

www.raisecom.com

802.1x Configuration Guide

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 ©2007 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:

Address: 2nd Floor, South Building of Rainbow Plaza, No.11 Shangdi Information Road,
Haidian District, Beijing 100085

Tel: +86-10-82883305

Fax: +86-10-82883056

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 ... 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 ... specification, instead of the web page above, please send comments to:

export@raisecom.com

We hope to hear from you!

CONTENTS

Release Notes	5
Chapter 1 802.1x Configuration Guide	1
1.1 802.1x principle overview	1
1.2 Configure 802.1x	2
1.2.1 Default 802.1x configuration	2
1.2.2 Basic 802.1x configuration	2
1.2.3 802.1x reauthorization configuration	5
1.2.4 Configure 802.1x timer	6
1.2.5 802.1x statistics cleanup	8
1.2.6 Maintenance	9
1.2.7 Configuration example	9

Release Notes

Date of Release	Manual Version	Software Version	Revisions

Preface

About This Manual

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

Who Should Read This Manual

This manual is a valuable reference for sales and marketing staff, after service staff and telecommunication network designers. For those who want to have an overview of the features, applications, structure and specifications of ... device, this is also a recommended document.

Relevant Manuals

《Raisecom NView System User Manual》

《Raisecom Nview System Installation and Deployment Manual》

《... User Manual》

《... Commands Notebook》

Organization

This manual is an introduction of the main functions of ... EMS. To have a quick grasp of the using of the EMS of ... , please read this manual carefully. The manual is composed of the following chapters

Chapter 1 Overview

This chapter briefly introduces the basic function of ...

Chapter 2 Configuration Management

This chapter mainly introduces the central site configuration management function of the

Chapter 3 Performance Management

This chapter focuses on performance management function of

Chapter 4 Device Maintenance Management

This chapter introduces the device maintenance management function of

Appendix A Alarm Type

The alarm types supported by

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 1 802.1x Configuration Guide

1.1 802.1x principle overview

802.1x module is based on IEEE802.1x protocol, or port based network access control technology, it makes authorization and control to access equipments on the equipments' physical access layer, and defines the point-to-point connection mode between the access equipment and access port.

The system structure of IEEE 802.1x includes three parts:

- ✓ Supplicant
- ✓ Authenticator
- ✓ Authorization Server

LAN access control equipment (like access switch) needs the Authenticator of 802.1x; user side equipment, like computer, needs to install 802.1x client (Supplicant) software (or the 802.1x client pre-positioned in Windows XP); while 802.1x Authorization Server System usually stays in operator's AAA centre.

Authenticator and Authorization Server exchange information using Extensible Authorization Protocol; while Supplicant and Authenticator use EAPOL (EAP over LANs, defined in IEEE802.1x) for communication, the authorization data is encapsulated in EAP frame. The authorization data is encapsulated in the message of other AAA upper layer protocol (like RADIUS) so that it is able to go through complicated network and reach Authorization Server, this process is called EAP Realy.

The figure below is 802.1x system structure:

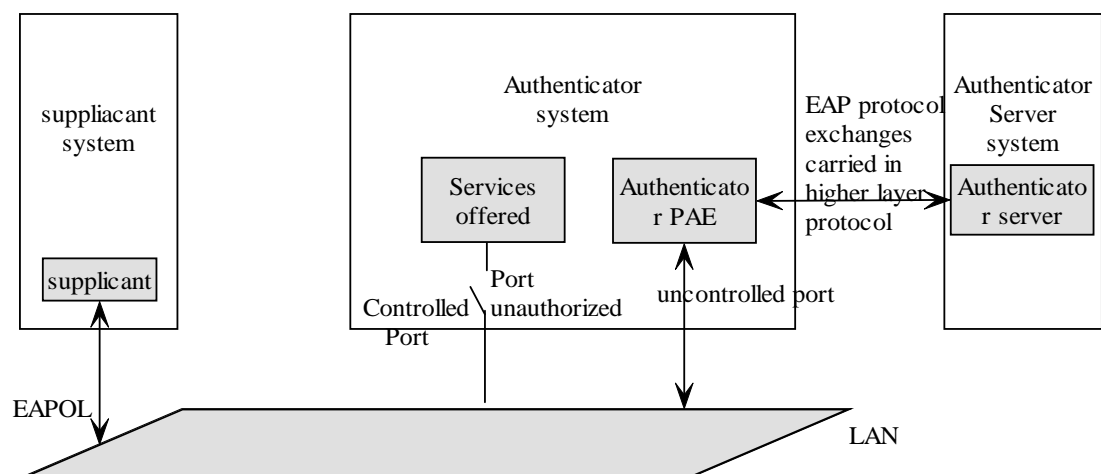


Fig 1: 802.1x system structure

'port based network access control' means to do authorization and control to the access equipments in LAN access control equipment port layer. If the user equipment connected to the port can go through the authorization, then it is able to visit the resources in LAN; if it can not pass the authorization, then it can not visit the network resources through switch – same as physical link down.

1.2 Configure 802.1x

802.1x configuration includes:

1. Default 802.1x configuration situation;
2. Enable/disable 802.1x global feature and port feature;
3. Configure RADIUS server IP address and RADIUS public key;
4. Show RADIUS server configuration;
5. Configure port access control mode;
6. Enable/disable 802.1 x reauthorization function;
7. Configure 802.1x reauthorization period;
- 8 Configure 802.1x silence time;
9. Configure Request/Identity resending period;
10. Configure Request/Identity resending period;
11. Configure RADIUS server overtime.

1.2.1 Default 802.1x configuration

Function	Default value
Global 802.1x feature	disable
Port 802.1x feature	disable
Port access control mode	auto
RADIUS server overtime	100s
802.1x reauthorization function	disable
802.1x reauthorization period	3600s
802.1 silence time	60s
Request/Identity resending period	30s
Request/Challenge resending period	30s

1.2.2 Basic 802.1x configuration

The basic 802.1x configuration is shown below:

- ✓ Enable/disable 802.1x global feature and port feature;
- ✓ Configure RADIUS server IP address and RADIUS public key;
- ✓ Configure port access control mode.

1. Enable/disable 802.1x global feature and port feature;

802.1x feature includes global 802.1x feature and port 802.1x feature, if one of them is not enabled, it will lead to 802.1x feature shown as constraint authorization passing through. 802.1x protocol and spanning tree protocol (STP) can not be opened at the same time in the same port.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	dot1x { disable enable }	Enable/disable global 802.1x feature
3	interface { port line client } <i><1- MAX_PORT_NUM ></i>	Enter ethernet physical port mode <i>1- MAX_PORT_NUM</i> the equipment port
4	dot1x { disable enable }	Enable/disable port 802.1x feature
5	exit	Return to global configuration mode
6	exit	Return to privileged EXEC mode
7	show dot1x { port-list line client } portlist	Show physical port 802.1x configuration information <i>Portlist</i> use ‘_’ and ‘,’ to input more ports number

⚠ Notice:

- If a port has enabled STP and 802.1x protocol port can not be opened successfully, we need to disable port STP first.
- 802.1x protocol is physical port based access control protocol, it is not suggested that user enable 802.1x feature on aggregation port and not-Access port. When several users connects to the same switch port using shared network, if one user passes the authorization, then other users do not need authorization before they visit the network, but in this situation several user doing authorization at the same time may

cause unsuccessful authorization because of interaction.

2. Configure RADIUS server IP address and RADIUS public key:

Configuring RADIUS server IP address and RADIUS public key is a necessary precondition of 802.1x port authorization.

The configuration steps are as follows:

Step	Command	Description
1	[no] radius <i>ipaddress</i>	Configure RADIUS server IP address
2	[no] radius-key <i>string</i>	Configure RADIUS server public key
3	show radius-server	Show RADIUS server configuration information

3. Configure port access control mode:

Port access control mode can be divided into three states: auto, authorized-force, unauthorized-force. By default it is auto. When global 802.1x feature and port 802.1x feature is on, the configuration determines directly if the authorization process will use authorized-force, unauthorized-force or protocol control mode.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface { port line client } <i><1-MAX_PORT_NUM></i>	Enter ethernet physical port mode <i>1-MAX_PORT_NUM</i> equipment port
3	dot1x auth-control { auto authorized-force unauthorized-force }	Configure port control mode
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC

		mode
6	show dot1x { port-list line client} portlist	Show physical port 802.1x configuration information <i>Portlist</i> use ‘_’ and ‘,’ to input more port numbers.

1.2.3 802.1x reauthorization configuration

Reauthorization function is for authorized users, so you should make sure that global and port 802.1x feature are enabled. By default reauthorization function is disabled. The authorized port keeps the state of authorized in the process of authorization; if reauthorization failed, then the port will enter unauthorized state.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface { port line client} <1-MAX_PORT_NUM>	Enter ethernet physical port mode <i>1-MAX_PORT_NUM</i> equipment port
3	dot1x reauthentication { enable disable }	Enable/disable reauthorization function
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show dot1x { port-list line client} portlist	Show physical port 802.1x configuration

 information

Portlist, use ‘ _ ’

and ‘ , ’ to input

more port numbers

1.2.4 Configure 802.1x timer

In 802.1x authorization process, there are 5 timers related:

1. reauth-period: reauthorization overtime timer. In the time configured by the timer, 802.1x reauthorization will be raised. Reauth-period-value: the time length configured by reauthorization overtime timer, range is 1-65535, unit is second. By default it is 3600 seconds.
2. quit-period: quiet timer. When user authorization failed, the switch needs to keep quiet for a period of time, which is configured by quiet timer. When quiet timer exceeds the time it will make reauthorization. In quiet time, the switch will not process authorization messages. Quiet-period-value: the quiet time value configured by quiet timer, rang is 10-120, unit is second. By default, quiet-period-value is 60 seconds;
3. tx-period: transmission overtime timer. When the switch sends Request/Identity messages to user request end, the switch will start the timer, if in the configured time length user end software can not send request answering messages, the switch will re-send authorization request message, which will be sent three times. Tx-period-value: the time length configured by sending overtime timer, range is 10-120, unit is second. By default tx-period-value is 30 seconds.
4. supp-timeout: Supplicant authorized timeout timer. When the switch sends Request/Challenge message to user request end, the switch will start supp-timeout timer. if the user request end can not react in the time length configured in the timer, the switch will re-send the message twice. Supp-timeout-value: the time length configured by Supplicant authorization overtime timer, range is 10-120, unit is second. By default supp-timeout-value is 30 seconds.
5. server-timeout: Authentication Server. The timer defines the authenticator and the total overtime-length of RADIUS server dialog, when the timer exceeds the time the authenticator will end the dialog with RADIUS server, and start a new authorization process. The resending times and interval of RADIUS is determined by the switch RADIUS client. The switch RADIUS client message resend 3 times, while the waiting time is 5s. server-timeout-value: the overtime length configured by RADIUS server timer, range is 100-300, unit is second. By default server-timeout-value is 100s.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface { port line client } <1- MAX_PORT_NUM >	Enter ethernet physical port mode
3	[no] dot1x timer	Configure

	reauth-period <i>reauth-period-value</i>	reauthorization timer value Range is 1-65535, unit is second. By default the value is 3600s
4	[no] dot1x timer quiet-period <i>quiet-period-value</i>	Configure quiet-time timer value Range is 10-120, unit is second. By default quiet-period-value is 60s
5	[no] dot1x timer tx-period <i>tx-period-value</i>	Configure Request/Identity resending timer value Range is 10-120, unit is second. By default tx-period-value is 30s
6	[no] dot1x timer supp-timeout <i>supp-timeout-value</i>	Configure Request/Challenge resending timer value Range is 10-120, unit is second. By default supp-timeout-value is 30s
7	[no] dot1x timer server-timeout <i>server-timeout-value</i>	Configure RADIUS server overtime timer value Range is 100-300,

		unit is second. By default server-timeout-value is 100s
8	exit	Return to global configuration mode
9	exit	Return to privileged EXEC mode
10	show dot1x { port-list line client} portlist	Show physical port 802.1x configuration information Portlist, use '_' and ',' to input more port numbers.

1.2.5 802.1x statistics cleanup

Monitoring and port statistics information is used to count the EAPOL messages number for the switches and user end exchanging data. Cleaning port stat. will clean all the statistics information of the selected ports. The steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	clear dot1x{ port-list line client } portlist statistics	Clear physical port 802.1x statistics information
3	exit	Return to privileged EXEC mode
4	show dot1x { port-list line client} portlist statistics	Show physical port 802.1x statistics information Portlist, use '_' and ',' to input more port numbers.

1.2.6 Maintenance

Use **show** to show the configuration and running state of switch 802.1x function for the convenience of monitoring and maintenance.

The related **show** commands are shown below:

Command	Description
show radius-server	Show RADIUS server configuration
show dot1x { port-list line client} portlist	Show physical port 802.1x configuration information
show dot1x { port-list line client} portlist statistics	Show physical port 802.1x statistics information

1.2.7 Configuration example

1. Configuration request:

- PC user can visit outer network after passing RADIUS server authorization
- In authorization-force mode, PC needs not authorization before visiting outer network;
- In unauthorization-force mode, PC can not visit outer network;
- After passing authorization, PC will do reauthorization 600s later automatically.

2. Network structure:

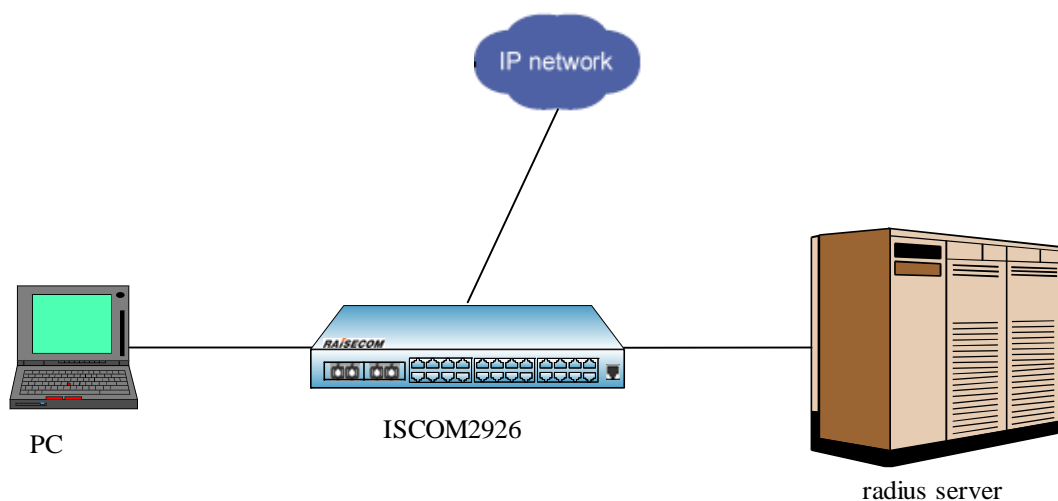


Fig 2: network structure

3. Configuration steps:

- Configure RADIUS server:

Follow ISCOM switch 802.1x user guide, add user raisecom in the server, the password is 123;

- Configure switch IP address and RADIUS server address:

```
Raisecom(config)#interface ip 0  
Raisecom(config-ip)#ip address 10.10.0.1 255.255.0.0 1  
Raisecom(config-ip)#exit  
Raisecom(config)#ip default-gateway 10.10.0.2  
Raisecom(config)#exit  
Raisecom# radius 192.168.0.1  
Raisecom# radius-key raisecom
```

- Configure enabling global and port 802.1x authorization function:

```
Raisecom(config)#dot1x enable  
Raisecom(config)#interface port 1  
Raisecom(config-port)#spanning-tree disable(STP and 802.1x are mutex)  
Raisecom(config-port)# dot1x enable
```

- PC end uses the client software for authorization request, username: raisecom, password: 123;
The PC client software will inform passing authorization, then we can visit outer network;

- Change the authorization mode to authorization-force mode:

```
Raisecom(config)#interface port 1  
Raisecom(config-port)#dot1x auth-control authorized-force
```

- PC end uses the client software for authorization request, username: raisecom, password: 123;
The PC client software will inform passing authorization, then we can visit outer network;

- Chang authorization-force mode to unauthorization-force mode

```
Raisecom(config)#interface port 1  
Raisecom(config-port)#dot1x auth-control unauthorized-force
```

- PC end uses the client software for authorization request, username: raisecom, password: 123;
The PC client software will inform passing authorization, then we can visit outer network;

- Enable reauthorization, and configure the time to 600s:

```
Raisecom(config)#interface port 1
```

```
Raisecom(config-port)#dot1x reauthentication enable
```

- Show the statistics information:

```
Raisecom#show dot1x port-list 1 statistics
```

⚠ Notice:

- The switch's IP address, RADIUS server IP and key must well configured first of all;



北京瑞斯康达科技发展有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: 2nd Floor, South Building of Rainbow Plaza, No.11 Shangdi Information Road,
Haidian District, Beijing Postcode: 100085 Tel: +86-10-82883305 Fax: +86-10-82883056
Email: export@raisecom.com <http://www.raisecom.com>