

Basic Configuration Commands

Table of Contents

1	System Management Commands.....	- 1 -
1.1	Configuring File Management Commands.....	- 1 -
1.1.1	File System Management.....	- 1 -
1.1.2	File System Commands.....	- 1 -
1.1.3	File System Commands.....	- 1 -
1.1.4	Software Update.....	- 2 -
1.1.5	Configuration Update.....	- 3 -
1.1.6	Use ftp to update the Software and Configuration.....	- 3 -
1.2	Basic System Management Configuration.....	- 5 -
1.2.1	Configure Ethernet IP Address.....	- 5 -
1.2.2	Configure Default Route.....	- 6 -
1.2.3	Test the Network Connection by PING.....	- 6 -
1.3	HTTP Configuration.....	- 7 -
1.3.1	HTTP Configuration.....	- 7 -
1.3.2	HTTP Configuration Example.....	- 8 -
2	Configure the Terminal.....	- 10 -
2.1	VTY Configuration Description.....	- 10 -
2.2	Configuration Task.....	- 10 -

2.2.1	Relationships between the line and the interface.....	- 10 -
2.3	Monitoring and Maintenance.....	- 11 -
2.4	VTY Configuration Example.....	- 11 -
3	Network Management Configuration.....	- 12 -
3.1	Configure SNMP.....	- 12 -
3.1.1	Overview.....	- 12 -
3.1.2	SNMP Configuration Task.....	- 15 -
3.1.3	Example.....	- 18 -
3.2	Configure RMON.....	- 19 -
3.2.1	RMON Configuration Task.....	- 19 -
3.3	Configure PDP.....	- 23 -
3.3.1	Overview.....	- 23 -
3.3.2	PDP Configuration Task.....	- 23 -
3.3.3	Example for PDP Configuration.....	- 25 -
4	SSH Configuration.....	- 27 -
4.1	SSH Overview.....	- 27 -
4.1.1	SSH server.....	- 27 -
4.1.2	SSH client.....	- 27 -
4.1.3	Implement Features.....	- 27 -
4.2	Configuration Task.....	- 27 -

4.2.1	Configure Authentication Methods List.....	- 27 -
4.2.2	Configure Access Control List.....	- 27 -
4.2.3	Configure the timeout for authentication.....	- 28 -
4.2.4	Configure the number of authentication retries.....	- 28 -
4.2.5	Enable SSH server.....	- 28 -
4.3	Example for ssh server Configuration.....	- 29 -
4.3.1	Access Control List.....	- 29 -
4.3.2	Global Configuration.....	- 29 -

1 System Management Commands

1.1 Configuring File Management Commands

1.1.1 File System Management

File names in FLASH can only have 20 characters at most, and not case-sensitive.

1.1.2 File System Commands

All commands in boldface are keywords and the rest are parameters. The part of [] is optional.

Command	Purpose
format	Format the file system, and delete all data.
dir [filename]	Display filename and directory name. Filenames in [] indicate to display the file named begin with these letters. The file is displayed in the following format: Index filename <FILE> length of the file created time
delete filename	Delete a file. If the file is not exist, prompt that the file is not exist.
md dirname	Create a directory
rd dirname	Delete a directory. If the directory is not existed, prompt that the directory is not existed.
more filename	Display the content of a file.
cd	Change the current file system path.
pwd	Display the current path.

1.1.3 File System Commands

monitor#boot flash <local_filename>

This command is used to start the switch software in FLASH. There may be multiple switch software in FLASH.

Parameters

Parameter	Description
flash	The file is saved in FLASH.
<i>local_filename</i>	The filename saved in FLASH. The users must enter the filename.

Example

```
monitor#boot flash switch.bin
```

1.1.4 Software Update

The user can use this command to download the switch system software locally or remotely for a version upgrade or a special feature version (such as data encryption) that you have customized to the company.

There are two ways to update the software in monitoring state.

1) Use TFTP protocol

```
monitor#copy tftp flash [ip_addr]
```

This command is used to copy the file from the tftp server to the system's FLASH. After the user entering the command, the system will prompt the user to enter the remote server name and remote file name.

Parameters

Parameter	Description
Flash:	The file is saved in FLASH.
Ip_addr	IP address of the TFTP server. If it is not specified, it will prompt the user to enter after running copy command.

Example

Read the file named "main.bin" from the server, then write to the switch and named "switch.bin".

```
monitor#copy tftp flash
```

```
Prompt: Source file name[]?main.bin
```

```
Prompt: Remote-server ip address[]?192.168.20.1
```

```
Prompt: Destination file name[main.bin]?switch.bin
```

```
please wait ...
```

```
#####
#####
#####
#####
#####
#####
```

```
TFTP:successfully receive 3377 blocks ,1728902 bytes
```

```
monitor#
```

1.1.5 Configuration Update

The configuration of the switch is saved as a file with the file name startup-config. The user can update the configuration using commands similar to software updates.

- 1) Use TFTP protocol

```
monitor#copy tftp flash startup-config
```

1.1.6 Use ftp to update the Software and Configuration

```
config #copy ftp flash [ip_addr|option]
```

In the formal program, it can also use ftp to update software and configuration under the management state. Use the copy command to download files from the ftp server to the switch, or you can upload a file from the switch file system to the ftp server. After the user

entering the command, the system will prompt the user for the remote server name and the remote file name.

```
copy{ftp:[[/login-name:[login-password]@]location]/directory]/filename)}|flash:filename
>}{flash<:filename>|ftp:[[/login-name:[login-password]@]location]/directory]/filename}<
blksize><mode><type>
```

Parameters

Parameter	Description
login-name	The username of the file server. If it is not specified, it will prompt the user to enter after running copy command.
login-password	Password of the file server. If it is not specified, it will prompt the user to enter after running copy command.
nchecksize	Don't detect the size of the file on the server.
vrf	Provide vrf binding for MPLS-enabled device.
blksize	Data transfer block size (the default value is 512.)
ip-addr	IP address of the ftp server. If it is not specified, it will prompt the user to enter after running copy command.
active	Specify to connect the ftp server using active method.
passive	Specify to connect the ftp server using passive method.
type	Set the type of the transmission data (ascii or Binary)

Example

Download the file “main.bin” from the server, then write it to the switch and named “switch.bin”.

```
config#copy ftp flash
```

```
Prompt: ftp user name[anonymous]? login-nam
```

```
Prompt: ftp user password[anonymous]? login-password
```

```
Prompt: Source file name[]?main.bin
```

```
Prompt: Remote-server ip address[]?192.168.20.1
```


Prompt: Destination file name[main.bin]?switch.bin

Or config#copy ftp://login-nam:login-password@192.168.20.1/main.bin flash:switch.bin

#####

#####

FTP:successfully receive 3377 blocks ,1728902 bytes

config#

Note:

- 1) When the ftp server cannot be access and the waiting time is too long due to the tcp time-out(the default value is 75s), the tcp connecting time can be changed by setting the global command **ip tcp synwait-time**. But it is not suggested.
- 2) When using ftp in some network condition which may exist the slow data transfer situation, please adjust the size of the transport block to get the best results. The default size of 512 bytes, it can achieve high operational efficiency in the most networks.

1.2 Basic System Management Configuration

1.2.1 Configure Ethernet IP Address

monitor#ip address <ip_addr> <net_mask>

This command is used to configure Ethernet IP address. The default value is 192.168.0.1. and the Netmask is 255.255.255.0.

Parameters

Parameter	Description
ip_addr	Ethernet IP address.
net_mask	Ethernet Netmask.

Example

```
monitor#ip address 192.168.1.1 255.255.255.0
```

1.2.2 Configure Default Route

```
monitor#ip route default <ip_addr>
```

This command is used to configure the default route. And it can only configure 1 default route.

Parameters

Parameter	Description
ip_addr	IP address of the gateway.

Example

```
monitor#ip route default 192.168.1.1
```

1.2.3 Test the Network Connection by PING

```
monitor#ping <ip_address>
```

This command is used to test the condition of the network connection.

Parameters

Parameter	Description
ip_addr	Destination IP address

Example

```
monitor#ping 192.168.20.100
```

```
PING 192.168.20.100: 56 data bytes
```

```
64 bytes from 192.168.20.100: icmp_seq=0. time=0. ms
```

```
64 bytes from 192.168.20.100: icmp_seq=1. time=0. ms
```

64 bytes from 192.168.20.100: icmp_seq=2. time=0. ms

64 bytes from 192.168.20.100: icmp_seq=3. time=0. ms

----192.168.20.100 PING Statistics----

4 packets transmitted, 4 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/0

1.3 HTTP Configuration

1.3.1 HTTP Configuration

- Enable http service
- Change the port number of the http service
- Configure the password of the http service
- Specify the access control list for http service

1) Enable http service

By default, http service is disabled.

Use the following command to enable http service under the global configuration mode.

Command	Purpose
Ip http server	Enable http service

2) Change the port number of the http service

By default, the monitoring port number of http service is 80.

Use the following command to change the port number of the http service under the global configuration mode.

Command	Purpose
Ip http port number	Change the port number of the http service

3) Configure the password of the http service

http uses enable password as the access password. If you want to authenticate http access, you need to set the enable password. Use the following command to configure the enable password in the global configuration mode:

Command	Purpose
Enable password {0 7} line	Configure enable password.

4) Specify the access control list for http service

To control the host access http service, specify the access control list for http service. Use the following command to specify the access control list for http service.

Command	Purpose
ip http access-class STRING	specify the access control list for http service

1.3.2 HTTP Configuration Example

Following uses the default port(80) as http service port, and are only allowed to access from 192.168.20.0/24:

➤ ip acl configuration:

```
ip access-list standard http-acl
```

```
permit 192.168.20.0 255.255.255.0
```

➤ global configuration:

ip http access-class http-acl

ip http server

2 Configure the Terminal

2.1 VTY Configuration Description

Use **line** command to configure parameters of terminal simply and flexibly, and the configuration process is suitable for the using habit of customers. The displayed width and height of the terminal can be set by the **line** command.

2.2 Configuration Task

There are 4 types of lines: console, auxiliary, asynchronous and virtual terminal lines. Different systems have different numbers of these lines. Refer to the following software and hardware configuration guide for proper configuration of the device.

Line type	Interface	Description	Number rule
CON(CTY)	Console	Used to login the system to run configure service.	Number 0
VTY	Virtual asynchronous	Used to connect Telnet、X.25 PAD、HTTP and Rlogin of the sync port in the system[like Ethernet or Serial interface]	Number 1~32 from beginning

2.2.1 Relationships between the line and the interface

1) Relationship between Sync interface and VTY line

Virtual terminal lines provide access to the system through a synchronous interface. When a user connects to the system through a VTY line, the user is connecting to a virtual port on an interface. There can be multiple virtual ports for each synchronization interface.

For example, several Telnet connect to 1 interface [Ethernet or serial interface].

The VTY configuration needs to do the following:

- (1) Enter the row configuration mode.
- (2) Configure the terminal parameters.

Refer to the "VTY Configuration Example" section below for the configuration of VTY.

2.3 Monitoring and Maintenance

Use **show line** to check the configuration of VTY.

2.4 VTY Configuration Example

Following configurations will cancel the output line limit per screen of all VTY, and **more** tips will not be prompted:

```
config#line vty 0 32
```

```
config_line#length 0
```

3 Network Management Configuration

3.1 Configure SNMP

3.1.1 Overview

SNMP system includes the following 3 parts:

- SNMP management side (NMS)
- SNMP Agent (AGENT)
- Management Information Base (MIB)

SNMP is the application layer protocol. It provides a message format for communication between the SNMP management side and the agent.

The SNMP management side can be part of the network management system (NMS, such as CiscoWorks). Agents and MIBs reside on the system. To configure SNMP on the system, you need to define the relationship between the management and the agent.

The SNMP agent contains MIB variables that the SNMP management can query or change the value of these variables. The management side can get the value of the variable from the agent, or store the variable value at the agent. The agent collects data from the MIB. The MIB is a repository of device parameters and network data. Agents can also respond to requests from the management side to read or set data. The SNMP agent can actively send traps to the management side. A trap is a message that alerts the SNMP management side to a condition of the network. Traps can indicate incorrect user authentication, reboot, link status (start or shutdown), TCP connection shutdown, loss of connection to neighboring systems, or other important events.

1) SNMP Notice

When a special event occurs, the system can send an inform to the SNMP management side. For example, when the proxy system encounters an error condition, it may send a message to the management side.

SNMP notice can be sent as traps or inform requests. The receiver receives a trap without any response, and then the sender cannot determine whether the trap has been

received, so the trap is unreliable. In contrast, the SNMP management side receiving the inform request uses the SNMP response PDU as the response of the message. If the management does not receive a inform request, it will not send the response. If the sender does not receive the reply, the inform request can be sent again. In this way, the notice is more likely to reach the destination.

Because the inform requests are more reliable, they consume more resources of the system and the network. Traps are discarded as soon as they are issued. In contrast to this, the inform request must remain in memory until a response is received or the request timed out. In addition, the trap can only be sent once, and the inform request can be sent again multiple times. Resend the inform request will increase the network traffic and the load on the network. Thus, traps and inform requests provide a balance between reliability and resources. If the SNMP management need to receive each notice, the inform request can be used; traps can be used if you care about the network traffic or the system's memory and do not have to receive each notification.

Our company's system currently supports traps, and provides an extension of the notification request.

2) SNMP Version

Our company's system support the following SNMP version

- SNMPv1- Simple Network Management Protocol, a complete Internet Standard, defined in RFC1157.
- SNMPv2C- the SNMPv2's community-based management framework, Internet Test Protocol, defined in RFC1901.

Our 3-layer switches also can support following SNMP:

- SNMPv3- Simple Network Management Protocol Version 3, defined in RFC1157.

SNMPv1 uses community-based security. The management group that can access the proxy MIB is defined with an IP address access control list and password.

SNMPv3 can provide authentication and encryption operation for SNMP packets to ensure the safe access to the device.

SNMPv3 provides the following security features:

- Integrity of the Message: Ensure that the message in the transmission process has not been tampered with.
- Authentication: To ensure the legitimacy of the source of the message
- Encryption: Encrypts the message, unauthenticated hosts cannot decrypt even if they got the message.

SNMPv3 provides security models and security levels. A security model is an authentication policy that is implemented by configuring the user name and the group of the user. The security level refers to the different authentication modes supported in the security model. SNMPv3 user-based security model supports three security levels, and in the order from high to low, respectively, is the authentication and encryption, authentication without encryption and not certified. Transfer the summary value of the authentication key which is calculated by MD5 or SHA hash algorithm in the network, and compare them in the SNMP engine to ensure that the password is not released. Use DES encryption algorithm to ensure that the device is not eavesdropped by a third party. The administrator can authenticate the device by configuring the user / password pair and the group where the user belongs to. The access to MIB for different operation of the user can be determined by configuring the group and the view. The group also limits the minimum number of users in the group Security Level.

The agent SNMP must be configured to the SNMP version supported by the management workstation. The agent can communicate with multiple management terminals.

3) Supported MIB

SNMP of the system supports all MIB II variables (described in RFC 1213) and SNMP traps (described in RFC 1215).

Our company supports the private MIB expansion for each system.

3.1.2 SNMP Configuration Task

SNMP configuration task:

- Configure SNMP View
- Create or modify access control for SNMP communities
- Set the system administrator's contact method and the system location
- Define the max length of the SNMP agent packet
- Monitor SNMP status
- Configure SNMP traps

1) Configure SNMP View

The SNMP view is used to specify access to the MIB: include and exclude. Use the following command to configure the SNMP view.

Command	Description
<code>snmp-server view <i>name oid</i> [exclude include]</code>	Add the MIB leaf or table specified by oid to the SNMP view name and specify the access for the object identifier specified by oid in the SNMP view name, exclude to deny access, include to allow access

A subset that can be accessed in the SNMP view removes all objects that are denied access for all MIB objects that are configured to allow access; the object which is not configured cannot be accessed by default.

After you configure the SNMP view, you can apply the SNMP view to the SNMP community name configuration to limit the subset of accessible objects for that community name.

2) Create or modify access control for SNMP communities

Use the SNMP community string to define the relationship between the SNMP management and the agent. The community string is similar to the password which is used to allow the access to the system agent. Optionally, you can specify one or more of the following attributes associated with a community string:

Allow the use of community strings to obtain proxy access to the SNMP manager's IP address access list.

Define a MIB view of all MIB object subsets that have access to the specified community.

Specifies the community's read and write access to MIB objects with access.

In the global configuration mode, use the following command to configure the community string:

Command	Description
snmp-server community <i>string</i> [view <i>view-name</i>] [ro rw] [<i>word</i>]	Define a community access string.

You can configure one or more community strings. Use **no snmp-server community** to remove a given community string.

For community strings configuration, please refer to the chapter "SNMP Commands".

3) Set the system administrator's contact method and the system location

sysContact and **sysLocation** are the administrative variables in the system group in MIB that define the contact ID and the actual location of the node (system) that is being managed. This information can be accessed through the configuration file. Use one or more of the following commands in global configuration mode:

Command	Description
snmp-server contact <i>text</i>	Set the node contact string
snmp-server location <i>text</i>	Set the node location string

4) Define the max length of the SNMP agent packet

When the SNMP agent receives a request or responds, it can set the maximum length of the packet. Use the following command in global configuration mode:

Command	Description
snmp-server packetsize <i>byte-count</i>	Sets the maximum length of the packet.

5) Monitor SNMP status

Use the following command in global configuration mode to monitor SNMP input and output statistics, including illegal community string entries, errors, and the number of requested variables.

Command	Description
show snmp	Monitor SNMP status

6) Configure SNMP traps

Use the following command to configure the system to send SNMP traps (the second task is optional):

➤ Configure the trap sent by system

In the global configuration mode, use the following command to configure the system to send traps to a host.

Command	Description
snmp-server host host community-string [trap-type]	Specifies the recipient of the trap message.
snmp-server host host [traps informs]{version {v1 v2c v3 {auth noauth priv } }}community-string [trap-type]	Specify the recipient of the trap message, and the version number and user name of the trap information. Note: For SNMPv3 traps, you must configure the SNMP engine ID for the host before configuring the host that received the trap.

After the system is powered on, the SNMP agent starts automatically and all types of traps are activated. Use **snmp-server host** to specify the host and which type of trap the host will receive.

Some traps need to be controlled by other commands. For example, if you want to send an SNMP link trap when the interface is open or closed, you need to activate the link trap using **snmp trap link-status** in interface configuration mode. Use the interface configuration command **no snmp trap link-stat** to close these traps.

In order for the host to receive a trap, you must configure the snmp-server host command for that host.

➤ Change trap operating parameters

As an option, you can specify the source interface that generates the trap, and specify the length of the message (packet) queue length or retransmission interval for each host

In the global configuration mode, use the following optional command to change the trap run parameters:

Command	Description
snmp-server trap-source <i>interface</i>	Specifies the source interface that generates the trap message. The command also sets the source IP address for the message.
snmp-server queue-length <i>length</i>	Create a message queue length for each trap host. The default value is 10.
snmp-server trap-timeout <i>seconds</i>	Defines the frequency of retransmission trap messages in the retransmission queue. The default value is 30 seconds.

7) SNMP bind source address

In the global configuration mode, use the following command to set the source address of SNMP packets.

Command	Description
snmp source-addr <i>ipaddress</i>	Set the source address of SNMP packets

3.1.3 Example

```
snmp-server community public RO
```

```
snmp-server community private RW
```

```
snmp-server host 192.168.10.2 public
```

In this example, it configures the community string **public** which have access to read all MIB variables and private which have the access to write all MIB variables. The user can use the community string to read the MIB variables in the system, read the MIB variables in the system and write the MIB variables that can be written in the system. It also specifies that when the system needs to send a trap message, the community string **public** is used to send trap messages to 192.168.20.2. For example, when a port of the system is down, the system will send a linkdown trap message to 192.168.20.2.

3.2 Configure RMON

3.2.1 RMON Configuration Task

Following are the RMON configuration task:

- Configure the rMon alarm function
- Configure the rMon event function
- Configure the rMon statistics function
- Configure the rMon history function
- Display the rMon configuration

1) Configure the rMon alarm function

You can configure the rMon alarm function through the command line or SNMP network management. If you need to configure the SNMP network through the SNMP network management, you need to configure the SNMP of the switch. After the alarm function is configured, the device can monitor some statistics in the system. To configure the rMon alarm function, follow these steps:

Command	Description
configure	Enter the global configuration mode.
rmon alarm index variable interval {absolute delta} rising-threshold value [eventnumber] falling-threshold value [eventnumber] [owner string]	<p>Add a rMon alarm index</p> <p>Index is the index for the entry, the valid range is 1~65535.</p> <p>Variable means that the object of the monitored MIB must be a valid MIB object in the system, and only objects of type INTEGER, Counter, Gauge or TimeTicks can be detected.</p> <p>Interval is the interval of the sampling time, in seconds, the effective range of 1 ~ 4294967295.</p> <p>Use absolute to directly monitor the value of the MIB object; use delta to monitor changes in MIB object values between two samples.</p> <p>Value is used to indicate the threshold at which the alarm is generated, and the corresponding</p>

	<p>eventnumber represents the index of the event that occurs when the threshold is reached; eventnumber is optional.</p> <p>The owner string can be used to describe some of the descriptive information about the alert.</p>
exit	Back to the management mode
write	Save the configuration

After an alarm entry is complete, the device acquires the value of oid specified by variable every interval. It is compared with the previous value according to the alarm type (absolute or delta). If the statistics are larger than the previous value and exceed the rising-threshold, it will raise an event with an index of eventnumber (if eventnumber is zero or the event table does not have an event that is indexed as eventnumber), and if the oid specified by variable is not available, the item status is set to invalid. When you use the **rmon alarm** command to configure the alarm entries with the same index multiple times, only the last configured parameter is valid. Use **no rmon alarm index** to delete the alarm entry with the index.

2) Configure the rMon event function

Configure the rMon event as follows

Steps	Command	Description
1	configure	Enter the global configuration mode.
2	rmon event index [description string] [log] [owner string] [trap community]	<p>Add an rMon event entry.</p> <p>Index is the index of the entry. The valid range is 1 ~ 65535.</p> <p>description represents the description of the event.</p> <p>log indicates that the event is raised in the log table to add a message.</p> <p>trap indicates that a trap will be generated when the event was raised. community is the community name.</p> <p>owner string can be used to describe some descriptive information about the event.</p>
3	exit	Back to the management mode
4	write	Save the configuration

After the rMon event is configured, the eventLastTimeSent field of the event entry is updated to the sysUpTime when the rMon alarm is triggered. If the event is configured with the log attribute, add one information list to the log table. If the trap attribute is configured, send a trap by community. When the rmon event command is used to configure the event entry with the same index multiple times, only the last configured parameter is valid. Use **no rmon event index** to delete the event entry whose index is index.

3) Configure the rMon statistics function

The rMon statistics group is used to monitor the statistics on each interface on the device. RMon statistics function configuration steps are as follows:

Steps	Command	Description
1	configure	Enter the global configuration mode.
2	interface iftype ifid	Enter the interface mode. Iftype is the type of the interface. Ifid is the id for the interface.
3	rmon collection stat index [owner string]	Enable the statistics function on the interface. Index is the index of the statistics entry. owner string can be used to describe some descriptive information about the statistics table.
4	exit	Back to the global configuration mode.
5	exit	Back to the management mode
6	write	Save the configuration

When you use **rmon collection stat** to configure the event table entry with the same index multiple times, only the last configured parameter is valid. Use **no rmon collection stats index** to delete the entry whose index is index.

4) Configure the rMon history function

The RMON history group collects statistics for different time periods on an interface on the device. Following are the rMon history function configuration:

Steps	Command	Description
1	configure	Enter the global configuration mode.
2	interface iftype ifid	Enter the interface mode. Iftype is the type of the interface. Ifid is the id for the interface.
3	rmon collection history index [buckets bucket-number] [interval second] [owner owner-name]	Enable the history function on the interface. Index is the index of the history entry. In all data collected by this history control entry, the latest bucket-number entry needs to be retained. Users can view the Ethernet history table to get these statistics. The default value is 50. second is the interval for obtaining statistics every two times. The default value is 1800 seconds (half an hour). owner string can be used to describe some descriptive information about the statistics table.
4	exit	Back to the global configuration mode.
5	exit	Back to the management mode
6	write	Save the configuration

After adding a history control entry, the device gets the statistics from the specified interface every second and adds the result as an entry to the Ethernet history table. When you use **rmon collection history index** to configure the history entry of the same index multiple times, only the last configured parameter is valid. Use **no rmon history index** to delete the index control entry whose index is index. Note that the bucket-number is too large and the interval second is too small will occupy too much system resources.

5) Display the rMon configuration

Use **show** command to display the rMon configuration.

Command	Description
show rmon [alarm] [event] [statistics] [history]	Display rmon configuration information

	<p>alarm indicates the configuration for alarm entry.</p> <p>event indicates the configuration for event entry and also displays the entry caused by that the event is be raised.</p> <p>statistics indicates the configuration for statistic entry and also display the statistic collected on the interface.</p> <p>history indicates configuration for history entry and also display the latest statistics collected on the interface in specified intervals.</p>
--	---

3.3 Configure PDP

3.3.1 Overview

The PDP protocol is the two-layer protocol used to discover the network device and help management program to discover all the neighbors of the known device. Use PDP to learn the device type and the SNMP agent address of the neighbor device. The neighbor device is discovered by PDP, and the network management program can query the neighbor device with SNMP to obtain the network topology.

PDP can discover the neighbor device, but cannot accept the SNMP to query neighbor device. Therefore, the switch can only be at the edge of the network. Otherwise, the complete network topology cannot be obtained.

PDP on the switch can be configured on all SANPs (such as Ethernet).

There are several switches that currently support PDP:

S2008/S2026B/S2116/S2224D/S2224M/S2226/S2448/S3224/S3224M/S3424/S3448/S3512/S3524

3.3.2 PDP Configuration Task

- Default PDP configuration
- Configure PDP clock and information save time
- Configure PDP version
- Enable PDP

- Enable PDP on port
- Monitor and manage PDP

1) Default PDP configuration

Function	Default
PDP global configuration	Disable
PDP port configuration	Disable
PDP clock (frequency of sending message)	60s
Save PDP information	180s
PDP version	2

2) Configure PDP clock and information save time

When setting the frequency of PDP sending messages and saving PDP information, you can use the following command in global configuration mode:

Command	Description
pdp timer <i>seconds</i>	Set the frequency for PDP sending message
pdp holdtime <i>seconds</i>	Set the time for saving PDP information

3) Configure PDP version

Use the following command to set PDP version in global configuration mode.

Command	Description
pdp version {1 2}	Set PDP version

4) Enable PDP

PDP is not enabled on the default configuration. You can use the following command to enable PDP.

Command	Description
pdp run	Enable the PDP on the switch

5) Enable PDP on port

PDP is not enabled in the default configuration. Use the following command in interface configuration mode to enable PDP on the port, after enabling PDP on the switch:

Command	Description
pdp enable	Enable PDP on the port

6) Monitor and manage PDP

Use the following command to monitor PDP.

Command	Description
show pdp traffic	Display the count of receiving and sending PDP packet by the switch
show pdp neighbor [detail]	Display the neighbors discovered by PDP

3.3.3 Example for PDP Configuration

Example 1: Enable PDP

```
config# pdp run
```

```
config# int f0/0
```

```
config_f0/0#pdp enable
```

Example 2: Configure PDP clock and information save time

```
config#pdp timer 30
```

```
config#pdp holdtime 90
```

Example 3: Configure PDP version

```
config#pdp version 1
```

Example 4: Monitor PDP information

```
config#show pdp neighbors
```

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater

Device ID Local Intrfce Holdtme Capability Platform Port ID

joe Eth 0 133 4500 Eth 0

sam Eth 0 152 R AS5200 Eth 0

4 SSH Configuration

4.1 SSH Overview

4.1.1 SSH server

The SSH client connect the device safely and securely through the SSH server. This connection provides the function similar with telnet. SSH server supports encryption algorithms including des, 3des and blowfish.

4.1.2 SSH client

SSH client is running on the SSH protocol, and provide authentication and encryption. Because using authentication and encryption, the SSH client allows secure communication between the communication devices or between other devices that support the SSH server in an insecure network environment. SSH client supports encryption algorithms including des, 3des and blowfish.

4.1.3 Implement Features

ssh server and ssh client support ssh version 1.5. It only supports shell.

4.2 Configuration Task

4.2.1 Configure Authentication Methods List

SSH server use login authentication and the default name of authentication methods list is "default".

Command	Description
Ip sshd auth_method STRING	Configure authentication methods list

4.2.2 Configure Access Control List

To control the access to ssh server of the device, you can configure access control list for ssh server. Use the following command to configure in global configuration mode.

Command	Description
Ip sshd access-class STRING	Configure access control list

4.2.3 Configure the timeout for authentication

After the client and server establish the connection, if the server cannot pass the authentication within the set time, the server will close the connection.

Use the following command to configure the access control list in global configuration mode.

Command	Description
Ip sshd timeout <60-65535>	Configure the timeout for authentication

4.2.4 Configure the number of authentication retries

When the user authentication fails and exceed the maximum of authentication times, the SSH server does not allow the user to continue again, unless the connection is restarted. It can retry 3 times by default.

Use the following command to configure the maximum number of retries in the global configuration mode:

Command	Description
Ip sshd auth-retries <0-65535>	Configure the maximum of

4.2.5 Enable SSH server

The SSH server is enabled by default. When enable the SSH server, the device generates an rsa key pair and then monitor the connection requests from the client. This process takes about one or two minutes.

Use the following command to enable SSH server in the global configuration mode:

Command	Description
Ip sshd enable	Enable ssh server. The bits number of the key is 1024.

4.3 Example for ssh server Configuration

The following configuration only allows hosts with IP 192.168.20.40 to access the ssh server and use the local user database to identify the user.

4.3.1 Access Control List

```
ip access-list standard ssh-acl
```

```
permit 192.168.20.40
```

4.3.2 Global Configuration

```
aaa authentication login ssh-auth local
```

```
ip sshd auth-method ssh-auth
```

```
ip sshd access-class ssh-acl
```

```
ip sshd enable
```