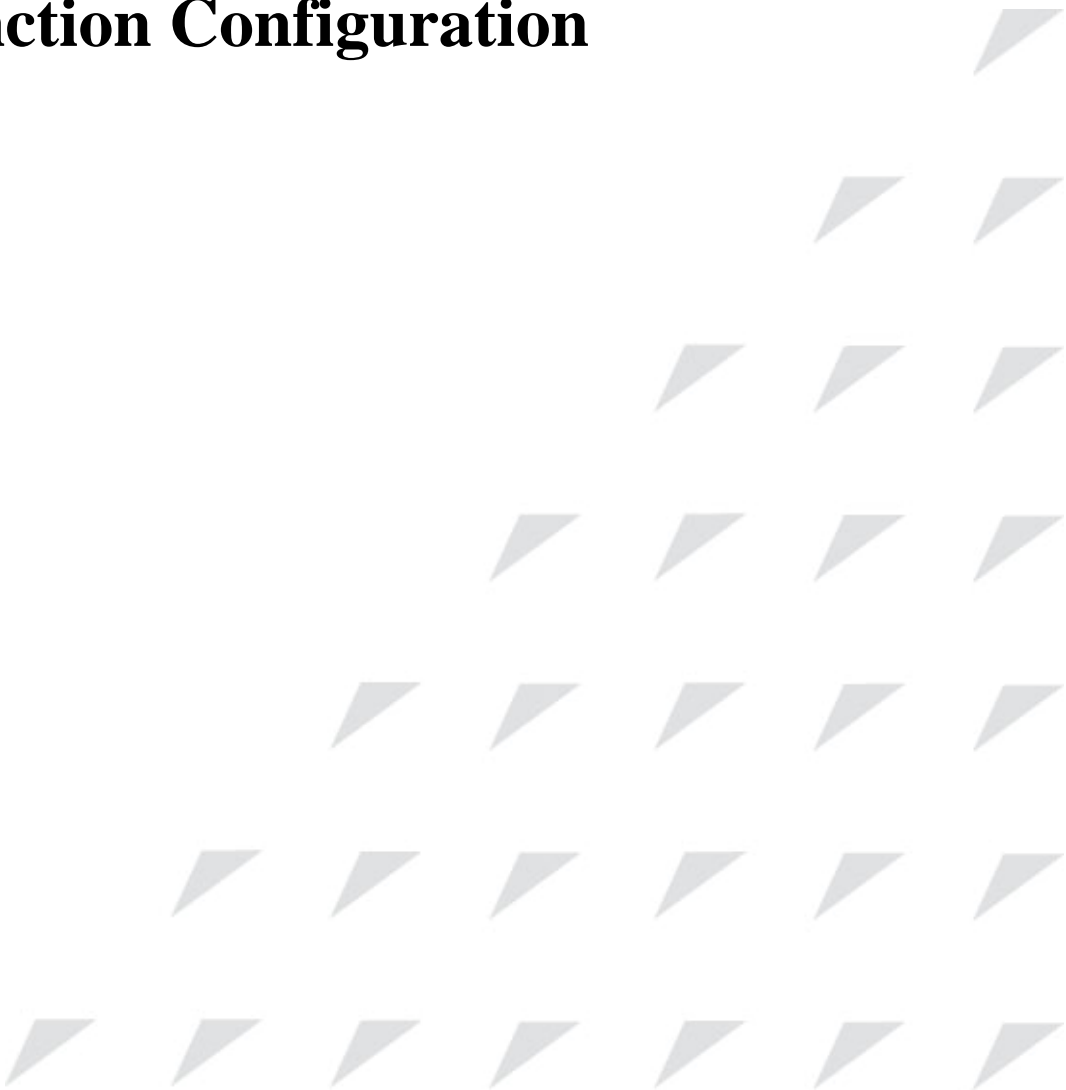


www.raisecom.com

System Function Configuration



Legal Notices

Raisecom Technology Co., Ltd makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. **Raisecom Technology Co., Ltd** shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty.

A copy of the specific warranty terms applicable to your Raisecom product and replacement parts can be obtained from Service Office.

Restricted Rights Legend.

All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of **Raisecom Technology Co., Ltd.** The information contained in this document is subject to change without notice.

Copyright Notices.

Copyright ©2006 Raisecom. All rights reserved.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in Writing from **Raisecom Technology Co., Ltd.**

Trademark Notices

RAISECOM is the trademark of Raisecom Technology Co., Ltd.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Windows® 2000 is a U.S. registered trademark of Microsoft Corporation.

Windows® XP is a U.S. registered trademark of Microsoft Corporation.

Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

Contact Information

Technical Assistance Center

The Raisecom TAC is available to all customers who need technical assistance with a Raisecom product, technology, or, solution. You can communicate with us through the following methods:

Add: 1120, Haitai Tower, 229 Fourth North Loop Middle Road, Haidian District, Beijing 100083

Tel: +86-10-82884499 Ext.878 (International Department)

Fax: +86-10-82885200, +86-10-82884411

World Wide Web

You can access the most current Raisecom product information on the World Wide Web at the following URL:

<http://www.raisecom.com>

Feedback

Comments and questions about how the NView iEMS system software works are welcomed. Please review the FAQ in the related manual, and if your question is not covered, send email by using the following web page:

<http://www.raisecom.com/en/xcontactus/contactus.htm>.

If you have comments on the NView iEMS specification, instead of the web page above, please send comments to:

export@raisecom.com

We hope to hear from you!

CONTENTS

Chapter 1	System Overview	8
Overview		错误！未定义书签。
Function feature		错误！未定义书签。
Caption 2		错误！未定义书签。
Caption 3		错误！未定义书签。
Chapter 2	System Operation	错误！未定义书签。
Overview		错误！未定义书签。
System installation		错误！未定义书签。
System activation		错误！未定义书签。
Shutdown system		错误！未定义书签。
System Upgrade		错误！未定义书签。
System maintain		错误！未定义书签。
Chapter 3	System Security Management	错误！未定义书签。
Overview		错误！未定义书签。
User management		错误！未定义书签。
User group management		错误！未定义书签。
Management domain management		错误！未定义书签。
Operation log management		错误！未定义书签。
Influence on Device Configuratin Operations		错误！未定义书签。
Influence on operations		错误！未定义书签。
Chapter 4	System Overview	错误！未定义书签。
Appendix A	Abbreviation	错误！未定义书签。
Appendix B	FAQ	错误！未定义书签。
Index		错误！未定义书签。



Preface

About This Manual

This manual introduces primary functions of the configuration management software for RC series products.

Who Should Read This Manual

Sales and marketing engineers, after service staff and telecommunication network design engineers could use this manual as a valuable reference. If you want to get an overview on features, applications, architectures and specifications of Raisecom RC series integrated access devices, you could find useful information in this manual as well.

Compliance

The RC series products developed by Raisecom are strictly complied with the following standards as well as ITU-T, IEEE, IETF and related standards from other international telecommunication standard organizations:

YD/T900-1997 SDH Equipment Technical Requirements - Clock

YD/T973-1998 SDH 155Mb/s and 622Mb/s Technical conditions of optical transmitter module and receiver module

YD/T1017-1999 Network node interface for the Synchronous Digital Hierarchy (SDH)

YD/T1022-1999 Requirement of synchronous digital hierarchy (SDH) equipment function

YD/T1078-2000 SDH Transmission Network Technique Requirements-Interworking of Network Protection Architectures

YD/T1111.1-2001 Technical Requirements of SDH Optical Transmitter/Optical Receiver Modules——2.488320 Gb/s Optical Receiver Modules

YD/T1111.2- 2001 Technical Requirements of SHD Optical Transmitter/Optical Receiver Modules——2.488320 Gb/s Optical Transmitter Modules

YD/T1179- 2002 Technical Specification of Ethernet over SDH

G.703 Physical/electrical characteristics of hierarchical digital interfaces

G.704 Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels

G.707 Network node interface for the synchronous digital hierarchy (SDH)

G.774 Synchronous digital hierarchy (SDH) - Management information model for the network element view

G.781 Synchronization layer functions

G.783 Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks

G.784 Synchronous digital hierarchy (SDH) management

G.803 Architecture of transport networks based on the synchronous digital hierarchy (SDH)

G.813 Timing characteristics of SDH equipment slave clocks (SEC)

G.823 The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy

G.825 The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)

G.826 End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections

G.828 Error performance parameters and objectives for international, constant bit-rate synchronous digital paths

G.829 Error performance events for SDH multiplex and regenerator sections

G.831 Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)

G.841 Types and characteristics of SDH network protection architectures

G.842 Interworking of SDH network protection architectures

G.957 Optical interfaces for equipments and systems relating to the synchronous digital hierarchy

G.691 Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers

G.664 Optical safety procedures and requirements for optical transport systems

I.731 ATM Types and general characteristics of ATM equipment

I.732 ATM Functional characteristics of ATM equipment

IEEE 802.1Q Virtual Local Area Networks (LANs)

IEEE 802.1p Traffic Class Expediting and Dynamic Multicast Filtering

IEEE 802.3 CSMA/CD Access Method and Physical Layer Instruction

Chapter 3 System Function Configuration

3.1 File Management

3.1.1 Profile Management

The default configuration storage file name of the system is **:startup_config.conf**. The configuration storage file could be written into the flash file system through the command **write**, and the configuration information will be re-configured automatically the next time the system reboot. Use **erase** to delete the file. The configuration information file **startup_config.conf** could be uploaded to the server or downloaded to the system to replace the original configuration information, through FTP protocol with the command **upload** and **download**. Use **show startup-config** to show the configuration information in storage. Use **show running-config** to show the current configuration information in the system.

Command	description
write	write the configuration file into the flash file system, and the configuration information in storage will be re-configured automatically after the system rebooting
erase	delete the file
show startup-config	the configuration information in storage
show running-config	The configuration information in the current system

3.1.2 BOOTROM file management

BOOTROM, boot of the switch, initialize the switch. User can upgrade BootROM file through FTP. BootROM file system is called **bootrom**(or **bootromfull**) in default cases. With the command **ftp file-name**, user can set these file system names.

When powered, the switch will run **BootROM** file first. When 'Press space into Bootrom menu...' is shown, user can enter **Bootrom** menu bar by pressing ENTER, and carry out the following operation:

'?' show all the commands available

'h' show all the commands available

'v' show the version of **Bootrom**

'b' quick start executive command

'T' download configuration file through the switch ports

'N' set the MAC address

'R' reboot the switch

System File Management

The documents that keep the equipment running, like host software and configuration files, are kept in the storage devices. For the convenience and efficiency of user's managing the equipment, the equipment manage the documents in the way of Document System. The function of the document system contains catalog's creating and deleting, document's copying and display, and so on. In default cases, the document system will remind user for confirmation if the command may lose any data(like deleting or recovering files).

- With the command **upload** and **download**, program files could be uploaded to the server or downloaded to the system through the TFTP protocol or FTP protocol;
- Use **dir** to look over the system FLASH files;
- Use **show version** to look over the software version;
- Use **clock** to set system time;
- Use **logout** to exit the current system.

Command	Description
dir	To look over the system files
show version	To look over the software version
clock	To set system time
logout	exit

3.1.4 FPGA files management

FPGA(field programmable gate arrays) is the most integrated in Application Specific Integrated Circuit(ASIC). To accomplish user's logic, subscriber can re-configure the logical module and I/O module in FPGA, which can also be used on CPU's simulation. User's programming data to FPGA, stored in FLASH chip, could be uploaded to FPGA when powered and initialized. Online-programming is also available, making the system reconstructed online.

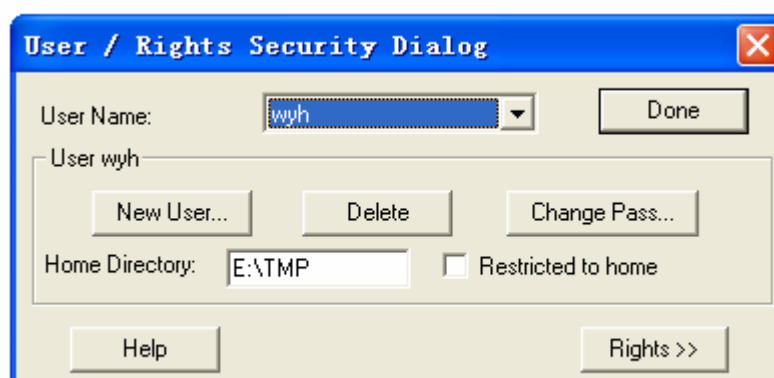
When powered, the FPGA chip will write the data in EPROM into programming ROM and get into working state after the configuration finished. When power off, FPGA will be empty and the logic inside is gone, thus FPGA could be repeated used. There is no special programmer for FPGA programming, the universal EPROM, PROM programmer can fit it. When the function of FPGA needs to be modified, only on piece of EPROM needs to be changed. So, by one FPGA different programming data brings different circuit function.

命令	描述
Upload	Files are uploaded to server
{system-boot startup-configure remote-fpga } ftp A.B.C.D	through FTP protocol
username password filename	A.B.C.D:IP destination address

	username server user name
	password user's password
	filename filename(o.0)
download {system-boot startup-configure bootstrap remote-fpga} ftp A.B.C.D username password filename	By FTP protocol the files are downloaded to the system and replace the files before. A.B.C.D:IP destination address username server user name password user's password filename filename(o.0)
upload {system-boot startup-configure remote-fpga } tftp A.B.C.D filename	Files are uploaded to server through FTP protocol A.B.C.D:IP destination address filename filename
download {system-boot startup-configure remote-fpga } tftp A.B.C.D filename	Files are uploaded to server through FTP protocol A.B.C.D:IP destination address filename filename

A typical configuration example

When subscriber has already have his/her own configuration files or new upgrade files, he/she can download the configuration files into the switch. To make it, subscriber should open the FTP software, like wftpd32.exe, and set user name, password and file path. As shown below, user name is wyj, password:123, the path of the configuration file is E:\TMP.



User uses serial line to connect the switch and PC, and connect the line to the switch port, as shown below. Open the terminal emulation program, such as **SecureCRT 5.1**. Take Console management as reference when using Console interface.



User can also use **Upload, download** to upload and download files from FTP. The connection line is shown as figure.

For example:

Using FTP to download system file **ROS_4.3.313.ISCOM2926.31.20080602** to the switch, user should set the switch IP address:20.0.0.10 first, then open the FTP software **wftpd32.exe** and set user name, password, and file path. Input **download** and select **system-boot**, input the host IP address: 20.0.0.10, user name, password of the FTP software, and all the process is done.

```
Raisecom#config
```

```
Raisecom(config)#interface ip 0
```

```
Raisecom(config-ip)#ip address 20.0.0.10 1
```

Set successfully

```
Raisecom(config-ip)#exit
```

```
Raisecom(config)#exit
```

```
Raisecom#download startup-config ftp 20.0.0.221 wyh 123
```

```
ROS_4.3.313.ISCOM2926.31.20080602
```

Waiting....Start

Getting from source ...Done

Writing to destination...Size 1754K / 1754K

Success!

When the files in switch need to be uploaded to the host, user can use TFTP to upload **startup-config** to the host. To do this, user should set the IP address 20.0.0.10 of the switch, then open the TFTP software **Cisco TFTP Server** to set the file path, input **upload**, host IP address 20.0.0.221, and upload the generated file name WW.

```
Raisecom#config
```

```
Raisecom(config)#interface ip 0
```

```
Raisecom(config-ip)#ip address 20.0.0.10 1
```

Set successfully

```
Raisecom(config-ip)#exit
```

```
Raisecom(config)#exit
```

```
Raisecom#upload startup-config tftp 20.0.0.221 ww
```

Waiting....Start

Getting from source ...Done

Writing to destination...Size 1K / 1K

Success!

3.2 Switch Management

3.2.1 Console Management

Local control port management means using a console port of a terminal or a PC that is running terminal simulation program to configure and manage the switch. This management approach is out-of-band management, and needs no network for communication. Thus the console port can configure and manage the switch even if the network is not going on well.

Local management manage the switch by connecting the terminal and console program inside the switch.

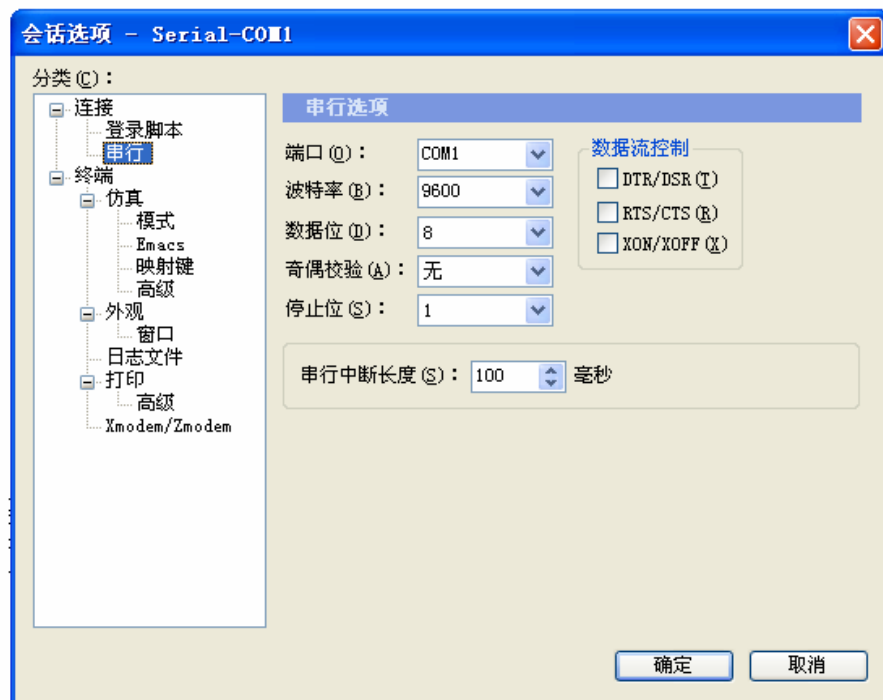
To login in the Ethernet switch through the console port, the user's terminal communication parameter configuration and the configuration of switch's console port should be consistent. The default configuration of the switch's console port is shown below

属性	缺省值
波特率	9600bit/s
流控方式	不进行流控
校验方式	无校验位
停止位	1
数据位	8

First, connect the switch console port and the serial port of PC, and keep the PC online. As shown below,



Then, run the terminal simulation program on PC, such as **SecureCRT 5.1**, as is shown below. Select the serial port connected with the switch port, and configure the terminal communication parameter as: baud rate 9600 bit/s, 8 data bits, 1 stop bit, no validation and flow control, serial interrupted default value 100ms.



At last, download the system files to the switch and run it through console port. The calculation of the switch data can also be observed and controlled by computer.

3.2.2 telnet management

The TELNET protocol aims at offering a communication mechanism which is generally universal, two-way and 8 byte available. Its main objective is letting terminal interface device and the process for terminal interact. In addition, as you can see, the protocol could be used in terminal communication (connection) and process to process communication(distributed computing).

A general thought: a telnet connection is a connection which is used to transfer TCP that contains TELNET control data.

TELNET protocol base on the following 3 ideas mainly: first, virtual network terminals; second, the principle of negotiating options; third, viewing the terminal and process as a balanced approach.

User can make remote management and maintenance through Telnet. Both switch client and telnet client need corresponding configuration so that user can login in the switch by Telnet.

When user login on a switch, the picture following shows the detail:



User can start TELNET services by command..

step	command	description
1	config	Enter global configuration mode
2	interface ip 0	Enter IP port mode

3	ip address A.B.C.D [A.B.C.D] <1-4094>	Configure the IP address A.B.C.D IP address [A.B.C.D] subnet mask <1-4094> vlan number
4	exit	Exit global configuration mode and enter enable mode
5	telnet-server {accept close max-session}port-list	Set telnet services port-list port list
6	show telnet-server	Show telnet configuration

3.2.3.2 SSH default configuration

function	Default value
SSH server status	Stop
Key-pair	No

3.2.3.3 SSH configuration

Before the server start key-pair have to be created. User manage command creating and key-pair deletion by key-pair. User use keys to create command and key-pair, before new key-pair is created, user must delete the key-pair that existed, because only one key-pair can be created on one equipment.

step	Command	description
1	config	Enter global configuration mode
2	key-pair generate KEYNAME rsa [modulus <768-2048>] [comment COMMENT]	Create key pair KEYNAME key-pair name 768-2048 range of the module length COMMENT key-pair comment
3	ssh server KEYNAME	Start SSH server KEYNAME key-pair name
4	exit	Return to global configuration mode
5	show key-pair KEYNAME	Show key-pair information

User can use **no ssh server** to stop SSH server after the SSH server start.

The key-pair will be stored on the equipment automatically after successful creation, until user delete it or the equipment is formatted.

Step	Command	Description
1	config	Enter global configuration mode
2	key-pair destroy KEYNAME	Destroy key-pair

3	exit	Return to global configuration mode
4	show key-pair KEYNAME	Show key-pair information

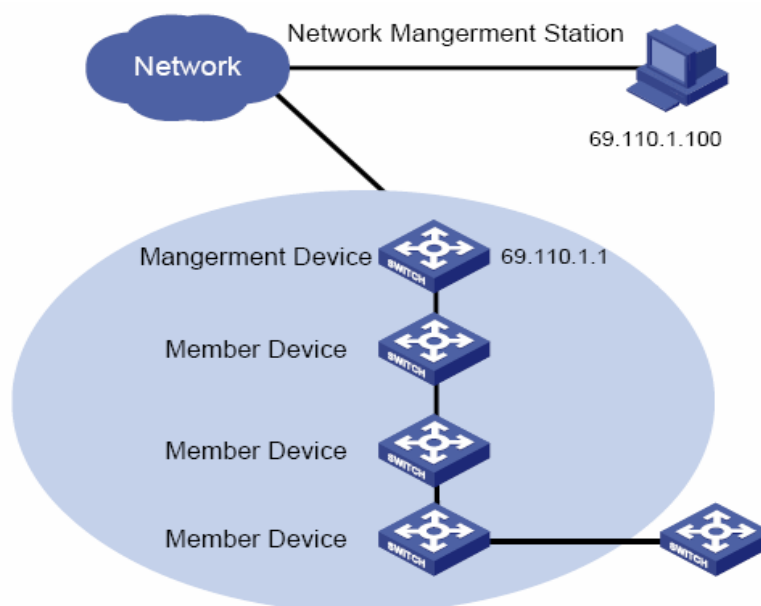
Monitoring And Maintaining

Command	Description
show key-pair KEYNAME	Show key-pair information
show ssh server	Show server configuration information
show ssh session	Show SSH dialog information

Cluster 'rcommand' Management

Cluster 'rcommand' Function Introduction

Using Raisecom cluster management function, network administrator is able to manage several switch through a registered IP address of the main switch. The main switch is command facility, while the other switches that are under administration will be member equipments. Member equipment needs not IP address setting usually, it is managed and maintained by manage equipment's redirection. The typical using environment is shown below:



Cluster management contains three protocol: RNDP (Raisecom Neighbor Discover Protocol), RTDP (Raisecom Topology Discover Protocol) and RCMP (Raisecom Cluster Management Protocol). RNDP see to the facility neighbor discovery and information collection, RTDP see to collecting and handling all the network topology information, while RCMP see to the cluster member's joining, validation, deletion and so on. Among them, RTDP and RCMP communicate in cluster VLAN. So, appropriate configuration to VLAN2 is needed to make sure that RTDP and RCMP communicate normally, when there be facility that does not support Raisecom cluster management function between the two facilities that need cluster management.

Different roles form by the different degrees and functions of each switch in the cluster, but user can constitute a certain switch's role form configuration. The roles in cluster include supervisory unit, member

unit and alternate unit.

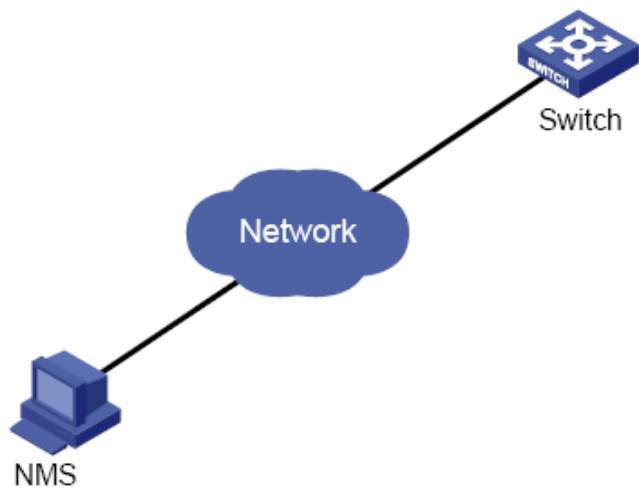
Rcommand, like telnet, can login member switch on the command-line interface of the supervisor switch. Consult cluster management function about configuration and commands of cluster management.

3.2.5 NMS Management

NMS: Network Management System. It has 5 functions: alarming, performance, configuration, safety and accounting. In SNMP, NMS is the workstation running the client program. IBM NetView and Sun NetManager are the usual NMS stations in use. When SNMP Agent receives the query message Get-Request, Get-Next-Request, Get-Bulk-Request about MIB from NMS, Agent carry out **read** or **write** to MIB according to the message style, then create **Response** message according to the operation result and sent it to NMS as response.

On the other side, once SNMP Agent receives any change on facilities like normal/hot booting or anything unusual it will create a **Trap** message and report it to NMS actively.

User can login the switch through NMS, manage and configure the switch by the Agent process on the switch. As shown below.



3.2.6 User Logging Management

User can login, configure and manage the switch by the following way:1, local login from Console port;2, local or remote login using Telnet through Ethernet port;3, login from NMS port. User’s name and password is needed when logging, by default username is **raisecom**, password **raisecom**..

Setp	Command	Description
1	user USERNAME password { no-encryption md5 } PASSWORD	User login USERNAME username; PASSWORD password;
2	user USERNAME privilege <1-15>	User login privileges; USERNAME username; <1-15> user privileges grade;

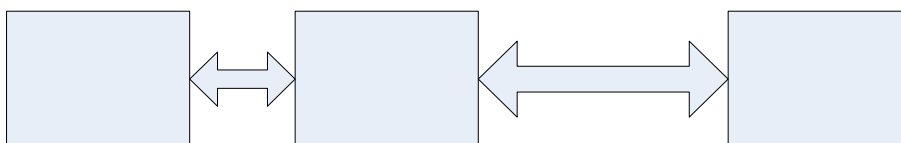
3	Write	Save configuration information
4	show user	Show user information

3.2.7 Expended OAM Management

Expended OAM, by IEEE802.3ah OAM link, manage and monitor remote facilities. It contains 3 parts of function:1,aquire and set remote facilities;2, download and upload remote facility files;3, manage the expended OAM line state and stat.. Specific functions are as follows:

- ✓ Remote attribution acquirement: local facility can get remote facilities' attribution, configuration and statistics.
- ✓ Configuring remote facility basic function: local facility could configure remote facility function by expending OAM, including host name, port enable/disable, port speed duplex, port bandwidth, failover and so on.
- ✓ Configuring remote facility management parameter: configure network administration parameter for remote facility that support SNMP network administration, like IP address, gateway, group parameter and VLAN management, and carry out comprehensive network management through SNMP protocol.
- ✓ Remote TRAP: when remote facilities find **LINK UP/DOWN** port, the remote port will inform local port by sending expended OAM **notification** frame, then the local port will send remote TRAP alarm to network administrator.
- ✓ Expended remote end loopback: the local end is able to manage remote fiber port inner loop function, and set the loopback data to decide if CRC needs re-computing.
- ✓ Resetting remote facilities: orders from local end is able to reset or reboot remote facilities.
- ✓ Other remote facilities' function management: as remote facilities increases, local facility can manage more remote end functions by expend OAM protocol, like SFP, Q-in-Q, virtual line diagnoses and so on.
- ✓ Downloading remote end files: remote end files could be downloaded to remote facilities directly from FTP/TFTP server, another way is downloading them from server to local end, then to the remote facilities.
- ✓ Uploading remote end files: remote end files could be uploaded to remote facilities directly from FTP/TFTP server, another way is uploading them from server to local end, then to the remote facilities.
- ✓ Expended OAM line stat. and function management.

Expended OAM network is shown as below. Local switch MASTER:ISCOM2828F; remote end SLAVE: RC552-GE.



Notice:

- The expended OAM line could be established only between the local facility and remote facility, that is to say, the facility on each end must be OAM active mode and OAM passive mode respectively.

3.3 Keepalive Function

3.3.1 The Introduction To Keepalive Principle

To find out the facility out of order in time, user needs to acquire the facility information periodically to see if the facility is available and the basic facility information. Users can receive the state of **Keepalive Trap** information collection facility from NMS periodically without any operation. Keepalive module send TRAP periodically to NMS about the basic information of facilities, including facilities' name, facilities' OID, the hardware and software version, MAC address and IP address.

Keepalive module send **keepalive trap** that contains the basic information of the switch to the network administration station, so that the network administration station could find the switch in a short time.

3.3.2 Keepalive Default Configuration

Function	Default value
keepalive trap switch	On
Keepalive alternation	300 seconds

3.3.3 Keepalive Configuration

By default, KEEPALIVE is open on the switch, and the switch send KEEPALIVE trap periodically. By carrying out the following command in global configuration mode, KEEPALIVE can be set OPEN, CLOSE and PAUSE. If it is CLOSE, the configuration can be loaded. And if it is PAUSE, the configuration can not be saved, the configuration is still default after reboot..

Step	Command	Description
1	config	Enter configuration mode
2	interface ip 0	Enter IP port mode
3	ip address A.B.C.D [A.B.C.D] <1-4094>	Configure the IP address of the switch A.B.C.D IP address [A.B.C.D] subnet mask <1-4094> vlan number
4	exit	Quit global configuration mode and enter privileged EXEC mode
5	snmp-server host A.B.C.D version 3 { noauthnopriv authnopriv } NAME [udpport <1-65535>] [bridge] [config] [interface] [rmon] [snmp] [ospf]	Configure SNMPv3 Trap the destination host A.B.C.D IP address NAME SNMPv3 team name <1-65535> the UDP port number which the destination use to receive TRAP
6	snmp-server keepalive-trap interval <120-28800>	Set he interval time fo the switch sending KEEPALIVE-TRAP to SNMP network administration station <120-28800> the interval range, the unit is second
7	snmp-server keepalive-trap { enable disable pause }	Start, close, pause sending keepalive trap
8	exit	Return to privileged EXEC mode
9	show snmp config	Show basic SNMP configuration

3.3.4 Monitoring And Maintenance

Show is used to show switch the operation and configuration for maintenance and monitoring. To do this, the following **show** command is available:

Command	Description
<code>show snmp config</code>	Show the basic configuration of SNMP

3.3.5 An Example Of Typical Configuration



As is shown above, set the IP address as 20.0.0.10 first, then configure the SNMPv2c Trap destination host address: add a **host_1** host address, username public, SNMP version v2c, all trap, set the interval time 500S of the switch sending **keepalive-trap** to SNMP network administration station, open **keepalive trap**, show basic SNMP information at last.

```
Raisecom#config
Raisecom(config)# int ip 0
Raisecom(config-ip)#ip address 20.0.0.10 1
Raisecom(config-ip)#exit
Raisecom(config)#snmp-server host 20.0.0.221 version 2c public
Raisecom(config)#snmp-server keepalive-trap interval 500
Raisecom(config)#snmp-server keepalive-trap enable
Raisecom(config)# show snmp config
```

3.4 Task Scheduling Function

3.4.1 The Introduction To Task Scheduling Function Principle

The function is to carry out certain command periodically and maintain the switch configuration function seasonally. By configuring time list a time attribution list could be found, including start time , periodically time and end time. There are two kinds of time attribution, one begins when the switch starts, which is relative time; the other is the normal time, including year, month, day and so on, which is absolute time.

3.4.2 Task Scheduling Configuration

1. Setting task schedule:

Step	Command	Description
1	config	Enter global configuration mode

2	schedule-list list-no start { up-time days time [every days time [stop days time]] date-time date time [every { day week days time } [stop date time]]}	Add or modify sechedule-list table. The command set the beginning time and end time of scheduling task, and the cycling interval. list-no : the range of scheduling list number<0-99>; days time : from the start-up time start, it is relative time; input format days: <0-65535>, time: HH:MM:SS such as 3 3:2:1 date time : the calculation of time is in accordance with the system data, it is absolute time; input format: MMM-DD-YYYY HH:MM:SS like jan-1-2003 or 1-1-2003, the range of YYYY is from 1970 to 2199.
3	<i>command-string</i> schedule-list <i>list-no</i>	Add the commands that support schedule-list to the scheduling list. <i>command-string</i> <i>command</i> <i>string</i> . <i>list-no</i> <i>list number</i> <i>range</i> <0-99>
4	show schedule-list	Show schedule-list configuration。

3.4.3 Monitoring And Maintaining

Command	Description
show schedule-list	Show schedule-list configuration

3.4.4 Typical Configuration

First, add a **schedule-list** table, **List number:** 1, the beginning time is Feb-2-2004 0:0:0 according to system date, and perform every six days, while the terminal time is Feb-2-2005. Then, add the commands that support **schedule-list** to schedule list, and show the **schedule-list** configuration at last.

```
Raisecom#config
Raisecom(config)#schedule-list 1 start date-time Feb-2-2004 0:0:0 every 6 0:0:0 stop Feb-2-2005 0:0:0
Raisecom(config)#storm-control dlf schedule-list 1
Raisecom(config)#exit
Raisecom# show schedule-list
```

3.5 Fault Location

Fault Location Principle

When anything abnormal happened in the system, fault location can be carried out by examining the facilities' running information, which includes the following contents:

- 1 RAM using;
- 2 port driver;
- 3 process and stack state;
- 4 port UP/DOWN statistics;
- 5 the information needed for fault location.

3.5.2 Memory Show

Command	Description
show memory	Show the memory state

3.5.3 Port Driver Memory Pool Show

Command	Description
show buffer [port <1-26>]	Show the port driver pool state; <1-26> port range

3.5.4 Port UP/DOWN History

Command	Description
show diags link-flap	Show the UP/DOWN statistics

3.5.5 Fault Location Information Summarize Show

Command	Description
show tech-support	Show the fault location information summarize.

This command shows the information summarize for fault location, including:

- 1 version (**show version**)
- 2 running configuration information (**show running-config**)
- 3 current CPU utilization (**show cpu-utilization**)
- 4 memory usage (**show memory**)
- 5 port driver pool usage (**show buffer**)
- 6 processes (**show processes**)
- 7 files in flash (**dir**)
- 8 current system time (**show clock**)
- 9 interface port state (**show interface port**)
- 10 interface port statistics (**show interface port statistics**)
- 11 port **UP/DOWN** statistics (**show diags link-flap**)
- 12 SNMP statistics (**show snmp statistics**)
- 13 spanning-tree in general (**show spanning-tree**)
- 14 vlan statistics (**show vlan static**)
- 15 ARP (**show arp**)
- 16 trunk (**show trunk**)
- 17 TCP link state

3.6 Ping Diagnose Function

3.6.1 Ping Principle

Ping is the most frequently-used command for troubleshooting, which is usually used to test if the link between the two hosts works. **Ping** is carried out by ICMP ECHO messages usually. It is made of ICMP reply and questioning messages, and if the network works well a reply messages will be received.

Ping can also be carried out through other paths, such as UDP, TCP and SNMP. In general, almost all the requests/replies can be used to acquire reply time. Usually, the ways except ICMP ECHO is used to settle the problem that some routers' no response or low response priority leads to the wrong answering time.

3.6.2 Ping Configuration

Test if the remote host is accessible.

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip 0	Enter ip port mode

3	ip address A.B.C.D [A.B.C.D] <1-4094>	Configure the ip address on the switch A.B.C.D IP address [A.B.C.D] subnet mask <1-4094> vlan number
4	exit	Exit global configuration mode and enter privileged EXEC mode
5	exit	Exit privileged EXEC mode
6	ping Ipaddress [count NumPktsRe] [size SizeofIcmpeChPkt] [waittime PktTimOut]	Test if the remote host is accessible <i>Ipaddress</i> : test the IP address A.B.C.D <i>NumPktsRe</i> : <i>Number of packets to receive</i> specify the package number before the ping program ends <1-65535> <i>SizeofIcmpeChPkt</i> : <i>Size of icmp echo packet</i> specify the size of the ICMP answering message<1-4096> <i>PktTimOut</i> : <i>Packet timeout in seconds</i> specify the time-out time of ping waiting for answer <1-100> ,the unit is milliseconds

3.6.3 Typical Configuration Example

As is shown below, the host connects the switch with cable. User can confirm if the connection works through the command **ping**, while the switch is also able to transfer data to the host through **ping**.



1 Set the switch IP address as 20.0.0.10, the connection IP address as 10.168.0.221, the number of messages sent is 3, the message size is 100, waiting time 3. Because the destination IP address goes against the PC IP,

the connection does not work.

```
Raisecom#config
```

```
Raisecom(config)# int ip 0
```

```
Raisecom(config-ip)#ip address 20.0.0.10 1
```

```
Raisecom(config-ip)#exit
```

```
Raisecom(config)#exit
```

```
Raisecom#ping 10.168.0.221 count 3 size 100 waittime 3
```

Type CTRL+C to abort.

Sending 3, 108-byte ICMP Echos to 10.168.0.221 , timeout is 3 seconds:

UUU

no answer from 10.168.0.221

Ping unsuccessfully

2 connect PC, the IP address is 20.0.0.221, set the switch IP 20.0.0.10, connect success will be shown.

```
Raisecom#config
```

```
Raisecom(config)# int ip 0
```

```
Raisecom(config-ip)#ip address 20.0.0.10 1
```

```
Raisecom(config-ip)#exit
```

```
Raisecom(config)#exit
```

```
Raisecom#ping 20.0.0.10 count 3 size 100 waittime 3
```

Type CTRL+C to abort.

Sending 3, 108-byte ICMP Echos to 20.0.0.221 , timeout is 3 seconds:

!!!

Success rate is 100 percent(3/3)

round-trip (ms) min/avg/max = 0/10/32

3.7 tracerout Diagnose

3.7.1 traceroute Principle

Traceroute, like **ping**, is a useful way of network management, which is use to find the route that the router s and lines that the message actually passes.

L3 Traceroute is carried out by sending a group of incremental TTL probe packets. Probe packets work in the form of UDP or ICMP Echo. If only TTL>0, or a ICMP will be returned per hop to the destination. From this message the RRT of per hop on the way to destination.

3.7.3 traceroute Configuration

Before L3 Traceroute is used, the IP address and default gateway of the switch need configuration first.

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip 0	Enter IP configuration mode

3	ip address A. B. C. D [A. B. C. D] <1-4094>	Configure the IP address of the switch <i>A. B. C. D</i> IP address <i>[A. B. C. D]</i> subnet mask <1-4094> vlan number
4	exit	Quit global configuration mode and enter privileged EXEC mode
5	ip default-gateway A.B.C.D	Configure the default gateway <i>A.B.C.D</i> gateway number
6	show int ip	Show IP configuration
7	show running	Show default gateway configuration
8	traceroute A. B. C. D [firstTTL <1-255>] [maxTTL <1-255>] [port <1-65535>] [waittime <1-60>] [count <1-10>]	<i>traceRoute</i> show the route to destination <i>A. B. C. D</i> IP address <i>firstTTL</i> initialize TTL value <i>maxTTL</i> maximize TTL value <1-255> TTL value range <1-65535> Port number range <1-60> waiting time range <1-10> count value

3.7.3 Typical Configuration Example

Example: set the IP address as 10.0.0.8, default gateway 10.100.0.1, trace the route to 58.63.236.42(www.sina.com.cn)

Raisecom#**config**

Raisecom(config)# **int ip 0**

Raisecom(config-ip)#**ip address** 10.0.0.8 1

Raisecom(config-ip)#**exit**

Raisecom(config)#**ip default-gateway** 10.100.0.1

Raisecom(config)#**exit**

Raisecom#**Tracing** the route to 58.63.236.42

Type ctrl+c to abort.

```

1  10.0.0.1    10 ms    10 ms    10 ms
2  192.168.101.5  3 ms      3 ms     73 ms
3  192.168.101.5  10 ms     10 ms    10 ms
4  202.96.4.81  18 ms     16 ms    19 ms
5  202.106.228.177  9 ms      5 ms     12 ms
6  202.106.228.5  10 ms      8 ms      9 ms
7  202.96.12.25  7 ms       8 ms      5 ms
8  219.158.11.66  24 ms     20 ms     10 ms
9  202.97.15.57  101 ms    101 ms    126 ms
10 202.97.60.185  218 ms    222 ms    205 ms
11 202.97.40.58  119 ms    112 ms    113 ms
12 219.136.246.134 118 ms    142 ms    131 ms

```

13	219.136.246.6	138 ms	135 ms	110 ms
14	58.63.232.46	103 ms	115 ms	105 ms
15	58.63.236.42	199 ms	205 ms	197 ms

Trace complete.

3.8 telnetd

telnetd Principle

Telnet is the standard protocol and main way of remote login, which offers the ability of working on the local machine for remote host. The telnetd module in ROS4.0 implements the function of telnet server, letting telnet remote client login the facility so that it could be logged in and managed by telnet client.

3.8.2 telnet Default Configuration

Funcktion	Default value
Telnet server up-ling limit	5
telnet server link physical port	所有端口

3.8.3 telnetd Configuration

1 Close telnet configuration

S	Command	Description
t e p		
1	config	Enter global configuration mode
2	telnet-server close	Telnet server close
	terminal-telnet <1-5>	<1-5> end telnet dialog number
3	exit	Return to privileged EXEC mode
4	show telnet-server	Show current telnet server configuration

2 Set the telnet server linking upper-limit

Ste	Command	Description
p		

1	config	Enter global configuration mode
2	telnet-server max-session <0-5>	Set the telnet server linking upper-limit <0-5> linking number
3	telnet-server accept port-list (all {1-MAX_PORT_STR})	Set the available port of the telnet server port-list: port list All: all the ports MAX_PORT_STR: port upper limit
4	exit	Return to privileged EXEC mode
5	show telnet-server	Show the current configuration of the telnet server
6	Show information port	Show information port

3.8.4 Typical Configuration Example

1 Set the linking upper limit of the telnet server as 3, open the available ports of Telnet server and show the current configuration.

Raisecom#**config**

Raisecom(config)#**telnet-server max-session 3**

Set successfully

Raisecom(config)#**telnet-server accept port 3**

Raisecom(config)#**exit**

Raisecom#**show telnet-server**

Max session: 3

Accept port-list: 1-26

3.9 Watchdog Function

3.9.1 Watchdog Principle

By configuring the watchdog software, the system program going into endless loop can be avoided, and the system stability will be better.

3.9.2 Configure Watchdog

Enable and Disable watchdog

Step	Command	Description
------	---------	-------------

1	<code>watchdog {enable disable}</code>	Enable: open watchdog Disable: close watchdog
2	<code>Show watchdog</code>	Show watchdog state

3.9.4 Typical Configuration Example

Open watchdog and show the state

```
Raisecom#watchdog enable
```

Set successfully

```
Raisecom#show watchdog
```

Watchdog function: Enable