SICOM Series Industrial Ethernet Switch

Command Line Configuration Manual

Publisher: KYLAND Technology CO., LTD.
Address: Chongxin Creative Building, Shixing East Road 18#, Shijingshan District, Beijing, China
Website: http://www.kyland.cn
Postcode: 100041
Tel: (+8610)88796676
FAX: (+8610)88796678
E-mail: sales@kyland.cn
Version: V1, May. 2009
No.:27030042-10

CONTENTS

Chapter 1 CLI Command Introduction

This chapter mainly introduces how to configure SICOM series Industrial Ethernet Switch by CLI command and the instructions of command set.

1.1 Login the Switch

1.1.1 Command Line

User can log in command line via serial port or Telnet.

To log in via serial port, connecting serial ports between PC and switch is required. See more details of serial port configuration in Chapter 1.4

Start up the switch, select the serial port, and type the key “Enter”; you can see the prompt in the serial port. At default state, the prompt is “kyland>”.

 **Note**:
If you want to keep the change after the switch reboot, please use the “save” command after your configuration. See more details in Common Command Description。

1.1.2 Command Grammar

To use the command line interface (CLI) as the following steps:

1. Type “Enable” after you enter CLI and command prompt pop up, enter command line mode, there will be a command prompt “kyland#”.
2. Type the command name. If the command doesn’t contain any parameter that need to be input by user, skip to step three. If the command contains parameters that require user to input, please continue the following steps: If the command need a parameter, please input the parameter, and key words might be needed when you typing the parameter.
   Command parameters specify the type of parameters. The types of parameter might be values in a certain range, string or IP address. The key word is the object that the command work to. If the command requires more than one parameters, please type the key words and parameters one by one with the command instructions until <cr> appears.
3. After input the full command, type the key “Enter”

1.1.3 Grammar Help

The grammar help is integrated in command line interface. If not sure about the grammar, please type the first part of command you know, followed with "?" or type the key "Space" and " ?" The command line will automatically display the possible command list of the rest part. Users can choose the right one and finish the rest part until the command line shows "<cr>". Then type the key "Enter" to finish.

1.1.4 Complete Command by Grammar Help

When you type key of "Tab", management software can complete command. When you enter a part of command and type key of "Tab", the possible commands will be listed if the matching commands are more than one; if only one matching command. the command line will automatically complete the rest part of the command and move the cursor to the end
EX:

1. Type the command:
   `KYLAND#show`
2. Type key of "Space" and "Tab", you can see:

broadcaontrol	Broadcontrol
clock	Display the system clock
config	System configuration
fdb	Fdb
history	Display the session command history
igmp	Igmp snooping protocol
interface	Interface status and configuration
manager	Management station status
memory	System memory statistics information
dt-ring	DT-Ring protocol
rstp	Rapid spanning tree protocol
running-config	Current operating configuration
snmp	SNMP status
switch	Show switch status
telnet	Telnet configure information
timer	show timer message
trunk	Show vlan information
uptime	Display the system uptime
version	System hardware and software status
vlan	Show vlan information

Above information are the possible commands after the "show" command. User can select the correct command. If the command is long, user can also type the key "Tab" to finish the command.

1.1.5 Symbol in Command

In the management software, only one symbol "< >" is supported. It means a parameter is required in this part of the command.
For example: dt-ring new <1-32> domain <1-32> master

1.1.6 Types of Command Parameters

Normally the command in an angle bracket "< >" is command parameters. There are four types of command parameters in this series switches.

A range of number:
When the numbers in "< >" is connected by a short line, which means the parameter is a number between this range.
For example: <1-255> means user can input any number in this range (more than or equal 1, less than or equal 255), such as "2".

IP address:
The "A.B.C.D" in angle bracket means the parameter is IP address. User must input a valid IP address.
For example: 192.168.0.1

String:
If the content in "< >" is not above two forms, a string or a hexadecimal number is required. Users can input a "?" at this place to know the detail parameter description. For example: <macaddr> means the required parameter is a hex MAC address, Such as 005023344325 is a Mac address. And <name> requires a string to be the subject's name.

1.1.7 Command Abbreviation

Command abbreviation is that users only input the first several letters of the command word or the key word. As long as these letters don't cause ambiguity, switch is able to recognize that command, and user can type the key "Enter" to run that command. But if the required parameter is VLAN's name, etc, it need to be fully input. In the below example, the VLAN's name is "market".
Example, adding port 1 to "market" with untagged form:
In VLAN, typing the following command:

```
KYLAND>
KYLAND>enable
KYLAND#config terminal
KYLAND(config)#
```

```
KYLAND(config)#vlan 2
KYLAND(config-vlan2)#description market
KYLAND(config-vlan2)#add port 1 untag priority 0
```

This command line can be abbreviated to:

```
KYLAND>
KYLAND>ena
KYLAND#con ter
KYLAND(config)#
KYLAND(config)#vlan 2
KYLAND(config-vlan2)#desc market
KYLAND(config-vlan2)#add port 1 un pr 0
```

Above two kinds of commands have same functions.

Note:

When using command abbreviation function, user must input enough letters to avoid ambiguity.

1.1.8 History Command

The software can keep the record of the latest 10 history commands user used.
To show history command list, use the following command:

```
Kyland#show history
```

1.2 Common Commands

This part mainly describes several common commands, and some specially used commands will be discussed in other chapters.

1.2.1 Mode Configuration

Command lines provide two types of modes: one is Read Only mode, the other is Configuration Mode. At Read Only mode, user can only read a part of system configuration information. At Configuration Mode, user can read and configure all system configuration information. At configuration mode, you can use some commands to enter certain protocols' independent configuration mode, such as: "KYLAND#" is interface configuration mode.
At Read Only mode, the prompt ends with ">" i.e. "KYLAND>"
At Configuring mode, the prompt ends with "#" i.e. "KYLAND#"

- **Enable configuration mode**
  Enable configuration mode at Read Only mode, using this command:
  `KYLAND>enable`
  Type the key "Enter", and password is required:
  `Password:`
  With correct password, enter the Configuration Mode
- **Disable Configuration Mode, using the following command:**
  `KYLAND#disable`

1.2.2 Password Configuration

SICOM series industrial Ethernet switch support the password checking function for command line and Telnet

- **Password configuration**
  `KYLAND(config)# enable password <1-20>`

1.2.3 Showing version

- To show software version, using the command:

```
KYLAND#show version
Industry Ethernet Switch Software
Version: 1.2.3
Compiled time: 2009-01-13  18:14

BootRomVersion: 1.0.20
Compiled time: 2008-05-15  14:18

HardWare:SICOM-3024
```

1.2.4 Showing device running function

At Configuration Mode, to display system running function, using the command:
`KYLAND#show running-config`

1.2.5 Showing device configuration information

At configuration mode, using below command to see the system configuration
`KYLAND#show config`

1.2.6 Save configuration and restore default configuration

- **To save current configurations**

```
KYLAND# save
```

- **To restore default configuration**

```
KYLAND# load default
```

 **Note:**

If users want to reset switch's start configuration information, use this command to delete former configuration.

1.3 Switch Management Methods

SICOM series industrial Ethernet switches are mainly managed by the following methods:

- Connecting a terminal (or terminal emulation software) with switch's Console port to access switch's CLI
- Using Telnet to manage switch
- Using SNMP to manage switch
- Using WEB to manage switch

1.4 Console Management

Using Console RJ45 serial port at the front panel of switch to connect with switch's built-in CLI interface. For SICOM series switch, the configuration of Console port is as below:

Baud Rate	9600
Bit	8
Parity	None
Stop Bit	1
Flow Control	None

When connecting switch with Console port, VT100 terminal emulation is recommended. Configuration steps: at hyper terminal interface, open "file" menu, select "attribute", and click "configure" at the window, then select VT100 in the list.

Chapter 2 Port Configuration

2.1 Port Configuration Overview

The port configuration of SICOM series Industrial Ethernet Switch contains port-related configuration and the configuration of port-based functions. In the port configuration commands, user can configure the functions of auto-negotiation, port enable, duplex, flow control, mirroring, port rate, ACL, etc.

Auto negotiation:
SICOM series Industrial Ethernet Switch supports the auto-negotiation function for ports; ports with auto-negotiation function can automatically negotiate the communication mode (duplex state, communication speed, etc) according to the port state in the other end. This function only work to 10/100M copper port and 1000M fiber or copper port; 100Base-FX ports do not support auto negotiation and their fixed rate is 100M and the duplex mode is full duplex.

Flow control:
SICOM series Industrial Ethernet Switch supports 802.3-based port flow control. At full duplex mode, if the port receives data beyond its limit, the port would transmit flow control frames so as to prevent the packet loss caused by the rate limit. At the half duplex mode, if the port receives data beyond its limit, the port would generate the back pressure half duplex collision detection frames to reduce the transmitting data from the sending end.

Mirroring
The mirroring of SICOM series Industrial Ethernet Switch is port-based mirroring. Its function is to copy the data at the mirroring port to mirrored port(s) with the purpose of monitoring mirroring ports, and so on.

ACL:
SICOM series Industrial Ethernet Switch supports Port + MAC-based ACL function with “accept” and “reject” two modes which can basically guarantee the port security. At the “accept” mode, only the configured MAC address can pass through switch. At the “reject” mode, configured MAC address is not allowed to pass through the switch.

2.2 Configure Port Functions

2.2.1 Enter port configuration menu

- Enter port configuration, using the below command:
  `KYLAND(config)# int eth <1,24>`
  Take port 1 as example in the following examples.

2.2.2 Enable/disable port

- **Enable port**
  `KYLAND(config-if-eth1)# no lock`

- **Disable port**
  `KYLAND(config-if-eth1)# lock`

2.2.3 Auto- negotiation configuration

- **Enable auto-negotiation**
  `KYLAND(config-if-eth1)# auto-negotiation`

- **Disable auto-negotiation**
  `KYLAND(config-if-eth1)# no auto-negotiation`

2.2.4 Port rate configuration

Port rate configuration (10M/100M/1000M) makes ports work under the fixed rate.

- **10M port rate configuration:**
  `KYLAND(config-if-eth1)# speed 10m`

- **100M port rate configuration:**
  `KYLAND(config-if-eth1)# speed 100m`

- **1000M port rate configuration:**
  `KYLAND(config-if-eth1)# speed 1000m`

Note:
Do not set 1000M speed to the 10M/100M ports.

2.2.5 Port duplex configuration

- **Full duplex configuration:**
  ```
  KYLAND(config-if-eth1)# duplex
  ```

- **Half duplex configuration:**
  ```
  KYLAND(config-if-eth1)# no duplex
  ```

2.2.6 Port flow control configuration

- **Enable the flow control**
  ```
  KYLAND(config-if-eth1)# flow-control
  ```

- **Disable the flow control:**
  ```
  KYLAND(config-if-eth1)# no flow-control
  ```

2.3 Port mirroring configuration

2.3.1 Enable/disable port mirroring

- **Enable port mirroring**
  ```
  KYLAND(config-if-eth1)# mirror enable
  ```
  Enable the port mirroring and set this port as mirroring port

- **Disable port mirroring**
  ```
  KYLAND(config-if-eth1)# mirror disable
  ```

2.3.2 Mirroring port configuration

- **Adding egress mirroring to mirrored ports**
  ```
  KYLAND(config-if-eth1)# mirror add egress port 2
  ```

- **Adding ingress mirroring to mirrored ports**
  ```
  KYLAND(config-if-eth1)# mirror add ingress port 2
  ```

- **Delete egress mirroring from mirrored ports**
  ```
  KYLAND(config-if-eth1)# mirror delete egress port 2
  ```

- **Delete ingress mirroring from mirrored ports**

```
KYLAND(config-if-eth1)# mirror delete ingress port 2
```

2.4 ACL configuration

- **Setting "accept" mode for port ACL**

```
KYLAND(config-if-eth1)# acl mode accept
```

- **Setting "reject" mode for port ACL**

```
KYLAND(config-if-eth1)# acl mode reject
```

- **Setting none for port ACL**

```
KYLAND(config-if-eth1)# acl mode none
```

- **Adding MAC address for port**

```
KYLAND(config-if-eth1)# acl mac add HH:HH:HH:HH:HH:HH
```

- **Delete MAC address for port**

```
KYLAND(config-if-eth1)# acl mac delete HH:HH:HH:HH:HH:HH
```

2.5 Configure query function

2.5.1 ACL configuration query

- **Query of ACL port mode configuration**

```
KYLAND(config-if-eth1)# show acl mode
```

- **Query of ACL port MAC address configuration**

```
KYLAND(config-if-eth1)# show acl mac
```

2.5.2 Port statistics query

```
KYLAND(config-if-eth1)# show stats
```

2.5.3 Port mirroring query

```
KYLAND# show mirror
```

2.5.4 Port configuration query

```
KYLAND# show int eth <1, 24>
```

The parameter <1, 24>: Port ID.

Chapter 3 Port speed limitation

3.1 Overview of port speed limitation function

SICOM series Industrial Ethernet Switch supports port transmitting rate limitation, services limitation and broadcast limitation, which all belong to the traffic limitation function.

Support max 26 ports' speed limitation at the same time.
Support user typing specific limit value
Speed limitation range
The minimum limitation value: 64Kbps;
the max limitation value: 100*100Kbps (100M port)
Speed limitation accuracy
Different accuracy in different speed limitation range, see more detail in the below table:

Users' setting range	Step value	Error range	Example
64K~1.792M	64K	Between -32K~32K	Input value: 65K Actual value:64K Input value:127K Actual value: 128K
2M~100M	1M	Between -0.5M~0.5M	Input value:2.3M Actual value；2M Input value: 2.8M Actual value:3M

Control Interface: support the speed limitation control by CONSOLE port, Telnet and WEB.
Limitation mode:
Speed limitation is divided into two groups, group 1 and group 2. The message firstly access group 1 which is specialized in the limitation of service messages and is fixed to all ports. Group 2 is used to do limitation to other messages and it is also fixed to all ports.
Default configuration:
Service messages: unicast, multicast
Broadcast messages: broadcast, reserved multicast, unknown unicast, unknown multicast.
Support separated limitation of service messages and broadcast messages
Support overall speed limitation for transmitting messages.
Support showing all ports' speed limitation configuration
Support showing each port's speed limitation configuration

3.2 Setting port rate mask (types of message)

Ingress direction

- **Configure the types of message speed limitation**

  `SWITCH(config)#port-rate ingress [service|broadcast] [add|delete] <0,4>`

  The parameter <0, 4> 0: unicast, 1: multicast, 2: broadcast, 3: reserved multicast, 4: Destination Lookup Fail (DLF) (including unknown unicast, unknown multicast)

- **Showing the types of message speed limitation in ingress direction**

  `SWITCH(config)#port-rate ingress show`

- **Showing overall port speed limitation configuration**

  `SWITCH#show port-rate`

3.3 Port rate configuration

Ingress direction

- **Service/broadcast limitation configuration**

  `SWITCH(config-if-eth x)#port-rate ingress [service|broadcast] rate <64-1000000>`

  The parameter <64-1000000> is the parameter in speed limitation range, x means the ID of speed limitation port

- **Disable service/broadcast limitation**

  `SWITCH(config-if-eth x)#port-rate ingress [service|broadcast] disable`

Egress direction

- **Port transmitting speed limitation configuration**

  `SWITCH(config-if-eth x)#port-rate egress rate <64-1000000>`

  The parameter <64-1000000> is the parameter in speed limitation range, x means ID of speed limitation port

- **Disable port transmitting speed limitation**

  `SWITCH(config-if-eth x)#port-rate egress disable`

  The parameter x means ID of speed limitation port

3.4 Showing a port's speed limitation

```
SWITCH(config-if-eth x)#show port-rate
```

The parameter x means the ID of speed limitation port

3.5 Showing overall port speed limitation configuration

```
SWITCH#show port-rate
```

Chapter 4 VLAN Function Configuration

4.1 VLAN function introduction

VLAN (Virtual Local Area Network) is a broadcast domain formed by a group of terminal workstations. The hosts (ports of Industrial Ethernet switch) in the same VLAN are able to communicate with each other and create a logical working group without considering the specific wiring. Dividing the corporate network into VLAN segments enhance network management and network security and control unnecessary data broadcasts.

In a shared network, a physical segment is a broadcast domain, but in a switching network, broadcast domain can be a virtual network segment formed by a group of MAC addresses. In this way, the division of working groups breaks down the geographical location restriction in the shared network and is completely divided by management functions. This grouping mode is based on the working flow greatly improve the network planning and restructuring management functions.

The workstations in a same VLAN, whatever they are connected to any switch, the communication between them is like in standalone hubs. Broadcasts in a VLAN can only be received by the members of this VLAN and would never be transmitted to other VLAN. This function greatly controls the broadcast storm. Meanwhile, different VLANs cannot do communication with each other without router, which enhance the network security in different company departments. Network administrators can wholly manage the information sharing in different company departments by configuring routers in different VLANs. Switch divides VLAN by MAC address of users' workstations, so user can freely move to work in corporate network. Wherever they get into the switching network, they can communicate with other users in VLAN freely.

VLAN might be formed by mixed network equipments, such as 10M Ethernet, 100M Ethernet, token ring, FDDI, CDDI, etc. and might be workstation, server, hub, etc.

VLAN's management need complex specialized software which achieve the network VLAN division, monitoring, etc functions and other expanded management functions by comprehensive management of users, MAC address, switch port number, VLAN number, etc. The most common used VLAN division method is based on MAC address. Some other switch manufacturers provide more VLAN division methods: MAC address, protocol address, switches port, network application type, and user rights.

When selecting switch, user should pay much attention to the VLAN function and choose the satisfactory and easy managed switch according to own requirements. At the same time, users should note that switch VLANs from different manufacturers is mostly not compatible at present.

4.2 VLAN function configuration

4.2.1 VLAN port configuration

VLAN port has two transmitting modes: drop and forward

- **Setting drop mode for VLAN port**

```
KYLAND(config)#vlan vlanmode drop
```

- **Setting forward mode for VLAN port**

```
KYLAND(config)#vlan vlanmode forward
```

- **Configure VLAN port by command line**

```
KYLAND(config)#vlan 2
```

- **Enter the port configuration menu, take VLAN 2 port as example,**

```
KYLAND(config-vlan2)#
```

4.2.2 Adding VLAN port

Each added port has two attributes: tag and untag

- **Adding port 2 with tag attribute into VLAN port**

```
KYLAND(config-vlan2)#add port 2 tag
```

- **Untag attribute has 7 priorities from 0 to 7, firstly adding port 3 with priority 5.**

```
KYLAND(config-vlan2)#add port 3 untag priority 5
```

4.2.3 Delete port from VLAN

- **Delete the port which must have been added into VLAN, delete port 3**

```
KYLAND(config-vlan2)#delete port 3
```

4.2.4 Adding the name of VLAN port

- **Change the name of VLAN into KYLAND**

```
KYLAND(config-vlan2)#description kyland
```

4.2.5 Back to the upper list

```
KYLAND(config-vlan2)#exit
```

4.2.6 Back to the main menu

```
KYLAND(config-vlan2)#end
```

4.3 PVLAN function configuration

4.3.1 Adding PVLAN

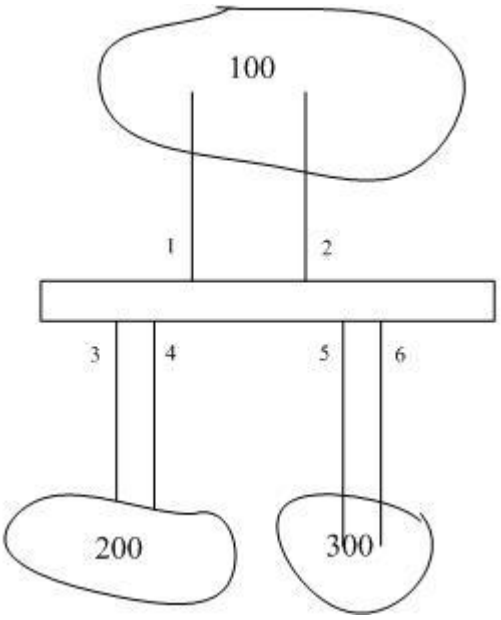
```
#SWITCH(config)#pvlan add <0,4093>
```
Note: adding the specified VLAN to PVLAN

4.3.2 Delete PVLAN

```
#SWITCH(config)#pvlan delete <0,4093>
```
Note: delete the specified VLAN from PVLAN

4.3.3 PVLAN configuration example

Configuration requirements:
Configuration topology is as follows:



Requirements:

- Port domain 100 can communicate with port domain 200
- Port domain 100 can communicate with port domain 300
- Port domain 200 cannot communicate with port domain 300

In order to get the functions described above, firstly configure port VLAN domain 100

1. VLAN configuration for port domain 100

- Create VLAN 100

```
#kyland(config)#vlan 100
```

- Adding Untag port

```
#kyland(config-vlan-100)#add port 1 untag priority 1
#kyland(config-vlan-100)#add port 2 untag priority 1
```

- Adding Tag port

```
#kyland(config-vlan-100)#add port 3 tag
#kyland(config-vlan-100)#add port 4 tag
#kyland(config-vlan-100)#add port 5 tag
#kyland(config-vlan-100)#add port 6 tag
```

2. VLAN configuration for port domain 200

- Create VLAN 200

```
#kyland(config)#vlan 200
```

- Adding Untag port

```
#kyland(config-vlan-200)#add port 3 untag priority 1
#kyland(config-vlan-200)#add port 4 untag priority 1
```

- Adding Tag port

```
#kyland(config-vlan-200)#add port 1 tag
#kyland(config-vlan-200)#add port 2 tag
```

3. VLAN configuration for port domain 300

- Create VLAN 300

```
#kyland(config)#vlan 300
```

- Adding Untag port

```
#kyland(config-vlan-300)#add port 5 untag priority 1
#kyland(config-vlan-300)#add port 6 untag priority 1
```

- Adding Tag port

```
#kyland(config-vlan-300)#add port 1 tag
#kyland(config-vlan-300)#add port 2 tag
```

- Adding into PVLAN

```
#kyland(config)#pvlan add 100
#kyland(config)#pvlan add 200
#kyland(config)#pvlan add 300
```

PVLAN configuration finishes.

Chapter 5 TRUNK function configuration

5.1 Brief introduction of TRUNK function

Port Trunking is to treat a number of physical ports as a logical transmitting port to share service flow and have the link backup function. SICOM series industrial Ethernet Switch support two Trunk groups and each of them support 4 ports' trunking.

Note:
In order to guarantee the normal working of Trunk services, the configured services for all ports in a same TRUNK group should be same.

5.2 TRUNK function configuration

5.2.1 Trunk port configuration

- **Configure the quantity of Trunk ports by command line**

```
KYLAND(config)#trunk 1
```

- **Enter the port configuration menu, take Trunk port 1 as example,**

```
KYLAND(config-trunk1)#
```

5.2.2 Adding Trunk port

- **Adding port 1 into Trunk port 1, and the quantity of added ports is different in different equipment.**

```
KYLAND(config-trunk1)#add port 1
```

5.2.3 Delete port from Trunk ports

- **Delete port 1 from Trunk port 1, and only the added ports can be delete from the Trunk port**

```
KYLAND(config-trunk1)#delete port 1
```

5.2.4 Back to main menu

```
KYLAND(config-trunk1)#end
```

5.2.5 Back to upper menu

```
KYLAND(config-trunk1)#exit
```

Chapter 6 QoS Configuration

6.1 QoS overview

QoS is the abbreviation of Quality of Service. It is a network ability of providing higher priority service, including dedicated bandwidth, jitter control, and delay (applied to real time and interactive traffic conditions), packet loss rate improvement, specified network traffic under different WAN, LAN and MAN technology, etc , meanwhile to ensure that the priority provided to each traffic would not prevent other traffic processing.

SICOM series industrial Ethernet switch support two kinds of scheduling modes: HQ-PREEMPT and WRR. In HQ-PREEMPT, when the highest priority service comes, firstly transmit the highest priority service. After this transmitting, WRR can schedule other priority services.

WRR schedules data packets according to users' setting proportion.
SICOM series switch support TOS/DSCP modes' selection.
SICOM series switch support setting weight ratio. The default vale is 8:4:2:1 (highest, high, low, and lowest)
SICOM series switch support 3 kinds of scheduling strategies: based on port (highest priority), based on TOS/DIFF and based on 802.p priority. The priority relation between these three strategies is port-based>TOS/DIFF-based>802.1p-based.
SICOM series switch support the remapping of 802.1p priority, IPTOS priority, DSCP priority with queues.

6.2 QoS configuration

6.2.1 Enable/disable QoS

User can enable and disable QoS function by command line and other QOS configurations can be set after this configuration.

- **Enable QoS**

```
KYLAND(config)# qos enable
```

- **Disable QOS**

```
KYLAND(config)# qos disable
```

6.2.2 QOS scheduling mode configuration

QOS support two scheduling modes:

- **Configure HQ-PREEMPT mode for QoS**

```
KYLAND(config)# qos schedule-mode hq-preempt
```

- **Configure WRR mode for QoS**

```
KYLAND(config)# qos schedule-mode wrr
```

6.2.3 Scheduling strategies configuration

SICOM series switch support 3 scheduling strategies: port-based priority, 802.1p-based priority and IP TOS/DIFF-based priority. All scheduling strategies are based on entering port data.

- Port-based priority only map two queues, highest and lowest
- 802.1p-based priority support 4 queues
- IP TOS/DIFF-based support 4 queues

Note:

The priority relations between these three scheduling strategies: port-based>IP TOS/DIFF-based>802.1P-based

---

Command behavior:

- **Enable port-based scheduling strategy**

```
KYLAND(config)# qos policy port-based add/delete port <1-MAX>
```

- **Disable port-based scheduling strategy**

```
KYLAND(config)# qos policy port-based delete port <1-MAX>
```

- **Enable 802.1p-based scheduling strategy**

```
KYLAND(config)# qos policy 802.1p-based add port <1-MAX>
```

- **Disable 802.1p-based scheduling strategy**

```
KYLAND(config)# qos policy 802.1p-based delete port <1-MAX>
```

- **Enable IP TOS-based scheduling strategy**

```
KYLAND(config)# qos policy tos-diff add port <1-MAX>
KYLAND(config)#qos tos-diff-mode tos
```

- **Enable IP DIFF-based scheduling strategy**

```
KYLAND(config)# qos policy tos-diff add port <1-MAX>
KYLAND(config)#qos tos-diff-mode diff-serv
```

- **Disable IP TOS/DIFF-based scheduling strategy**

```
KYLAND(config)# qos policy tos-diff delete port <1-MAX>
```

6.2.4 Priority weight ratio configuration

At the WRR scheduling mode, user can specify the priority weight ratio. In default state, the weight ratio of 4 priority queues is as follows;

Scheduling ratio	priority
8	Highest
4	High
2	Low
1	Lowest

Command lines are as follows:

- **Priority weight ratio configuration:**

```
KYLAND(config)# qos weight-config queue-0<1-55> queue-1<1-55>
queue-2 <1-55> queue-3 <1-55>
```

queue-0<1-55> is the lowest priority, queue-1 is low priority, queue-2 is high priority and queue-3 is highest priority.

Note:

The weight ratio of high priority is not less than that of low priority.

6.2.5 VLAN priority mapping configuration

SICOM series switch support 802.1p-based priority scheduling strategy. 802.1p priority is a priority scheduling strategy that distinguish message priority by VLAN TAG priority in 802.1Q messages. When the message enter the switch with Untag mode, switch add them into VLAN Tag according to port's 802.1p priority which is regarded as the message priority. 802.1p priority configuration of ports is described in the port configuration.

Configure 802.1p-based scheduling strategy, the mapping relation is showed in the below table at the default state.

802.1p priority	Priority queue
6-7	Queue 3 (Highest priority)

4-5	Queue 2 (high priority)
2-3	Queue 1 (low priority)
0-1	Queue 0(lowest priority)

- **VLAN priority mapping configuration**

```
KYLAND(config)# qos vlan priority <0-7> map queue <0-3>
```

6.2.6 TOS priority mapping configuration

The mapping relation is showed in the following table at default state:

IP TOS priority	Priority
6-7	Queue 3 (highest priority)
4-5	Queue 2 (high priority)
2-3	Queue 1(low priority)
0-1	Queue 0 (lowest priority)

- **TOS priority mapping configuration**

```
KYLAND(config)# qos tos priority <0-7> map queue <0-3>
```

6.2.7 DSCP priority mapping configuration

The mapping relations is showed in the following figure under the default state.

IP DSCP priority	Priority
47-63	Queue 3 (highest priority)
32-47	Queue 2 (high priority)
16-31	Queue 1 (low priority)
0-15	Queue 0 (lowest priority)

- **DSCP priority mapping configuration**

```
KYLAND(config)# qos diff-serv dscp priority <0-63> map queue <0-3>
```

6.2.8 Showing QoS configuration

```
KYLAND#show qos
```

Chapter 7 IGMP Snooping Configuration

7.1 IGMP Snooping Overview

IGMP(Internet Group Management Protocol), a part of IP protocol, is used to support and manage IP multicast between host and multicast router. IGMP is for resource discovery and to minimize network load to realize the effective on-line data tranmission.

SICOM series switch support IGMP Snooping function. IGMP Snooping is used to monitor IGMP messages between host and routers, and process these IGMP meassages. IGMP Snooping make swtich be able to track all network group members which are physically connected with switch. IGMP snooping runs between host and multicast routers to manage the member relationships.

SICOM series switch support message auto-query function, so that the switch can be applied in the network without Layer 3 switch or router.

SICOM series switch support the selection of IGMP qurey device and auto-query restraint function. It prevents query message increasing with the increase of query switches, and avoids the multicast service couldn't reaching the receiving end when the selected switch breakdown.

The general query time is 125 seconds according to the IGMP protocol and the max responding time is 10 seconds, so if the network topology change, the recovery time of multicast services is up to 135 seconds. Our DT-Ring, Dt+ and RSTP protocols have topology changing informing system, which can reduce the recovery time of multicast service to less than 5 seconds. It is recommended that using IGMP Snooping together with DT-Ring/DT+/RSTP protocol.

Note :

The max multicast addresses in switch is 256. Do not exceed this range.

7.2 IGMP Snooping Configuration

7.2.1 Configure IGMP Snooping auto-query function

If there is not Layer 3 switch or router, IGMP auto-query function is required. User can

specify switch(es) as query device(s). The selected query switch(es) periodcally send IGMP query message to maintain the IGMP multicast routing table. For the reliablity of multicast service, it is recommended to enable auto –query function for all switches.

At configuration mode, enable auto-query function of IGMP, using the following command line.

- **Enable IGMP auto-query function**

```
KYLAND(config)#igmp auto-query enable
```

- **Disable IGMP auto query function**

```
KYLAND(config)#igmp quto-query disable
```

7.2.2 Enable/disable IGMP Snooping

```
KYLAND(config)#igmp enable
```

7.2.3 Showing the information of IGMP Snooping multicast group members

Using the following command line :

```
KYLAND#show igmp-snooping
```

Chapter 8 DT-Ring Protocol configuration

8.1 Brief introduction of DT-Ring protocol family

Industrial field communication requires reliable communication and fast recovery from failure. In some areas, the data diversion, isolation and load balance are also required. The STP/RSTP/MSTP protocols cannot meet requirements above very well. DT-Ring protocol family is KYLAND's private communication protocol, and it is customized for industrial communication. This family includes DT-Ring, DT-Ring+ and DT-VLAN.

8.2 Introduction of DT-Ring

DT-Ring protocol is KYLAND's private communication protocol. It can detect the ring ports link status in a short time through less protocol messages, and switch the status of the ring connection. DT-Ring can realize the fast recovery and easy maintenance meeting the requirements of industrial communication.

Figure 8-1 displays a DT-Ring topology. One of the switches is configured as master while others as slave.

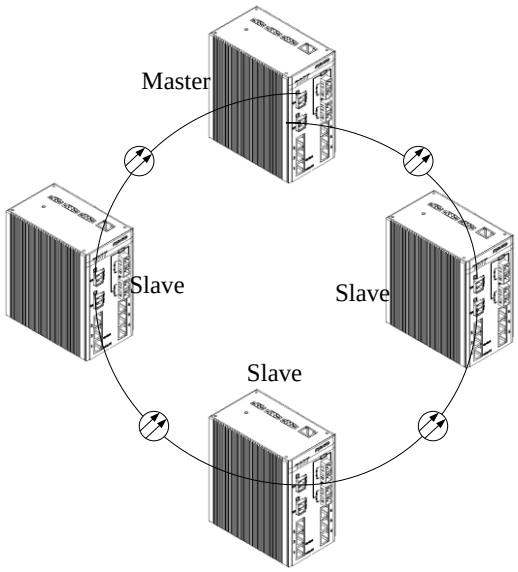


Figure 8-1 DT-Ring topology

Configuration instructions:

- Several domains are supported in one switch, and the tangent ring can be supported in this way.

- Each switch in a same ring should have same domain ID. The domain name should also be the same for easy maintenance.
- Only one master exists in one ring. Others should be all set as slaves.

The quantity of switches being connected in one ring should be determined according to following circumstances:

1. Network throughput. When quantity of the switches grows, the data flow on the ring ports also grows. We should keep the data flow less than the network throughput.
2. Recovery time. DT-Ring can realize fast recovery, however the time delay still exists. The time delay can be figured out by the formula:
   Max recovery time = (Quantity of the switches in the ring x 2.5 + 10) ms
   The max recovery time is related to the quantity of switches in one ring, and the recovery time grows together with the quantity.
3. Protection efficiency. DT-Ring can realize 1: N protection that means one unit can protect other N units. But if N is too large, then the protection efficiency will be reduced.
4. Easy maintenance. Too many switches in one ring will cause difficulties on maintenance.

8.3 DT-Ring configuration

8.3.1 Create / Delete DT-Ring domain

- **Create a DT-Ring domain**
  `KYLAND(config)#dt-ring new <1-31> domain <1-32> master/slave`
  The parameter <1-31>: domain name. The parameter <1-32> : domain ID.
  This domain can be set as master / slave.
- **Delete a DT-Ring domain**
  `KYLAND(config)#dt-ring del domain <1-32>`
  The parameter <1-32> : domain ID.

Note:
The first step of setting a DT-Ring is to create a new DT-Ring domain.

8.3.2 Create/Delete the ring ports

In a DT-Ring, ring ports should be configured to compose a redundant ring topology.

- **Create a ring port**
  `KYLAND(config)#dt-ring <1-32>`
  `KYLAND(config-dt-ring-1)#ringport add <1-10>`
  The parameter <1-32> : Domain ID.
  The parameter <1-10> :Port ID.

- **Delete a ring port**

  ```
  KYLAND(config)#dt-ring <1-32>
  KYLAND(config-dt-ring-1)#ringport delete <1-10>
  ```

  The parameter <1-32> : Domain ID

  The parameter<1-10> : Port ID

Note:

Only two ring ports are allowed, no more no less. Or the ring cannot work normally.

8.3.3 DT-Ring protocol Enable/Disable

Configuration is required in order to to enable the DT-Ring.

- **Enable DT-Ring**

  ```
  KYLAND(config)#dt-ring <1-32>
  KYLAND(config-dt-ring-1)#protocol enable
  ```

  The parameter <1-32> : Domain ID.

- **Disable DT-Ring**

  ```
  KYLAND(config)#dt-ring <1-32>
  KYLAND(config-dt-ring-1)#protocol disable
  ```

  The parameter <1-32> : Domain ID.

8.3.4 Display the status of the DT-Ring domain

This command can display the basic settings and protocol information.

- **Display the status of DT-Ring domain**

  ```
  KYLAND#show dt-ring <1-32>
  ```

  The parameter <1-32> : Domain ID.

Chapter 9 DT-VLAN protocol configuration

9.1 Introduction of DT-VLAN protocol

DT-VLAN is an extension protocol of DT-Ring. DT-Ring offers redundant protection based on ports, and only one redundant ring can be allowed in one redundant link circuit. DT-VLAN protocol is based on VLANs in one link circuit that several redundant rings can be supported according to the settings of the VLAN. It can control each VLAN's transfer and forward status and realize fast recovery.

If we can set several rings in one link circuit, since the masters can be different switches, the data flow can be diversed. In this way, it is possible to protect key business data flow, realize load balance through flexible networking and rasional allocation of data flow.

Figure 9-1 is a typical network topology. We can set one ring as SWITCH A <->LINK A-D-1<->SWITCH D<->LINK C-D<->SWITCH C<->LINK C-B<->SWITCH B<->LINK A-B-1<->SWITCH A. And set another ring as SWITCH A <->LINK A-D-2<->SWITCH D<->LINK C-D<->SWITCH C<->LINK C-B<->SWITCH B<->LINK A-B-2<->SWITCH A. The two redundant rings belong to different VLANs.

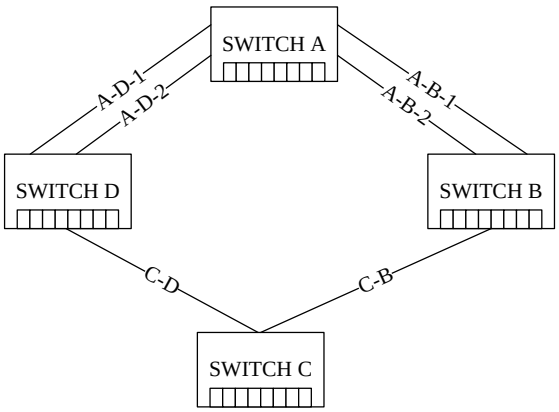


Figure 9-1 DT-VLAN typical topology

Configuration instructions :

- Several domains are supported in one switch, and the tangent ring can be supported in this way.
- Each switch in a same ring should have same domain ID. The domain name should also be the same for easy maintenance.
- Only one master exists in one ring. Others should be all set as slaves.
- One VLAN only belongs to one DT-Ring domain.
- While a switch has been set to support DT-VLAN, it cannot support DT-Ring based on

ports.

About the quantity of switches being connected in one ring, please refer to the introduction above.

9.2 DT-VLAN configuration

9.2.1 Change the setting of DT-Ring

To create a VLAN ring, the redundant ring mode should be set as VLAN. Since RSTP and DT-Ring are both based on ports, they cannot be set to support a VLAN ring.

- **Set redundant ring mode as VLAN mode**

  ```
  KYLAND(config)#dt-ring mode vlan-based
  ```

- **Set redundant ring mode as Port mode**

  ```
  KYLAND(config)#dt-ring mode port-based
  ```

9.2.2 Create/Delete DT-Ring domain

- **Create a DT-Ring domain**

  ```
  KYLAND(config)#dt-ring new <1-31> domain <1-32> master/slave
  ```

  The parameter <1-31>: domain name. The parameter <1-32> : domain ID.
  This domain can be set as master / slave.

- **Delete a DT-Ring domain**

  ```
  KYLAND(config)#dt-ring del domain <1-32>
  ```

  The parameter <1-32> : domain ID.

Note:
The first step of setting a DT-Ring is to create a new DT-Ring domain.

9.2.3 Create/Delete ring ports

In a DT-Ring, ring ports should be configured to compose a redundant ring topology.

- **Create a ring port**

  ```
  KYLAND(config)#dt-ring <1-32>
  KYLAND(config-dt-ring-1)#ringport add <1-10>
  ```

  The parameter <1-32> : Domain ID.
  The parameter <1-10> :Port ID.

- **Delete a ring port**

```
KYLAND(config)#dt-ring <1-32>
KYLAND(config-dt-ring-1)#ringport delete <1-10>
```

The parameter <1-32> : Domain ID

The parameter<1-10> : Port ID

Note:

Only two ring ports are allowed, no more no less. Or the ring cannot work normally.

9.2.4 Create/Delete VLAN

Create effective VLAN in DT-Ring, one VLAN can only be created in one DT-Ring once.

- **Create VLAN**

```
KYLAND(config)#dt-ring <1-32>
KYLAND(config-dt-ring-1)#vlan add <1-4093>
```

The parameter <1-32> : Domain ID

The parameter <1-4093> : VLAN ID

- **Delete VLAN**

```
KYLAND(config)#dt-ring <1-32>
KYLAND(config-dt-ring-1)#vlan delete <1-4093>
```

The parameter <1-32> : Domain ID

The parameter <1-4093> : VLAN ID

9.2.5 Enable/Disable DT-Ring Protocol

- **Enable DT-Ring**

```
KYLAND(config)#dt-ring <1-32>
KYLAND(config-dt-ring-1)#protocol enable
```

The parameter <1-32> : Domain ID.

- **Disable DT-Ring**

```
KYLAND(config)#dt-ring <1-32>
KYLAND(config-dt-ring-1)#protocol disable
```

The parameter <1-32> : Domain ID.

9.2.6 Display the status of the DT-Ring domain

This command can display the basic settings and protocol information.

- **Display the status of DT-Ring domain**

```
KYLAND#show dt-ring <1-32>
```

The parameter <1-32> : Domain ID.

Chapter 10 DT-Ring+ configuration

10.1 Introduction of DT-Ring+

DT-Ring+ is KYLAND's private communication protocol developed from DT-Ring and realizes the backup between two rings. Figure 10-1 displays the topology.

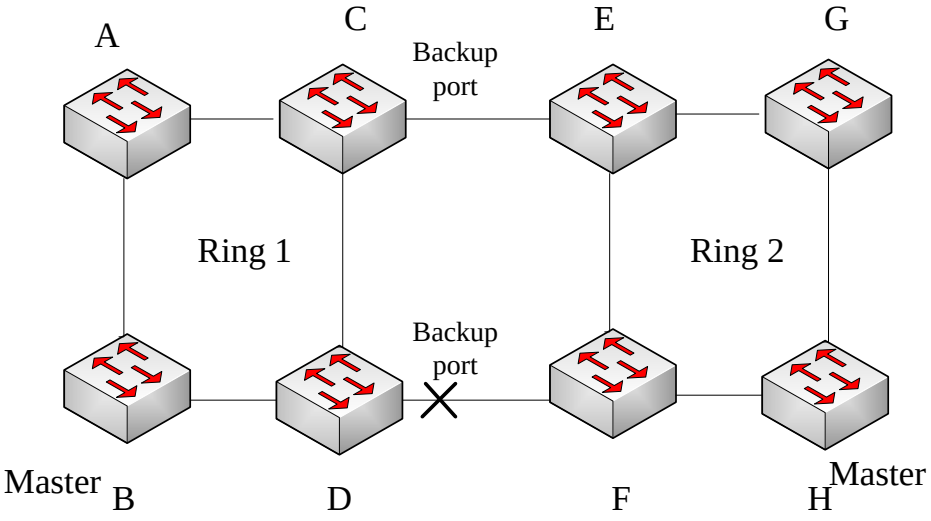


Figure 10-1 DT-Ring+ Topology

Configuration instructions:

- In one switch, only one backup port is allowed.
- In one ring, only two backup ports are allowed.
- In one ring, the backup port can be set on maseter or slave.

10.2 DT-Ring+ Configuration

10.2.1 Enable/Disable DT-Ring+

- **Enable DT-Ring+**

  `KYLAND(config)#dt <1-32>`

  `KYLAND(config-dt-ring-1)#dtring+ enable`

  The parameter <1-32> : Domain ID

  The parameter <1-10> : Port ID

- **Disable DT-Ring+**

  `KYLAND(config)#dt <1-32>`

  `KYLAND(config-dt-ring-1)#dtring+ disable`

  The parameter <1-32> : Domain ID

  The parameter <1-10> : Port ID

Note:

To set DT-Ring+, a DT-Ring domain should be created firstly.

10.2.2 Create/Delete backup ports

In DT-Ring+, we need to set two backup ports to compose the backup redundant rings.

- **Create a backup port**

  ```
  KYLAND(config)#dt <1-32>
  KYLAND(config-dt-ring-1)#backport add <1,26>
  ```

  The parameter <1-32> : Domain ID

  The parameter<1-10> : Port ID

- **Delete a backup port**

  ```
  KYLAND(config)#dt <1-32>
  KYLAND(config-dt-ring-1)#backport delete <1,26>
  ```

  The parameter <1-32> : Domain ID

  The parameter <1-10> : Port ID

Note:

Only two backup ports are allowed, no more no less. Or the ring cannot work normally.

10.2.3 Display the status of DT-Ring+

The command displays the information of backup ports.

- **Display the status of DT-Ring+**

  ```
  KYLAND#show dt <1-32>
  ```

  The parameter <1-32> : Domain ID

Chapter 11 RSTP configuration

11.1 Introduction of RSTP

RSTP (Rapid Spanning Tree Protocol) is a layer 2 management protocol developed from STP (Spanning Tree Protocol). It is compatibal with STP.

RSTP defines Root Bridge, Root Port, Designated Port, Path Cost and realizes the mission to cut redundant ring paths by creating a natural tree topology, and optimizes the link backup and path selection.

RSTP transfers protocol messages through a special configuration message named BPDU (Bridge Protocol Data Unit). BPDU is transfered in Ethernet data frame using a multicase MAC address 01-80-C2-00-00-00 as its destination.

RSTP realizes all functions of STP and offer more records toward network environment. By these records, RSTP can reduce the time delay from block to forward and recover the network rapidly without causing temporary ring.

SICOM series can fully support RSTP and STP. And it can also be connected with other devices which support STP.

SICOM series supports the function of enable/disable single port so that the STP edged-port can be disabled avoiding block status caused by the changing of network topology.

SICOM series realizes the function of port stabilization. This function solves the problem of frequent disconnections caused by the problem of port physical connections, and improve the reliability of the network performance.

11.2 RSTP configuration

11.2.1 RSTP bridge node

- **Enable RSTP**
  `KYLAND(config)#rstp enable`
- **Disable RSTP**
  `KYLAND(config)#rstp disable`
- **Bridge priority**
  `KYLAND(config)#rstp bridge priority <0x00-0xFFFF>`

The parameter <0x00-0xFFFF>: the value of bridge priority. It's range is 0x00 to 0xFFFF, the pace is 0x1000, default value is 0x8000.

The device's bridge priority and MAC address compose the bridge ID. RSTP determines current root bridge and root port by bridge ID. The less the value of priority is, the more priority the bridge will have. The device with the smallest bridge ID will be regarded as the root bridge.

In the network, the device will be forced to be the root by setting its priority value to be the smallest.

- **Setting bridge forward delay**

  `KYLAND(config)#rstp forward-delay <4-30>`

  The parameter <4-30>: forward delay (seconds). The default value is 15 seconds.
  Forward delay is the status transition time for Discarding -> Learning -> Forwarding. It is set by ROOT and it is unified in the whole network. This delay time also includes MAC address table's Short Ageing Time.

- **Setting bridge hello time**

  `KYLAND(config)#rstp hello-time <1-2>`

  The parameter of <1-2> is the hello time (seconds). The default value is 2. Hello time is the interval of sending BPDU periodically. It is set by ROOT and it is unified in the whole network.

- **Setting bridge max age**

  `KYLAND(config)#rstp rstp max-age <6-40>`

  The parameter <6-40>: message max age (seconds). The default value is 20.
  Max age determines the times one setting message being transmitted in the network. Each setting message will contain a Configuration Message Age. The setting message is generated in the ROOT. In the BPDU sent by ROOT, the message max age will always be 0. While the message passes one switch, the age will be added by 1. While the message age is bigger than maximum age, the message will be discarded. Max age limits the times a switch joins the RSTP calculation. The devices with a hop count bigger than the max age will not be calculated in the present spanning tree.

- **Setting protocol version**

  `KYLAND(config)#rstp rstp forceversion <0-2>`

  The parameter <0-2>: current protocol version, 0 for STP, 2 for RSTP, 1 is not valid.

Note:

The value of Forward Delay, Max Age, and Hello Time should correspond with following rules :

2 * (Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)

11,2,2 RSTP port configuration

- **Enable RSTP port**

  `KYLAND(config)#rstp port <1-10> enable`

  The parameter <1-10> : port ID
- **Disable RSTP port**

  `KYLAND(config)#rstp port <1-10> disable`

  The parameter <1-10> : port ID
- **Setting port path cost**

  `KYLAND(config)#rstp port <1-10> path-cost <1-20000000>`

  The parameter <1-10>: Port ID.

  The parameter<1-20000000>: Path cost to the root port.

  Path cost is a shortest path cost between current port and root port. It is determined by the bandwidth. The bigger the bandwidth is, the smaller the path cost will be. Modifying the path cost will change the forwarding path from current device to the root port.
- **Setting the port priority**

  `KYLAND(config)#rstp port <1-10> priority <0x00-0xFF>`

  The parameter <1-10>: Port ID

  The parameter <0x00-0xFF>: Port priority, the default value is 0x80.

  Both device port priority and port ID will be used in calculating the root port.
- **Check port protocol version**

  `KYLAND(config)#rstp port <1-10> mcheck`

  The parameter <1-10>: Port ID

  This function is to avoid the situation that both ends of the current link can support RSTP but they are working under STP protocol. Using `mcheck` command can force the devices which support RSTP work under RSTP status.

11.2.3 Display RSTP status

- **Display current protocol status**

  `KYLAND#show rstp`

  This command will display the protocol status of current bridge and all ports.

```
KYLAND#
```

```
KYLAND#show rstp
--------------------SPANNING TREE information in the bridge -----------
Root ID Mac Address          : 08:00:3e:32:53:22
Root ID Priority            : 0x8000
Designated Root Path Cost     : 0
Root Port                   : none
Root Max Age    20   Hello Time  2    Forward Delay  15

Bridge ID Mac Address        : 08:00:3e:32:53:22
Bridge ID Priority           : 0x8000
Bridge ForceVersion          : 2
Bridge Max Age  20   Hello Time  2    Forward Delay  15

-------------------All ports information in the bridge-----------------
Name   pri    cost       role span-state lk p2p    Desi-bridge-id    Dcost
D-port
1     0x80  2000000   Dis  Discarding N  N
2     0x80  2000000   Dis  Discarding N  N
3     0x80 200000     Desi Discarding Y  Y    0x8000:08003e325322 0     0x8003
4     0x80  2000000   Dis  Discarding N  N
5     0x80  2000000   None      None N  N
6     0x80  2000000   None      None N  N
7     0x80  200000    None      None N  Y
8     0x80  200000    None      None N  Y
9     0x80  20000     None      None N  Y
10    0x80  20000     None      None N  Y
```

Chapter 12 SNMP Configuration

12.1 Introduction of SNMP

SNMP is the most widely used network management protocol in TCP/IP. In the May of 1990, RFC 1157 defined the first version of SNMP (Simple Network Management Protocol)-SNMP v1. RFC1157 and RFC1155 together offer a method for monitoring and managing computer network. For this reason, SNMP has been widely used and became de facto standard of network management.

SNMP has been developed rapidly in the beginning of 1990's. However, it also has some obvious shortcomings. For example, it can not support mass data transmitting. It doesn't support Authentication and Privacy strategies. So, SNMP v2 was released in 1993. SNMP v2 can support:

SNMPv2c provides several advantages over SNMPv1. SNMPv2c has expanded data types of 64-bit counter. It calls for improved efficiency and performance by introducing the GETBULK operation. Confirmed event notification is sought by the introduction of the Inform operator. Enhanced error handling approach, improved sets, and a fine tuned Data Definition Language are some of the advantages of SNMPv2c over the SNMPv1.

SICOM series supports full SNMP v1 and v2.
SICOM series supports multiple EMS management stations (1-3).
SICOM series supports multiple trap IP addresses (1-5), and still extendable.
SICOM series supports standard MIB: RFC1213, RFC1757, RFC1493.
SICOM series private MIBs include: KYLAND-DEV.MIB, KYLAND-PORT.MIB, KYLAND-CARD.MIB, LLDP.MIB, KYLAND-ALARM.MIB.
SICOM series can support standard trap according to RFC1215, private trap with richer information, and its port status and ring status can be searched actively.

12.2 SNMP configuration

12.2.1 Enable/Disable SNMP

This function can enable or disable SNMP and this is the main switch SNMP function.

- **Enable SNMP**
  `KYLAND(config)#snmp enable`
- **Disable SNMP**
  `KYLAND(config)#no snmp enable`

12.2.2 Read/Write community name

Through this function of reading or writing community name, the access control of the device is realized and the communication security is enhanced because the device will only accept the message with a qualified community name.

- **Setting read only community name**

  `KYLAND(config)#snmp community <3-16> ro`

  The parameter <3-16>: number of characters.

- **Setting read/write community name**

  `KYLAND(config)#snmp community <3-16> rw`

  The parameter <3-16>: number of characters.

12.2.3 Trap IP address configuration

Trap IP address configuration realized selective trap message sending, and the device will only send trap messages to the listed IP addresses in Trap IP Address List.

- **Add trap IP address**

  `KYLAND(config)#snmp add-trapip <1-5> <H.H.H.H>`

  The parameter <1-5>: Trap IP serial no.

  The parameter<H.H.H.H>: Trap IP address.

- **Delete trap IP address**

  `KYLAND(config)#snmp del-trapip <1-5>`

  The parameter <1-5>: Trap IP serial no.

12.2.4 Request/Trap port number

Through setting device's request port number, the device will only response to the messages sent to this port number from EMS server, and realized the access control.

Through setting device's trap port number, the EMS server can only receive trap messages on this port number.

- **Request port number**

  `KYLAND(config)#snmp reqport <1-65535>`

  The parameter <1-65535>: Requested port number.

- **Trap port number**

  `KYLAND(config)#snmp trport <1-65535>`

  The parameter <1-65535>: Requested port number.

Note:

While setting request port number, the port number for EMS server to send request messages should also be modified, or the connection will be down.

12.2.5 Setting the number of EMS management stations

The number of EMS management station is the number of devices allowed to be connected. Controlling this number will help controlling the communication load and enhance the security. The ageing time of a management station is 1minute. During this period of time, the management station is not connected to other devices and its IP address is also removed from EMS IP list.

- **Setting the number of management stations**
  `KYLAND(config)#snmp emsnum <1-3>`
  The parameter <1-3> : the number of management station.

12.2.6 Enable/Disable Trap

- **Enable Trap**
  `KYLAND(config)#snmp trap enable`
- **Disable Trap**
  `KYLAND(config)#snmp trap disable`

12.3 Display SNMP status

- **Display SNMP status**
  `SWITCH#show manager`
  Display SNMP protocol enable/disable status, request/trap port number and EMS management station number.

- **Display SNMP read/write community name**
  `SWITCH#show snmp community`

- **Display connected devices EMS IP address list**
  `SWITCH#show snmp emsiplist`

- **Display Trap IP address list**
  `SWITCH#show snmp trapiplist`

- **Display SNMP receiving/sending message statistics.**
  `SWITCH#show snmp status`

Chapter 13 RMON configuration

13.1 Introduction of RMON

RMON (Remote Network Monitoring) is the most important enhancement toward SNMP. It defines standard network monitoring functions and communication interfaces between management console and remote monitor. RMON offers an effective way to monitor the network performance with reducing other agents and management stations' load.

RMON's main developing targets include :
Work offline : the network manager limits or stops the role poling of a monitor, and with limited search, the communication cost can be saved.
Active monitoring : if the resource is enough, and its behavior is not harmful, the monitor will actively monitor and record the network performance.
Fault inspecting and reporting : the monitor can inspect the fault and other circumstances such as block according to the recorded information and report to management station.
Increase the value of data : the network monitor can analyze the data collected in subnets, and reduce the burnden of management station.
Multiple managements supported : multiple management stations can be supported to realize the reliablility, fulfill different functions or manage different parts of one network. The monitor can be set be communicate with multiple management stations.
RMON MIB consists of several groups :

1. Statistics : real-time LAN statistics e.g. utilization, collisions, CRC errors
2. History: history of selected statistics
3. Alarm: definitions for RMON SNMP traps to be sent when statistics exceed defined thresholds
4. Event: send alerts (SNMP traps) for the Alarm group

13.2 RMON configuration

13.2.1 RMON operating parameters setting

- **Create statistics group**
  `KYLAND(config)#rmon stats add <1-65535> <1-10> <1,32>`
  The parameter <1-65535>: Statistics group ID, it's the statistics group's identification
  The parameter <1-10>: Port number
  The parameter <1, 32>: Creator's name
  The statistics group will record the statistics of data flow through the port
- **Delete statistics group**
  `KYLAND(config)#rmon stats delete <1-65535>`

The parameter <1-65535>: the statistics group ID.

- **Create history group**

  `KYLAND(config)#rmon his add <1-65535> <1-10> <1-65535> <1-3600> <1,32>`

  The first parameter <1-65535>: the history group ID. It's the identification of history group.

  The second parameter <1-10>: Port number

  The third parameter <1-65535>: the number of stored sampling, the default value is 50.

  The fourth parameter <1-3600>: the data sampling interval, the default value is 1800 (seconds).

  The fifth parameter <1, 32>: the creator's name

  The history group defines the sampling function of one or more monitors, stores selected statistics with appointed sampling interval.

- **Delete history group**

  `KYLAND(config)#rmon his delete <1-65535>`

  The parameter <1-65535>: the history group ID

- **Create alarm group**

  `KYLAND(config)#rmon alarm add <1-65535> <1-65535> <1,128> <1-2> <1-3> <1-65535> <1-65535> <1-65535> <1-65535> <1,32>`

  The first parameter <1-65535>: the alarm group ID.

  The second parameter <1-65535>: the sampling interval.

  The third parameter <1, 128>: the monitored statistics grouping node OID or ifEntry grouping node OID.

  The fourth parameter <1-2>: the sampling type, 1 for absolute sampling and 2 for relative sampling.

  The fifth parameter <1-3>: the alarm type, 1 for rising alarm, 2 for falling alarm, and 3 for rising alarm or falling alarm.

  The sixth parameter <1-65535>: the rising threshold.

  The seventh parameter <1-65535>: the falling threshold.

  The eighth parameter <1-65535>: the rising event index.

  The ninth parameter <1-65535>: the falling event index.

  The tenth parameter <1, 32>: the creator's name

  The alarm group creates a group of thresholds for monitored OID. If the threshold is exceeded, the monitor will create the alarm and send this alarm to the control center.

- **Delete alarm group**

  `KYLAND(config)#rmon alarm delete <1-65535>`

  The parameter <1-65535>: the alarm group ID.

- **Create event group**

  `KYLAND(config)#rmon event add <1-65535> <1,127> <1-4> <1,127> <1,32>`

  The first parameter <1-65535>: the event group ID.

  The second parameter <1,127>: the text description of this event.

  The third parameter <1-4>: the event type, 1 for NONE, 2 for LOG, 3 for SNMP-TRAP and 4 for LOG-AND-TRAP.

The fourth parameter <1,127>: the group name of management station receiving event trap.

The fifth parameter <1, 32>: the creator's name.

The event group supports the definition of the event. The event can be triggered by the conditions located in other places of MIB, and it can also trigger the action which is defined in other places of MIB. The event enables that the receiving messages are recorded in this group, and makes the monitor to send SNMP trap message to the management station.

- **Delete event group**

  `KYLAND(config)#rmon event delete <1-65535>`

  The parameter <1-65535>: the event group ID.

13.2.2 Display RMON status

- **Display RMON statistics group information**

  `KYLAND#show rmon stats`

  This command will display current statistics group setting information.

```
KYLAND#show rmon stats
StatsIndex       StatsDataSource   StatsOwner          Status
1              ifIndex.1       kyland            SNMP_VALID
2              ifIndex.2       kyland            SNMP_VALID
```

- **Display RMON history group setting information**

  `KYLAND#show rmon hisctrl`

  Display current history group setting information.

```
KYLAND#show rmon hisctrl
hisCtrlIndex  DataSource  BucketsRequested  BucketsGranted  Interval  Owner    Status
 1           ifIndex.1     3                3               5        kyland   SNMP_VALID
 2           ifIndex.2     3                3               5        kyland   SNMP_VALID
```

- **Display RMON history group sampling information**

  `KYLAND#show rmon ethhis`

  Display current history group sampling information.

```
KYLAND#show rmon ethhis
          ethHisIndex: 1        ethHisSampleIndex: 1
                HisIntervalStart: 0days 2h:5m:11s.90th
                DropEvnt:      0
                Octets:        1689
                Pkts:          16
                BroadCastPkts:  15
                MulticastPkts:  0
                CRCAlignErr:    0
                UndersizePkts:  0
                OversizePkts:   0
```

```
      Fragments:     0
      Jabbers:       0
      Collisions:    0
      Utilization:   1
ethHisIndex: 1        ethHisSampleIndex: 2
      HisIntervalStart: 0days 2h:5m:16s.90th
      DropEvnt:      0
      Octets:        1960
      Pkts:          18
      BroadCastPkts:  16
      MulticastPkts:  2
      CRCAlignErr:   0
      UndersizePkts:  0
      OversizePkts:   0
      Fragments:     0
      Jabbers:       0
      Collisions:    0
      Utilization:   1
ethHisIndex: 1        ethHisSampleIndex: 3
      HisIntervalStart: 0days 2h:5m:21s.90th
      DropEvnt:      0
      Octets:        1258
      Pkts:          14
      BroadCastPkts:  12
      MulticastPkts:  0
      CRCAlignErr:   0
      UndersizePkts:  0
      OversizePkts:   0
      Fragments:     0
      Jabbers:       0
      Collisions:    0
      Utilization:   1
ethHisIndex: 2        ethHisSampleIndex: 1
      HisIntervalStart: 0days 2h:5m:11s.90th
      DropEvnt:      0
      Octets:        0
      Pkts:          0
      BroadCastPkts:  0
      MulticastPkts:  0
      CRCAlignErr:   0
      UndersizePkts:  0
      OversizePkts:   0
      Fragments:     0
      Jabbers:       0
```

```
            Collisions:    0
            Utilization:   0
      ethHisIndex: 2        ethHisSampleIndex: 2
            HisIntervalStart: 0days 2h:5m:16s.90th
            DropEvnt:      0
            Octets:        0
            Pkts:          0
            BroadCastPkts:  0
            MulticastPkts:  0
            CRCAlignErr:   0
            UndersizePkts:  0
            OversizePkts:   0
            Fragments:     0
            Jabbers:       0
            Collisions:    0
            Utilization:   0
      ethHisIndex: 2        ethHisSampleIndex: 3
            HisIntervalStart: 0days 2h:5m:21s.90th
            DropEvnt:      0
            Octets:        0
            Pkts:          0
            BroadCastPkts:  0
            MulticastPkts:  0
            CRCAlignErr:   0
            UndersizePkts:  0
            OversizePkts:   0
            Fragments:     0
            Jabbers:       0
            Collisions:    0
           Utilization:   0
```

- **Display RMON alarm group setting information**

  KYLAND#show rmon stats

  Display current alarm group setting information.

```
KYLAND#show rmon alarm
      alarmIndex: 1
            Interval:         5
            Variable:         1 .3 .6 .1 .2 .1 .2 .2 .1 .16 .1
            SampleType:       ALARM_ABSOLUTE
            StartupAlarm:     ALARM_RISING
            RisingThreshold:   100
            FallingThreshold:  10
            RisingEventIndex:  1
            FallingEventIndex: 1
            Owner:            kyland
```

```
        Status            SNMP_VALID
    alarmIndex: 2
        Interval:         5
        Variable:         1 .3 .6 .1 .2 .1 .16 .1 .1 .1 .14 .1
        SampleType:       ALARM_ABSOLUTE
        StartupAlarm:     ALARM_RISING
        RisingThreshold:   100
        FallingThreshold:  10
        RisingEventIndex:  1
        FallingEventIndex: 1
        Owner:            kyland
       Status            SNMP_VALID
```

- **Display RMON event group setting information**

  KYLAND#show rmon stats

  Display current event group setting information.

```
KYLAND#show rmon event
      eventIndex:    1
      Description:   log and trap event
      Type:          log-and-trap
      Community:     public
      LastTimeSent:  0days 2h:15m:45s.0th
      Owner:         kyland
      Status         SNMP_VALID
```

- **Display RMON log**

  KYLAND#show rmon log

  Display current RMON log.

```
KYLAND#show rmon log
     logEvntIndex: 1      logIndex: 1
     logTime:       0days 2h:15m:42s.0th
     logDescription: alarm rising  2,1.3.6.1.2.1.16.1.1.1.14.1,1,5234,100
     logEvntIndex: 1        logIndex: 2
     logTime:       0days 2h:15m:45s.0th
     logDescription: alarm rising  1,1.3.6.1.2.1.2.2.1.16.1,1,288854,100
```

Chapter 14 ALARM management configuration

14.1 Introduction of ALARM management module

SICOM series switches support device alarm and related alarm report (SNMP trap), alarm enable/disable, and alarm searching. It assures that the alarm will be reported to the customer timely and accurately.
SICOM series switches support following alarm type:

Alarm type	Meaning
Link down alarm	Alarm while the link is down
DT-Ring master ring open alarm	Alarm while the master's ring status is open
Power supply alarm	Alarm while any of the working dual power supplies power is low level
IP conflict	Support monitoring IP address conflict
MAC conflict	Support monitoring MAC address conflict

Note: If IP conflict and MAC conflict happen together, it means these are own testing packets and it will not alarm.

SICOM series switches support alarm trap. While alarm is enabled, and alarm occurs, it will send SNMP trap to the manager to report the alarm.
SICOM series switches support alarm search by web page search, CLI/Telnet search, and SNMP management software search.
SICOM series switches support LED display for working status. While the device is working properly, the LED will flash in a frequency of 0.5HZ.

14.2 ALARM configuration

14.2.1 Port link down enable/disable

Port link down alarm enable/disable can be set through CLI command. The port disabled for link down alarm will not send trap message to the manager.

- **Setting port alarm management status**

  `KYLAND(config)#alarm port-id <1-26> alarmtype 8001 adstate <1-2>`

  The parameter <1-26>: Port index.

  8001 is alarm type.

  The parameter <1-2>: 1 for Enable and 2 for Disable.

14.2.2 Address conflict detect enable/disable

- **Setting address conflict detect enable/disable**

  `SWITCH(config)#address-conflict-detect [enable/disable]`

14.2.3 DT-Ring ring open alarm enable/disable

DT-Ring ring open alarm can be enabled or disabled through CLI command. The disabled port will not send trap message to the manager.

- **Setting DT-Ring ring alarm management status**

  `KYLAND(config)#alarm dt-domain <1-32> alarmtype 9001 adstate <1-2>`

  The parameter <1-32>: DT-Ring domain index.

  9001 is the DT-Ring ring open alarm type.

  The parameter <1-2>: 1 for Enable and 2 for Disable.

14.3 Display alarm status information

- **Display alarm information**

  `KYLAND#show alarm`

  This command will display the port, DT-Ring, power supply, IP and MAC conflict alarm management status.