD_B on Device C and configure it on all ports. According to this plan, the maintenance intermediate point of MD_B is configured on Device C, and its creation rule is Default rule.

By using the continuity detection function to detect all MD_A and MD_B in the maintenance of communication between endpoints, to link failures in the detection, the use of a loopback function for fault location; or to the entire network status after obtaining, using link path searching or fault location tracking function.

Network diagram :



Configuration steps :

Configuring VLAN and ports

VLAN 100 is created on each device and configured ports Ethernet1/0/1 ~ Ethernet1/0/4 belong to VLAN 100.

2) Enable CFM function

Enable CFM function on Device A.

```
[DeviceA> config t
[DeviceA] cfm enable
```

Device B~Device E

The configuration is similar to that of Device A, and the configuration process is slightly better.

3) Configuration service instance

4) # Create a maintenance domain MD_A with level 5 on Device A, create a maintenance set MA_A for VLAN 100 in MD_A, and create a service instance for MD_A and MA_A 1

```
[DeviceA] cfm md MD_A level 5
[DeviceA] cfm ma MA_A md MD_A vlan 100
[DeviceA] cfm service-instance 1 md MD_A ma MA_A
```

The configuration of Device E is similar to that of Device A, and the configuration process is slightly better.

In the Device B to create level 5 maintenance domain MD_A, created in MD_A VLAN 100 maintenance service to set MA_A, and for MD_A and MA_A to create a service instance 1; to create a level 3 maintenance domain MD_B, created in MD_B VLAN 100 maintenance service to set MA_B, and for MD_B and MA_B create a service instance 2.

```
[DeviceB] cfm md MD_A level 5
[DeviceB] cfm ma MA_A md MD_A vlan 100
[DeviceB] cfm service-instance 1 md MD_A ma MA_A
[DeviceB] cfm md MD_B level 3
[DeviceB] cfm ma MA_B md MD_B vlan 100
[DeviceB] cfm service-instance 2 md MD_B ma MA_B
```

The configuration of Device D is similar to that of Device B, and the configuration process is slightly better.

Create a maintenance domain MD_B with level 3 on Device C, create a maintenance set MA_B for VLAN 100 in MD_B, and create a service instance for MD_B and MA_B 2

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

```
[DeviceC] cfm md MD_B level 3
[DeviceC] cfm ma MA_B md MD_B vlan 100
[DeviceC] cfm service-instance 2 md MD_B ma MA_B
```

5) Configuration maintenance endpoint

Create an internal maintenance endpoint 1001 in service instance 1 on the DeviceA port Ethernet1/0/1, configure the remote maintenance endpoint list corresponding to the maintenance endpoint 1001, and then enable the endpoint 1001 to be maintained.

```
[DeviceA] interface ethernet 1/0/1
[DeviceA-Ethernet1/0/1] cfm mep 1001 service-instance 1 inbound
[DeviceA-Ethernet1/0/1] cfm remote-meplist 4002 5001 service-instance 1 mep 1001
[DeviceA-Ethernet1/0/1] cfm mep service-instance 1 mep 1001 enable
[DeviceA-Ethernet1/0/1] quit
```

On the DeviceB port Ethernet1/0/3, create the outgoing maintenance endpoint 2 in service instance 2001, configure the remote maintenance endpoint list corresponding to the maintenance endpoint 2001, and then enable the maintenance endpoint 2001.

```
[DeviceB] interface ethernet 1/0/3
[DeviceB-Ethernet1/0/3] cfm mep 2001 service-instance 2 outbound
[DeviceB-Ethernet1/0/3] cfm remote-meplist 2001 4001 service-instance 2 mep 2001
[DeviceB-Ethernet1/0/3] cfm mep service-instance 2 mep 2001 enable
[DeviceB-Ethernet1/0/3] quit
```

#On the port Ethernet1/0/1 of Device D, create the outbound maintenance endpoint 2 in service instance 4001, configure the remote maintenance endpoint list corresponding to the maintenance endpoint 4001, and then enable the maintenance endpoint 4001.

Create an internal maintenance endpoint 4002 in the service instance 1 on the port Ethernet1/0/3, and create a 4002 remote maintenance endpoint list at the same time.

```
[DeviceD] interface ethernet 1/0/1
[DeviceD-Ethernet1/0/1] cfm mep 4001 service-instance 2 outbound
[DeviceD-Ethernet1/0/1] cfm remote-meplist 2001 service-instance 2 mep 4001
[DeviceD-Ethernet1/0/1] cfm mep service-instance 2 mep 4001 enable
[DeviceD-Ethernet1/0/1] quit
[DeviceD] interface ethernet 1/0/3
[DeviceD-Ethernet1/0/3] cfm mep 4002 service-instance 1 inbound
[DeviceD-Ethernet1/0/3] cfm remote-meplist 1001 5001 service-instance 1 mep 4002
[DeviceD-Ethernet1/0/3] cfm mep service-instance 1 mep 4002 enable
[DeviceD-Ethernet1/0/3] quit
```

#On the port Ethernet1/0/4 of Device E, create and enable the internal maintenance endpoint 1 in the service instance 5001, and configure the remote maintenance endpoint list in the service instance 1.

```
[DeviceE] interface ethernet 1/0/4
[DeviceE-Ethernet1/0/4] cfm mep 5001 service-instance 1 inbound
[DeviceE-Ethernet1/0/4] cfm remote-meplist 1001 service-instance 1 mep 5001
[DeviceE-Ethernet1/0/4] cfm mep service-instance 1 mep 5001 enable
[DeviceE-Ethernet1/0/4] quit
```

6) Configuration maintenance intermediate point

Configuration rules for maintaining intermediate points are configured as Explicit rules in service instance 1 of Device B.

```
[DeviceB] cfm mip-rule explicit service-instance 1
```

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Configuration rules for maintaining intermediate points are configured as Default rules in service instance 2 of Device C.

```
[DeviceC] cfm mip-rule default service-instance 2
```

7) Configuration continuity detection function

On the port Ethernet1/0/1 of Device A, the CCM message sending function of endpoint 1001 is maintained in the enabling service instance 1.

```
[DeviceA] interface ethernet 1/0/1
```

```
[DeviceA-Ethernet1/0/1] cfm cc service-instance 1 mep 1001 enable
```

```
[DeviceA-Ethernet1/0/1] quit
```

On the port Ethernet1/0/3 of Device B, the CCM message sending function of endpoint 2001 is maintained in the enabling service instance 2.

```
[DeviceB] interface ethernet 1/0/3
```

```
[DeviceB-Ethernet1/0/3] cfm cc service-instance 2 mep 2001 enable
```

```
[DeviceB-Ethernet1/0/3] quit
```

On the port Ethernet1/0/1 of Device D, the CCM message sending function of the endpoint 4001 is maintained in the enabling service instance 2, and the CCM message sending function of the maintenance endpoint 4002 in the enabling service instance 1 is enabled on the port Ethernet1/0/3.

```
[DeviceD] interface ethernet 1/0/1
```

```
[DeviceD-Ethernet1/0/1] cfm cc service-instance 2 mep 4001 enable
```

```
[DeviceD-Ethernet1/0/1] quit
```

```
[DeviceD] interface ethernet 1/0/3
```

```
[DeviceD-Ethernet1/0/3] cfm cc service-instance 1 mep 4002 enable
```

```
[DeviceD-Ethernet1/0/3] quit
```

On the port Ethernet1/0/4 of Device E, the CCM message sending function of endpoint 5001 is maintained in the enabling service instance 1.

```
[DeviceE] interface ethernet 1/0/4
```

```
[DeviceE-Ethernet1/0/4] cfm cc service-instance 1 mep 5001 enable
```

```
[DeviceE-Ethernet1/0/4] quit
```

8) Check configuration effect

When the link fault is detected by the continuity detection function, the loopback function can be used to locate the fault. for example :

Loop back function is enabled on Device A to check the link status of endpoints 1001 to 5001 maintained in service instance 1. [DeviceA] cfm loopback service-instance 1 mep 1001 target-mep 5001

```
Loopback to 0010-FC00-6512 with the sequence number start from 43404:
```

```
Reply from 0010-FC00-6512: sequence number = 43404
```

```
Reply from 0010-FC00-6512: sequence number=43405
```

```
Reply from 0010-FC00-6512: sequence number=43406
```

```
Reply from 0010-FC00-6512: sequence number=43407
```

```
Reply from 0010-FC00-6512: sequence number=43408
```

```
Send:5 Received:5 Lost:0
```

After obtaining the whole network state through the continuity detection function, the link tracking function can be used to find the path or locate the fault. for example : # Find the path to maintain endpoints 1001 to 5001 in the service instance 1 of Device A.

```
[DeviceA] cfm linktrace service-instance 1 mep 1001 target-mep 5001
```

```
Linktrace to MEP 5001 with the sequence number 1001-43462
```

```
MAC Address      TTL      Last MAC      Relay Action
```

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

0010-FC00-6512	63	0010-FC00-6511	Hit
0010-FC00-6511	62	0010-FC00-6510	FDB

27. IPv6 basic configuration

The RT range of switches support basic IPv6 functions, including IPv6 two layer forwarding, IPv6 ND function. This chapter describes how to configure IPv6, including the following :

- IPv6 profile
- IPv6 basic configuration task profile
- Configure IPv6 basic functionality
- Configuring IPv6 neighbour discovery protocol
- IPv6 static routing configuration
- IPv6 display and maintenance

27.1 IPv6 profile

IPv6 (Internet Protocol Version 6, the Internet Protocol version 6) is the second generation standard protocol of network layer protocol, also known as IPng (IP Next Generation, the next generation of the Internet), it is IETF (Internet Engineering Task Force, Internet engineering task force) a set of standardized design, is an upgraded version of IPv4. The most significant difference between IPv6 and IPv4 is that the length of the IP address increases from 32 bits to 128 bits.

27.1.1 The characteristics of IPv6 protocol

1 Simplified message header format

By reducing or moving some fields in the IPv4 header to the extended header, the length of the IPv6 basic message header is reduced. IPv6 uses a fixed length of basic packet header, thus simplifying the forwarding equipment for IPv6 packet processing, and improving the forwarding efficiency. Although the length of the IPv6 address is four times the length of the IPv4 address, the length of the IPv6 basic message header is only 40 bytes, which is two times the length of the IPv4 header (excluding the option field).

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

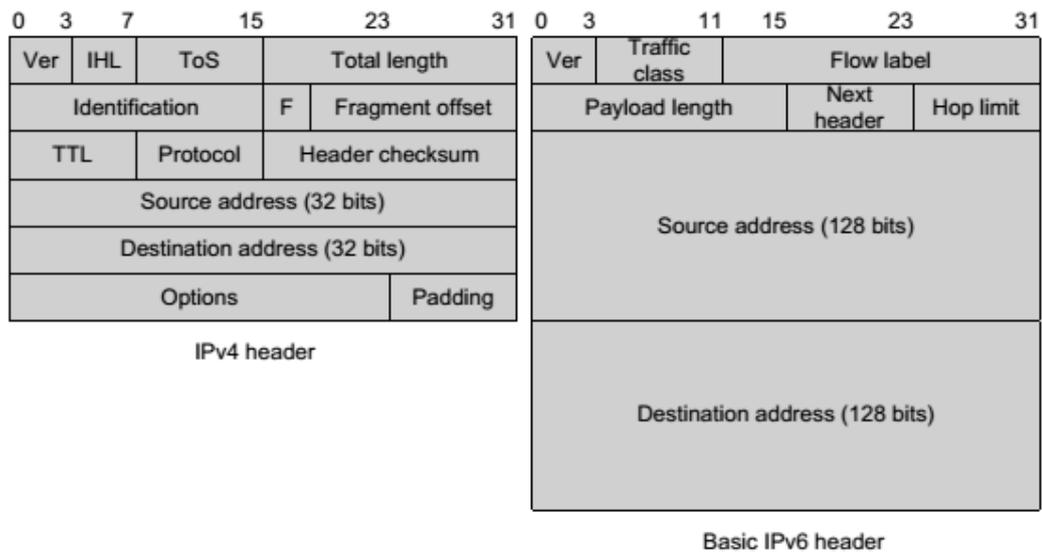


Figure 1-1 comparison of IPv4 header and IPv6 basic message header format

2 Plenty of address space

The source and destination address length of IPv6 is 128 bits (16 bytes). It can provide more than 3.4×10^{38} possible address spaces, fully meet the needs of multi-level address division, and address allocation of private networks within public networks and organizations.

3 Hierarchical address structure

The address space of IPv6 adopts hierarchical address structure, which is beneficial to fast routing lookup, and can effectively reduce the system resource occupied by IPv6 routing table by means of route aggregation.

4 Address auto configuration

In order to simplify host configuration, IPv6 supports stateful address configuration and stateless address configuration :

- 1) Stateful address configuration refers to obtaining IPv6 addresses and related information from a server (such as a DHCP server)
- 2) Stateless address configuration means that the host automatically configures the IPv6 address and related information according to its link layer address and the prefix information issued by the router. At the same time, the host can also form the link local address according to its own link layer address and default prefix (FE80:: /10) to realize the communication with other hosts on the chain.

5 Built in security

IPv6 uses IPSec as its standard extension head, providing end-to-end security features. This feature also provides a standard for solving network security problems and improves interoperability between different IPv6 applications.

6 Support QoS

The flow label (Flow Label) field of IPv6 header realizes the identification of traffic and allows the device to identify packets in a traffic and provide special processing.

7 Enhanced neighbour discovery mechanism

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

IPv6 neighbour discovery protocol by a group of ICMPv6 (Internet Control Message Protocol for IPv6 IPv6, the Internet control message protocol) message, manages the neighbour nodes (i.e., nodes on the same link) information interaction. It replaces ARP (Address Resolution Protocol, address resolution protocol), ICMPv4 router discovery and ICMPv4 redirection message, and provides a series of other functions.

8 Flexible extended headers

IPv6 cancels the option field in the IPv4 header, and introduces a variety of extended headers, which improves the processing efficiency and greatly enhances the flexibility of the IPv6 and provides a good scalability for the IP protocol. The option field in the IPv4 header is at most 40 bytes, while the size of the IPv6 extension header is limited by the size of the IPv6 message.

27.1.2 IPv6 address introduction

1. IPv6 address representation

The IPv6 address is represented as a series of 16 bit sixteen binary numbers separated by colons (:). Each IPv6 address is divided into 8 groups, each of which is represented by 16 bits in 4 sixteen decimal numbers, and groups and groups are separated by colons, such as 2001:0000:130F:0000:0000:09C0:876A:130B.

In order to simplify the representation of IPv6 address, the "0" in IPv6 address can be handled in the following way :

- 1) The preamble "0" in each group can be omitted, that is, the above address can be written as 2001:0:130F:0:0:9C0:876A:130B.
- 2) If the address contains a group of two or more consecutive 0, it can be replaced by a double colon ":" that is, the above address can be written as 2001:0:130F::9C0:876A:130B.

Note :

Only one double colon can be used in an IPv6 address ":", Otherwise, when the device transforms ":" to "0" to restore the 128 bit address, It is impossible to determine the number of "0" represented by ":".

The IPv6 address consists of two parts: address prefix and interface identifier. The address prefix is equivalent to the network number field part in the IPv4 address, and the interface identifier corresponds to the host number part in the IPv4 address.

The address prefix is represented as: IPv6 address / prefix length. Among them, the IPv6 address is any form listed previously, and the prefix length is a decimal number, which represents the leftmost number of the IPv6 address is the address prefix.

2 Address classification of IPv6

There are three types of address in IPv6: unicast address, multicast address and anycast address.

- 1) Unicast address: used to uniquely identify an interface, similar to the unicast address of IPv4. The data message sent to the unicast address will be transmitted to the interface identified by this address.
- 2) Multicast address: used to identify a set of interfaces (usually this group of interfaces belonging to different nodes), similar to the multicast address of IPv4. The data packets sent to the multicast address are transmitted to all the interfaces identified by this address.
- 3) Anycast address: used to identify a set of interfaces (usually, this group of interfaces belong to different nodes). Send any message address multicast data is transmitted a set of interfaces to the address identified

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

in the distance from the source node (recently measured according to the routing protocol using an interface).

There is no broadcast address in IPv6, and the function of broadcast address is realized by multicast address.

The IPv6 address type is specified by several preceding addresses (called the format prefix), and the corresponding relationship between the main address type and the format prefix is shown in Table 1-1.

Table 1-1 the corresponding relationship between address type and format prefix

3 Unicast address types

There are many types of IPv6 unicast addresses, including global unicast addresses, link local addresses, and site local addresses.

- 1) Global unicast address is equivalent to IPv4 public address, which is provided to network service provider. This type of address allows aggregation of routing prefixes, thus limiting the number of global routing tables.
- 2) Link local address is used for neighbour discovery protocol and communication between local upper nodes in stateless automatic configuration. Data packets that use link local address as source or destination address are not forwarded to other links.
- 3) The local address of the site is similar to the private address in IPv4. The data packets that use the local address of the site as the source or destination address are not forwarded to other sites outside the site (equivalent to a private network).
- 4) Loopback address: unicast address 0:0:0:0:0:0:1 (simplified as:: 1) is called loopback address, and cannot be assigned to any physical interface. Its function is the same as the loopback address in IPv4, that is, nodes send IPv6 messages to themselves.
- 5) Unknown address: Address::: called an unspecified address and cannot be assigned to any node. Before the node obtains the valid IPv6 address, it can fill the address in the source address field of the transmitted IPv6 message, but it cannot be used as the destination address in the IPv6 message.

4 multicast

The multicast address shown in table 1-2 is reserved for a special purpose multicast address.

Table 1-2 list of reserved IPv6 multicast addresses

In addition, there is a class of multicast address: the requested node (Solicited-Node) address. This address is mainly used to obtain link layer address of neighbour nodes on the same chain and realize duplicate address detection. Each unicast or anycast IPv6 address has a corresponding address of the requested node. Its format is :

FF02:0:0:0:1:FFXX:XXXX

Among them, FF02:0:0:0:1:FF is 104 bit fixed format; XX:XXXX is the post 24 bit of unicast or anycast IPv6 address.

5 The interface identifier of IEEE EUI-64 format

The interface identifier in the IPv6 unicast address is used to identify a unique interface on the link. At present, the IPv6 unicast address basically requires the interface identifier to be 64 bits. The interface identifier of the IEEE EUI-64 format changes from the link layer address (MAC address) of the interface. The interface identifier in the IPv6 address is 64 bits, and the MAC address is 48 bits. Therefore, it is necessary to insert the sixteen decimal number FFFE (111111111111110) at the middle position of the MAC address (starting from the twenty-fourth bit after the high position). To ensure that the interface

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

identifier obtained from the MAC address is unique, the Universal/Local (U/L) bit (starting from the high bit) is set to 1 seventh". Finally, the number of groups is used as the interface identifier of the EUI-64 format.

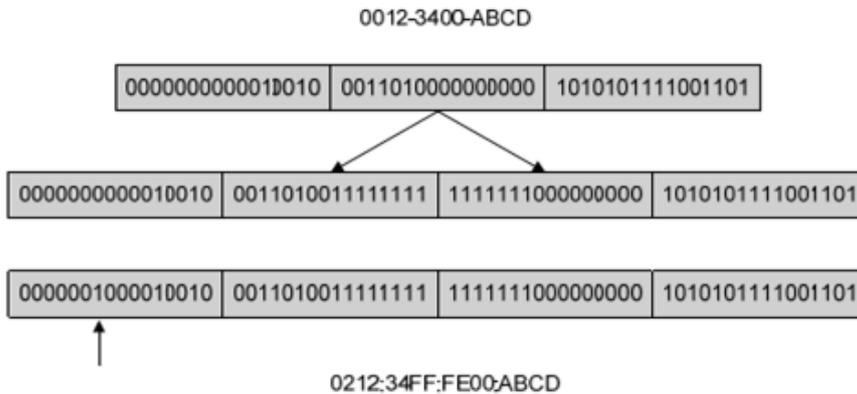


Figure 1-2 conversion process from MAC address to EUI-64 format interface identifier

27.1.3 IPv6 neighbour discovery protocol

IPv6 neighbour discovery protocol using ICMPv6 message five types, some functions to achieve the following: address resolution, verification of neighbours is reachable, duplicate address detection, router discovery / prefix discovery, address auto configuration and redirection.

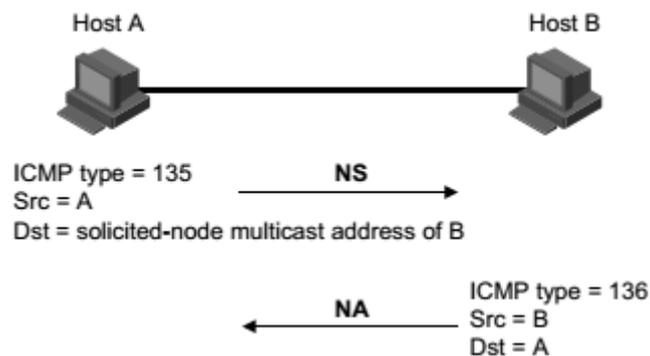
The type and role of ICMPv6 messages used by neighbour discovery protocols are shown in table 1-3.

Table 1-3 the type and role of ICMPv6 messages used in neighbour discovery protocols

The main functions of neighbour discovery protocol are as follows :

1 Address resolution

The link layer address of the neighbour node of the same chain is obtained (the same as the ARP function of IPv4), which is implemented by neighbour request message NS and neighbour notification message NA. As shown in Figure 1-3, node A is required to obtain the link layer address of node B.



Schematic diagram of address resolution in Figure 1-3

- (1) Node A sends NS messages in multicast mode. The source address of the NS message is the interface IPv6 address of the node A, and the destination address is the multicast address of the requested node of the node B. The message content contains the link layer address of the node A.
- (2) After the node B receives the NS message, it determines whether the destination address of the message is the multicast address of the requested node corresponding to its own IPv6 address. If it is, then

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

the node B can learn the link layer address of the node A and return the NA message in unicast mode, which contains its own link layer address.

(3) The node A obtains the link layer address of the node B from the received NA message.

2. Verify whether neighbours are reachable

After obtaining the link layer address of neighbour node, neighbour request message NS and neighbour notification message NA can verify whether neighbour node is reachable or not.

(1) The node sends the NS message, where the destination address is the IPv6 address of the neighbour node.

(2) If the acknowledgement message of neighbour node is received, the neighbour is reachable; otherwise, the neighbour is unreachable.

3. Duplicate address detection

When a node acquires an IPv6 address, it is necessary to use the repeated address detection function to determine whether the address has been used by other nodes (similar to the free ARP function of IPv4).

Duplicate address detection can be implemented by NS and NA, as shown in Figure 1-4.

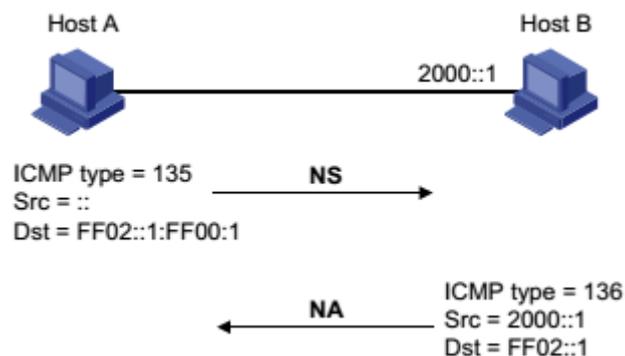


Fig. 1-4 duplicate address detection schematic diagram

(1) The node A sends the NS message, and the source address of the NS message is an unspecified address: the destination address is the multicast address of the requested node corresponding to the IPv6 address to be detected, and the message content contains the IPv6 address to be detected.

(2) If the node B has already used this IPv6 address, the NA message will be returned. It contains its own IPv6 address.

(3) The node A receives the NA message from the node B, and knows that the IPv6 address is already in use. Otherwise, the address is not used, and the node A can use the IPv6 address.

4. Router discovery / prefix discovery and address auto configuration

Router discovery / prefix discovery is that the node obtains the prefix of neighbour router and its network from the received RA message, and other configuration parameters.

Address stateless automatic configuration refers to the node to discover the acquired information according to the router discovery / prefix, and automatically configure the IPv6 address. The router discovery / prefix discovery is implemented through the router request message RS and the router notification message RA, and the specific process is as follows :

(1) When the node starts, it sends a request to the router through the RS message, requesting the prefix and other configuration information for the configuration of the node.

(2) The router returns the RA message, including prefix information options (the router also periodically releases RA messages).

(3) The node automatically configures the IPv6 address and other information of the interface by using the address prefix and other configuration parameters in the RA message returned by the router.

- Prefix information options include not only the address prefix information, but also the prefix lifetime (preferred lifetime) and valid (life cycle). When a node receives a periodically transmitted RA message, the prefix's preferred lifetime and valid lifetime are updated according to the message.
- In the effective life period, the automatically generated address can be used normally; after the expiration of the valid life period, the address automatically generated will be deleted.

5. Redirection

When the host is started, there may be only one default route to the default gateway in its routing table. When a certain condition is satisfied, the default gateway will send a redirect message to the source host ICMPv6, notify the host select Send follow-up message better next hop (IPv4 and ICMP redirect messages the same function).

- The ICMPv6 redirection message is sent to the host when the following conditions are met.
- The interface of receiving and forwarding data packets is the same interface.
- The selected route itself has not been created or modified by the ICMPv6 redirection message.
- The selected route is not a default route.
- The forwarding IPv6 data packet does not contain a route extension header.

27.1.4 IPv6 PMTU discovery

The links that are transmitted from the source to the destination may have different MTU links. In IPv6, when the length of message is greater than MTU of the link, the fragment of the message will be carried out at the source end, thus reducing the processing pressure of the intermediate forwarding device and rationally utilizing the network resources.

The purpose of the PMTU (Path MTU, path MTU) discovery mechanism is to find the smallest MTU on the path from the source end to the destination. The working process of PMTU is shown in Figure 1-5.

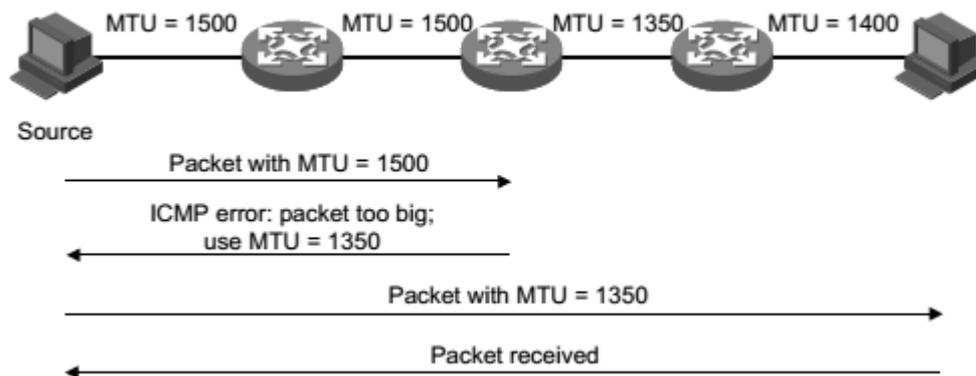


Figure 1-5 PMTU discovery work process

- (1) The source host uses its own MTU to segment the message, and then sends the message to the destination host.
- (2) The intermediate forwarding device receives the message forwarding, if packet forwarding interface support MTU value is less than the length of message packets are discarded, and the source to return a ICMPv6 error message, including forwarding fails MTU interface.
- (3) When the source host receives the error message, it will fragment and send the message by using the MTU carried by the message.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

(4) This is repeated until the destination host receives this message, thus determining the minimum MTU of the message from the source end to the destination path.

27.1.5 Protocol specification

The protocol specification related to the IPv6 foundation is available :

- RFC 1881 : IPv6 Address Allocation Management
- RFC 1887 : An Architecture for IPv6 Unicast Address Allocation
- RFC 1981 : Path MTU Discovery for IP version 6
- RFC 2375 : IPv6 Multicast Address Assignments
- RFC 2460 : Internet Protocol, Version 6 (IPv6) Specification.
- RFC 2461 : Neighbor Discovery for IP Version 6 (IPv6)
- RFC 2462 : IPv6 Stateless Address Autoconfiguration
- RFC 2463 : Internet Control Message Protocol (ICMPv6)for the Internet Protocol Version 6 (IPv6) Specification
- RFC 2464 : Transmission of IPv6 Packets over Ethernet Networks
- RFC 2526 : Reserved IPv6 Subnet Anycast Addresses
- RFC 3307 : Allocation Guidelines for IPv6 Multicast Addresses
- RFC 3513 : Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3596 : DNS Extensions to Support IP Version 6

27.2 IPv6 basic configuration task profile

Configuring the basic functions of IPv6

Configuring IPv6 neighbour discovery protocol

Configuring PMTU discovery

Configuring ICMPv6 message sending

27.3 Configure IPv6 basic functionality

27.3.1 Configuring IPv6 unicast address

IPv6 global unicast addresses are manually assigned.

IPv6 link local address is obtained in two ways :

- Automatic generation: when the VLAN port UP, the device automatically generates the link local address for the interface according to the link local address prefix (FE80::/10) and the link layer address of the interface ;
- Manually assigned: user manually configured IPv6 link local address.

Command	Description	CLI mode
ipv6 address <ipv6-address>/<prefix-length>	Manually specify the IPv6 address. By default, the local address of the link is automatically generated according to the VLAN interface MAC address under	Configuration mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

	the three layer interface.	
--	----------------------------	--

27.4 Configuring IPv6 neighbour discovery protocol

27.4.1 Configuring the parameters of the RA message

The user can configure the interface whether to send RA messages and send RA messages according to the actual situation and configure the related parameters in the RA message to notify the host. When the host receives the RA message, we can use these parameters to do the corresponding operation. The parameters and meanings of configurable RA messages are shown in table 1-4.

Table 1-4 parameters and descriptions in RA message

Parameter	Description
Cur Hop Limit	When the host sends the IPv6 message, it will fill the Hop Limit field in the IPv6 header with the parameter value. At the same time, the parameter value is also used as the Hop Limit field value in the device reply message.
Prefix Information	When the host on the same link receives the prefix information of the device, it can perform stateless automatic configuration and other operations.
M flag	To determine whether the host uses stateful automatic configuration to obtain the IPv6 address. If this flag is set to 1, the host will have state through automatic configuration (e.g. DHCP server) to obtain IPv6 address; otherwise, the stateless auto configuration to obtain IPv6 address, IPv6 address is generated according to their link layer address and router prefix information release.
O flag	To determine whether the host uses stateful automatic configuration to obtain additional information other than the IPv6 address. If you set the other configuration flag is 1, the host will have state through automatic configuration (e.g. DHCP server) to obtain information in addition to other IPv6 address; otherwise, the stateless auto configuration for additional information.
Router Lifetime	The time used to set the router that releases the RA message as the default router for the host. According to the router survival time parameter value in the received RA message, the host can determine whether or not the router that publishes the RA message will be the default router.
Retrans Timer	When the device sends NS messages, the NS message is re sent if the response is not received within the specified time interval.
Reachable Time	When the neighbor unreachability detection to verify that a neighbor, in time up to set, equipment up to that neighbor; exceed the time set, if you need to send messages to neighbours, neighbours will re confirm whether can reach.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Link MTU	The MTU option is used in the RA message to ensure that all nodes on the chain use the same MTU value, which is mainly used in the case that nodes may not know the link MTU. Other Neighbor Discovery messages must be silent and ignore this option.
----------	--

Configure hop limit

Command : **ipv6 nd cur-hop-limit** *value*

View mode : VLAN interface mode

Default configuration: by default, the number of hops issued by the router is limited to 64 hops

Eliminating the inhibition of RA message publishing

Command : **ipv6 nd send-ra**

View mode : VLAN interface mode

Default configuration: suppresses publication of RA messages by default

Configuring the maximum time interval and minimum time interval for RA message publishing

Command : **ipv6 nd max-ra-interval** *value*

View mode : VLAN interface mode

Default configuration: by default, the maximum time interval for RA message release is 600 seconds

Command : **ipv6 nd min-ra-interval** *value*

View mode : VLAN interface mode

Default configuration: by default, the minimum time interval for issuing RA messages is 198 seconds

Note :

- When a RA message is periodically published, the interval between the two adjacent times is randomly selected between the maximum time interval and the minimum time interval as the time interval for periodically issuing RA messages.
- The minimum time interval should be less than 0.75 times the maximum time interval.

Configuring prefix information in RA messages

Command : **ipv6 nd prefix** X:X::X:X/M (*valid-lifetime preferred-lifetime (off-link | no-autoconfig)*)

View mode : VLAN interface mode

Default configuration: by default, the prefix information in the RA message is not configured. The IPv6 address of the RA message will be used as the prefix information in the RA message.

Setting the managed address configuration flag bit

Command : **ipv6 nd managed-config-flag**

View mode : VLAN interface mode

Default configuration: by default, the managed address flag is 0, that is, the host automatically obtains the IPv6 address by stateless configuration.

Setting other configuration flag bits

Command : **ipv6 nd other-config-flag**

View mode : VLAN interface mode

Default configuration: by default, other configuration flags are 0, that is, the host automatically obtains other information by stateless configuration.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Configuring router lifetime in RA messages

Command : **ipv6 nd ra-lifetime** *value*

View mode : VLAN interface mode

Default configuration: by default, the lifetime of the router in the RA message is 1800 seconds.

Configuring a neighbour request message retransmission interval

Command : **ipv6 nd base retrans-timer** *value*

View mode : Configuration mode

Default configuration: by default, the time interval for sending NS messages by the interface is 1000 milliseconds.

Configuring retransmission interval of routers in RA messages

Command : **ipv6 nd retrans-timer** *value*

View mode : VLAN interface mode

Default configuration: by default, the value of the Retrans Timer field in the RA message issued by the interface is 0

Configuring the time to keep neighbors reachable

Command : **ipv6 nd base reachable-time** *value*

View mode : Configuration mode

Default configuration: by default, the interface maintains the reachable state of the neighbors for 30000 milliseconds.

Configuring the time to keep neighbors reachable

Command : **ipv6 nd reachable-time** *value*

View mode : VLAN interface mode

Default configuration: by default, the value of the Reachable Timer field in the RA message issued by the interface is 0.

Configuring link MTU size

Command : **ipv6 nd link-mtu** *value*

View mode : VLAN interface mode

Default configuration: by default, the value of the link MTU field in the RA message issued by the interface is 0.

When the source host sends the message from the interface, it will compare the MTU and Link MTU of the interface. If the message length is greater than two, the minimum value is used to segment the message.

27.4.2 Setting number to neighbour requests

Interface IPv6 address after the message is sent to the neighbour request duplicate address detection, if within a specified period of time (by IPv6 and retrans-timer configuration command) did not receive a response, then continue to send the request information, when sending the number reached number set, has not yet received a response, the address available.

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch

Command	Description	CLI mode
ipv6 nd dad attempts <value>	By default, the number of neighbour requests sent by repeated address detection is 1, and when the value is 0, it indicates the forbidden duplicate address detection.	Configuration mode

27.5 IPv6 static routing configuration

Command	Description	CLI mode
ipv6 route <X:X::X:X/M> (<X:X::X:X> <ifName>) <distance>	Configuring IPv6 static routing.	Configuration mode

27.6 IPv6 display and maintenance

After completing the above configuration, executing the show command in the privileged view can display the operation of the IPv6 after configuration, and verify the configuration effect by checking the display information.

Command	Description	CLI mode
show ipv6 ndp nc	Display neighbour information.	Privileged mode
show ipv6 interface (<ifName>) brief	Display the IPv6 information that can configure the IPv6 address interface	Privileged mode
show ipv6 route (database)	Display IPv6 routing	Privileged mode

	Document Title	Related to
	RT Series Layer 3 Industrial Switch Command Line Interface Manual	RT L3 Series Switch