

www.raisecom.com

ACL 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 ©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
1.1 Date of Release	5
1.2 Manual Version	5
1.3 Software Version	5
1.4 Revisions	5
1.5	5
1.6	5
1.7	5
1.8	5
1.9	5
1.10	5
1.11	5
1.12	5
Chapter 1 ACL Function Configuration	1
1.1 ACL Introduction	1
1.2 IP ACL Configuration	1
1.2.1 IP ACL Default Configuration	1
1.2.2 IP ACL Configuration	1
1.2.3 Monitoring and Maintenance	2
1.2.4 Specific Configuration Example:	3
1.3 MAC ACL Function	3
1.3.1 MAC ACL Default Configuration	3
1.3.2 MAC ACL Configuration	3
1.3.3 Monitoring and Maintenance	4
1.3.4 Specific Configuration Examples	5
1.4 MAP ACL Function	5
1.4.1 MAP ACL Default Configuration	6
1.4.2 MAP ACL Configuration	6
1.4.2 Monitoring and Maintenance	15
1.4.3 Specific Configuration Example	16
1.5 Application Configuration Based on Hardware ACL	16
1.5.1 Application Default Configuration Based on Hardware ACL	17
1.5.2 Application Configuration Based on Hardware ACL	17
1.5.3 Monitoring and Maintenance	20
1.5.4 Specific Configuration Examples	20
1.6 Configuration Function Based on Software IP ACL	21
1.6.1 Application Default Configuration Based on Software IP ACL	21
1.6.2 Layer-3 Interface Protect Configuration Based on IP ACL	21
1.6.3 Monitoring and Maintenance	22
1.6.4 Specific Configuration Example	22

Release Notes

Date of Release	Manual Version	Software Version	Revision
--------------------	-------------------	---------------------	----------

)

;

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 ACL Function Configuration

1.1 ACL Introduction

In order to filter packets, network equipment needs to set a series of matching rules to identify the filtered objects. Only after this, user can allow or prohibit relative packets to pass through according to the designated strategy in advance. ACL (Access Control list) is used to realize these operations.

ACL can be applied to VLAN, Layer-2 physical port and Layer-3 management interface.

ACL makes classification to packets according to a series of matching conditions; these conditions can be packet source address, destination address and port number etc. It is combined with a series of judgment sentences. After activating a ACL, switch will check each received packet according to the judgment conditions, packets will be forwarded or dropped then according to these conditions.

User can specify *permit* or *deny* while configuring ACLs. When it is set as *deny*, packets that are in accord with the rules will be dropped, the others will be forwarded; When it is set as *permit*, packets that are in accord with the rules will be forwarded, the others will be dropped.

1.2 IP ACL Configuration

Switch supports 400 IP access control lists at most with corresponding series number 0~399. it specifies classification rules according to the source IP address, destination IP address in the IP packet header, used TCP or UDP protocol port number and etc. packet attributes information, and then processes related operations to the packets according these rules. The construction of IP packet header can be referred to RFC791 and other related documents.

1.2.1 IP ACL Default Configuration

None.

1.2.2 IP ACL Configuartion

Steps	Command	Description
Step 1	config	Entry into global configuration mode
Step 2	ip-access-list <i>list-number</i> { deny permit } <i>protocol</i> { <i>source-address mask</i> any } [<i>source-protocol-port</i>] { <i>destination-address</i>	ip-access-list configuration IP address access control list <i>list-number</i> IP address access control

	<i>mask</i> any } [<i>destination-protocol-port</i>]	<p>listserial number, range from 0-399</p> <p>deny permit represents reject/accept access。</p> <p><i>protocol</i> binding protocol type.</p> <p><i>source-address mask</i> any is source IP address with its mask, format is dotted decimal in the form of A.B.C.D, any indicates arbitrary address.</p> <p><i>source-protocol-port</i> is source port for TCP/UDP protocol</p> <p><i>destination -address mask</i> any is the destination address and its mask, the format is dotted decimal as A.B.C.D; any indicates arbitrary address.</p> <p><i>destination -protocol-port</i> is the destination port of TCP/UPD.</p>
Step 3	exit	Exit global configuration mode and enter privileged EXEC mode
Step 4	show ip-access-list <i>list-number</i>	<p>Show IP access control list relevant information</p> <p><i>list-number</i> is the series number for the IP access control list to be shown, rang is 0-399.</p>
Step 5	No ip-access-list <i>list-number</i>	<p>Delete IP access control list</p> <p><i>list-number</i> is the list series number to be deleted</p>

1.2.3 Monitering and Maintenance

Check and display indicated IP ACL command:

Command	Description
show ip-access-list [{0-399}]	Show IP Access Control List

1.2.4 Specific Configuration Example:

➤ Destination

Configure source IP address as 192.168.1.0 segment, destination IP address as random address , protocol type as IP and access type as deny IP access rule;

Configure source IP address is 10.168.1.19; mask is 255.255.255.255; source protocol port is 80; destination address is random port; protocol type is TCP; visit type is deny IP access rule.

Configure source IP address is 10.168.1.19; mask is 255.255.255.255; destination address is 10.168.0.0 segment; protocol type is TCP; access type is permit's IP access rule.

➤ Set up Steps

```
Raisecom#config
```

```
Raisecom(config)#ip-access-list 0 deny ip 192.168.1.0 255.255.255.0 any
```

```
Raisecom(config)#ip-access-list 1 deny tcp 10.168.1.19 255.255.255.255 80 any
```

```
Raisecom(config)#ip-access-list 2 permit tcp 10.168.1.19 255.255.255.255 80 10.168.0.0 255.255.0.0 80
```

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

```
Raisecom#show ip-access-list
```

Src Ip: Source Ip Address

Dest Ip: Destination Ip Address

List	Access	Protocol	Ref.	Src Ip:Port	Dest Ip:Port
0	deny	IP	0	192.168.1.0:0	0.0.0.0:0
1	deny	TCP	0	10.168.1.19:80	0.0.0.0:0
2	permit	TCP	0	10.168.1.19:80	10.168.0.0:80

1.3 MAC ACL Function

Switch supports 400 digital-identified Layer-2 (MAC) access control lists at most with corresponding series number 0~399. Layer-2 access control list in conjunction with filter can process relevant operations to packets according to the source MAC address carried in Layer-2 frame, destination MAC address, source VLAN ID, Layer-2 protocol types and other Layer-2 information rules.

1.3.1 MAC ACL Default Configuration

None.

1.3.2 MAC ACL Configuration

Steps	Command	Description
-------	---------	-------------

Step 1	config	Entry into global configuration mode
Step 2	mac-access-list <i>list-number</i> { deny permit } [<i>protocol</i> any] { <i>source-MAC-address</i> any } { <i>destination-MAC-address</i> any }	<p>MAC access control list configuration</p> <p><i>list-number</i> access control list series number, range 0-399.</p> <p>deny permit indicates deny/permit access</p> <p>[<i>protocol</i> any] indicates bonded protocol type, any indicates unrestricted protocol type.</p> <p><i>source-MAC-address</i> indicates the source MAC address to be configured, format is hexadecimal string as “HHHH.HHHH.HHHH”, dotted every 4 characters; any indicates arbitrary source MAC address.</p> <p><i>destination-MAC-address</i> is the destination MAC address to be configured, format is hexadecimal string as “HHHH.HHHH.HHHH”, dotted every 4 characters; any indicates arbitrary destination MAC address.</p>
Step 3	exit	Exit global configuration mode and enter privileged EXEC mode
Step 4	show mac-access-list <i>list-number</i>	<p>Show MAC access control list</p> <p><i>list-number</i> is the series number for the MAC access control list to be shown, range is 0-399.</p>
Step 5	no mac-access-list <i>list-number</i>	<p>Delete configured MAC access control list</p> <p><i>list-number</i> is the list series number to be deleted</p>

1.3.3 Monitoring and Maintenance

Check and display indicated MAC ACL command

Command	Description
---------	-------------

```
show mac-access-list [{0-399}]
```

Display MAC access control list

1.3.4 Specific Configuration Examples

➤ Destination

Configure source MAC address as 1234.1234.1234; destination MAC address as 5678.5678.5678; protocol as IP; access type as deny's MAC access rule;

Configuration source MAC address as 1111.2222.3333; destination MAC address as 4444.5555.6666; protocol as ARP; access type as permit's MAC access rule.

➤ Set up Steps

```
Raisecom#config
```

```
Raisecom#config
```

```
Raisecom(config)# mac-access-list 0 deny ip 1234.1234.1234 5678.5678.5678
```

```
Raisecom(config)# mac-access-list 1 permit arp 1111.2222.3333 4444.5555.6666
```

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

```
Raisecom#show mac-access-list
```

Src Mac: Source MAC Address

Dest Mac: Destination MAC Address

List	Access	Protocol	Ref.	Src Mac	Dest Mac
0	deny	ip	0	1234.1234.1234	5678.5678.5678
1	permit	arp	0	1111.2222.3333	4444.5555.6666

1.4 MAP ACL Function

Switch supports 400 digital-identified access list maps at most with corresponding series number 0~399. Access list map can define more protocols and more detailed protocol character fields than IP access list and MAC access list, also can implement matching to any bytes in the first 64 bytes of Layer-2 frame according to user's definition before corresponding processing to the data packets from matched results. User needs to be familiar with Layer-2 data frame before using user-defined access list map.

Access list map uses command *match* to set the expected matching character field, no conflicts can exist in the same access list map when setting matching character field. Character fields that can be matched are shown below:

- Mac destination address
- Mac source address
- Ethernet protocol type
- CoS
- ARP protocol type
- Hardware address of ARP protocol sender
- Hardware address of ARP protocol receiver

- IP address of ARP protocol sender
- IP address of ARP protocol receiver
- IP protocol destination address
- IP protocol source address
- IP protocol priority
- IP protocol ToS
- IP protocol dscp
- IP protocol segmentation bit
- IP protocol type
- TCP protocol destination port
- TCP protocol source port
- TCP protocol bit
- UDP protocol destination port
- UDP protocol source port
- ICMP protocol information type
- ICMP protocol information code
- IGMP protocol information type

User can also use regular mask and offset to define any byte in the first 64 bytes in data frame, and then compare them with the user-defined rules to obtain the matched data frame, after this user can implement relevant operations. User-defined rules can be certain data fixed attributes, such as that in order to obtain all the TCP packets, user can define the rules as “06”, mask as “FF”, offset as “27”, by using such a method, regular rules and offsets can work together to pick up the segment of TCP protocol number in data frame, then compare it with defined rules to obtain all matched TCP packets.

Attention:

- Rules should be even hexadecimal, offset includes segment of 802.1Q VLAN TAG even if what the switch receives is untagged packet.

1.4.1 MAP ACL Default Configuration

None.

1.4.2 MAP ACL Configuration

Steps	Command	Description
Step 1	config	Entry into global configuration mode
Step 2	access-list-map <i>list-number</i> { deny permit }	<i>list-number</i> : list serial number, from 0-399 Deny permit deny or permit data packets to go through when matching.
Step 3	match mac { destination source } <i>HHHH.HHHH.HHHH</i>	Destination source match source mac or destination mac <i>HHHH.HHHH.HHHH</i> mac address

Step 4	match cos <0-7>	<0-7> match cos value
Step 5	match ethertype <i>HHHH [HHHH]</i>	<i>HHHH[HHHH]</i> match Ethernet type [mask]
Step 6	match {arp eapol flowcontrol ip ipv6 loopback mpls mpls-mcast pppoe pppoe-disc x25 x75}	arp ——match ARP protocol eapol ——match eapol protocol flowcontrol ——match flow control protocol ip ——match ip protocol ipv6 ——match ipv6 protocol loopback ——match loopback protocol mpls ——match mpls single cast protocol mpls-mcast ——match mpls group cast protocol pppoe ——match pppoe protocol pppoe-disc ——match pppoe discover protocol x25 ——match x25 protocol x75 ——match x75 protocol
Step 7	no match mac {destination source}	Do not match MAC address Destination source match source mac or destination mac
Step 8	no match cos	Do not match CoS value
Step 9	no match ethertype	Do not match Ethernet type
Step 10	match arp opcode {request reply}	Match arp protocol type request reply arp protocol reply /request packet
Step 11	match arp {sender-mac target-mac} <i>HHHH.HHHH.HHHH</i>	Match arp protocol hardware address

		sender-mac target-mac match arp sender/target mac address <i>HHHH.HHHH.HHHH</i> MAC address
Step 12	match arp {sender-ip target-ip} <i>A.B.C.D [A.B.C.D]</i>	matcharpprotocolIPAddress sender-ip target-ip sender/target IPAddress <i>A.B.C.D [A.B.C.D] laddress[mask]</i>
Step 13	no match arp opcode	do not matcharpprotocoltype
Step 14	no match arp {sender-mac target-mac}	do not matcharpprotocol 硬件 address
Step 15	no match arp {sender-ip target-ip}	do not matcharpprotocolIPAddress sender-ip target-ip sender/target IP address
Step 16	match ip {destination-address source-address} A.B.C.D [A.B.C.D]	Match IP protocol address destination-address source-address Ip protocol destination/source address <i>A.B.C.D [A.B.C.D] IP address [mask]</i>
Step 17	match ip precedence {<0-7> routine priority immediate flash flash-override critical internet network}	Match IP priority <0-7>—— IP priority value routine —— IP priority value 0 priority —— IP priority value 1 immediate —— IP priority value 2 flash —— IP priority value 3 flash-override —— IP priority value 4 critical —— IP priority value 5 internet —— IP priority value 6 network —— IP priority value 7
Step 18	match ip ToS {<0-15> normal min-monetary-cost min-delay max-reliability max-throughput}	Match IP priority ToS value <0-15>——ToS value

		<p>normal——normal ToS value (0)</p> <p>min-monetary-cost—— Min monetary cost ToS value (1)</p> <p>min-delay——Min delay ToS value (8)</p> <p>max-reliability——Max reliability ToS value (2)</p> <p>max-throughput——Max throughput ToS value (4)</p>
Step 19	match ip dscp {<0-63> af11 af12 af13 af21 af22 af23 af31 af32 af33 af41 af42 af43 cs1 cs2 cs3 cs4 cs5 cs6 cs7 ef default}	<p>Match IP DSCP value</p> <p><0-63>——IP DSCP value</p> <p>af11——AF11 DSCP value (001010)</p> <p>af12——AF12 DSCP value (001100)</p> <p>af13——AF13 DSCP value (001110)</p> <p>af21——AF21 DSCP value (010010)</p> <p>af22——AF22 DSCP value (010100)</p> <p>af23——AF23 DSCP value (010110)</p> <p>af31——AF31 DSCP value (011010)</p> <p>af32——AF32 DSCP value (011100)</p> <p>af33——AF33 DSCP value (011110)</p> <p>af41——AF41 DSCP value (100010)</p> <p>af42——AF42 DSCP value (100100)</p> <p>af43——AF43 DSCP value (100110)</p> <p>cs1——CS1(priority 1) DSCP value (001000)</p> <p>cs2——CS2(priority 2) DSCP value (010000)</p> <p>cs3——CS3(priority 3) DSCP value (011000)</p>

		<p>cs4——CS4(priority 4) DSCP value (100000)</p> <p>cs5——CS5(priority 5) DSCP value (101000)</p> <p>cs6——CS6(priority 6) DSCP value (110000)</p> <p>cs7——CS7(priority 7) DSCP value (111000)</p> <p>default——Default DSCP value (000000)</p> <p>ef——EF DSCP value (101110)</p>
Step 20	match ip no-fragments	Match no-fragment IP packet
Step 21	match ip protocol <0-255>	<p>Match IP protocol value</p> <p><0-255>——IP protocol type value</p>
Step 22	match ip { ahp esp gre icmp igmp igmp ipinip ospf pcp pim tcp udp }	<p>Match IP protocol value</p> <p>ahp——authorize header protocol</p> <p>esp——encapsulation security payload protocol</p> <p>gre—— General routing encapsulation protocol</p> <p>icmp——Internet control message protocol</p> <p>igmp——Internet group message protocol</p> <p>igrp——Interior gateway routing protocol</p> <p>ipinip——IP-in-IP tunnel</p> <p>ospf——Open shortest path first</p> <p>pcp——Payload compression protocol</p> <p>pim——protocol independent multicast</p>

		<p>protocol</p> <p>tcp—Transmission control protocol</p> <p>udp—user datagram protocol</p>
Step 23	no match ip {destination-address source-address}	<p>Do not match IP protocol address</p> <p>destination-address source-address IP protocol destination/source address</p>
Step 24	no match ip precedence	do not match IP priority
Step 25	no match ip ToS	do not match IP ToS value
Step 26	no match ip dscp	do not match IP DSCP value
Step 27	no match ip no-fragments	do not match IP no-fragment
Step 28	no match ip protocol	do not match IP protocol value
Step 29	match ip tcp { destination-port source-port } {<0-65535> bgp domain echo exec finger ftp ftp-data gopher hostname ident irc klogin kshell login lpd nntp pim-auto-rp pop2 pop3 smtp sunrpc syslog tacacs talk telnet time uucp whois www}	<p>Match Tcp protocol port number</p> <p>destination-port source-port TCP protocol destination/source port</p> <p><0-65535>—tcp port number</p> <p>bgp—border gateway protocol (179)</p> <p>domain—domain name service protocol (53)</p> <p>echo—echo protocol (7)</p> <p>exec—Exec (rsh, 512)</p> <p>finger—Finger (79)</p> <p>ftp—File transfer protocol (21)</p> <p>ftp-data—FTP data connections (20)</p> <p>gopher—Gopher (70)</p> <p>hostname—NIC hostname server (101)</p> <p>ident—identify protocol (113)</p>

		<p>irc——Internet Relay Chat protocol (194)</p> <p>klogin——Kerberos login (543)</p> <p>kshell——Kerberos shell (544)</p> <p>login——Login (rlogin, 513)</p> <p>lpd——Printer Service protocol(515)</p> <p>nntp——network news transport protocol</p> <p>pim-auto-rp——PIM Auto-RP (496)</p> <p>pop2——post office protocol v2 (109)</p> <p>pop3——post office protocol v3 (110)</p> <p>smtp——simple mail transport protocol (25)</p> <p>sunrpc——Sun Remote Procedure Call (111)</p> <p>syslog——System log (514)</p> <p>tacacs——TAC access control system (49)</p> <p>talk——Talk (517)</p> <p>telnet——Telnet (23)</p> <p>time——Time (37)</p> <p>uucp——Unix-to-Unix Copy program (540)</p> <p>whois——Nickname(43)</p> <p>www—— World Wide Web (HTTP, 80)</p>
第 30 步	match ip tcp {ack fin psh rst syn urg }	<p>Match TCP protocol bit</p> <p>ack——match ACK bit</p> <p>fin——matchFIN bit</p> <p>psh——matchPSH bit</p>

		rst ——match RST bit syn ——match SYN bit urg ——match URG bit
Step 31	no match ip tcp { destination-port source-port }	do not match Tcp protocol port number destination-port source-port TCP protocol destination/source port
Step 32	no match ip tcp { ack fin psh rst syn urg }	do not match TCP protocol bit ack ——match ACK bit fin ——match FIN bit psh ——match PSH bit rst ——match RST bit syn ——match SYN bit urg ——match URG bit
Step 33	match ip udp { destination-port source-port } { <0-65535> biff bootpc bootps domain echo mobile-ip netbios-dgm netbios-ns netbios-ss ntp pim-auto-rp rip snmp snmptrap sunrpc syslog tacacs talk tftp time who }	Match udp protocol port number destination-port source-port TCP protocol destination/source port <0-65535>——udp port number biff ——Biff (mail notification, comsat, 512) bootpc ——bootstrap protocol (BOOTP) client (68) bootps ——bootstrap protocol(BOOTP) server (67) domain ——domain name service protocol (53) echo ——echo protocol (7) mobile-ip ——mobile IP registration (434) netbios-dgm ——NetBios datagram

		<p>eservic (138)</p> <p>netbios-ns——NetBios name service (137)</p> <p>netbios-ss——NetBios session service (139)</p> <p>ntp——network time protocol(123)</p> <p>pim-auto-rp——PIM Auto-RP (496)</p> <p>rip—— routing information protocol(520)</p> <p>snmp——simple network magagement protocol(161)</p> <p>snmptrap——SNMP Traps (162)</p> <p>sunrpc——Sun remote procedure call (111)</p> <p>syslog——system log (514)</p> <p>tacacs——TAC access control system (49)</p> <p>talk——Talk (517)</p> <p>tftp—— trivial file transfer protocol(69)</p> <p>time——Time (37)</p> <p>who——Who service (rwho, 513)</p>
Step 34	no match ip udp { destination-port source-port }	<p>do not match udp protocol port number</p> <p>destination-port source-port TCP protocol destination/sourceport</p>
Step 35	match ip icmp <0-255> [<0-255>]	<p>Match icmp protocol information type</p> <p><0-255> [<0-255>] information type[information code]</p>
Step 36	match ip igmp {<0-255> dvmrp query leave-v2 report-v1 report-v2 report-v3 pim-v1 }	<p>Match igmp protocol information type</p> <p><0-255>——IGMP information type</p>

		<p>dvmrp——Distance Vector Multicast Routing Protocol</p> <p>leave-v2——IGMPv2 leave group</p> <p>pim-v1——protocol Independent Multicast version 1</p> <p>query——IGMP member query</p> <p>report-v1——IGMPv1 member report</p> <p>report-v2——IGMPv2 member report</p> <p>report-v3——IGMPv3 member report</p>
Step 37	match user-define <i>rule-string rule-mask</i> <0-64>	<p>Match user-defined segment</p> <p><i>rule-string</i>: user-defined regular string, must be combined of hexadecimal, no more than 64 bytes.</p> <p><i>rule-mask</i>: mask rule, used to implement “or” operation with data packet</p> <p><0-64>: offset, based on dataframe header, and implement “or” operation from the beginning of specified bytes</p>
Step 38	no match user-define	do not match user-defined segment
Step 39	exit	Exit global configuration mode and enter privileged EXEC mode
Step 40	show access-list-map [<i>list-number</i>]	<p>Show port <i>access-list-map</i></p> <p><i>list-number</i> is the port access-list-map series number to show, range is 0-399</p>
Step 41	no access-list-map <i>list-number</i>	<p>Delete user-defined access-list-map</p> <p><i>list-number</i> is the list number to delete</p>

1.4.2 Monitoring and Maintenance

Check and display indicated access control list command:

Command	Description
show access-list-map [{0-399}]	Display access control list map list

1.4.3 Specific Configuration Example

➤ Destination

To filter bytes 123456 from the 40th bytes in the data frame, access type is “deny”. ARP protocol request packet is filtered.

➤ Set up Steps

```
Raisecom#config
Raisecom(config)#access-list-map 0 deny
Raisecom(config-aclmap)#match user-define 123456 ffffff 40
Raisecom(config-aclmap)#exit
Raisecom(config)#access-list-map 1 permit
Raisecom(config-aclmap)# match arp opcode request
Raisecom(config-aclmap)#exit
Raisecom(config)#exit
Raisecom#show access-list-map
access-list-map 0 deny
        Match user-define 123456 ffffff 40
access-list-map 1 permit
        Match arp Opcode request
```

1.5 Application Configuration Based on Hardware ACL

3 steps for using ACL on Layer-2 physical port or VLAN are as follows::

1. Define ACL

Described in section 1.4.

2. Configuration Filter

After setting up ACL, you need to set the filter. Whether the filter is configured successfully depends on if the global status is enabled or not. You can use specific commands to make ACLs effective or to delete the filters that are already take effects. You can user command **no filter** to disable the related rules, if rules have been written in hardware, they will be deleted from the hardware and configurations.

In a physical port or VLAN filter rule can be composed by multi “permit/deny” statements and every statement indicated different size range of data packet. There is a problem of match order while a data packet and access control rule are matching. The match order of access control rule depends on configuration filter rule’s order. The later the order, the higher the priority. If there is conflicts in the rules, high priority will be followed.

There are four kinds of configurations: one is based on switch, one is based on port, one is based from ingress port to egress port, one is based on VLAN. For the filtering rules based on port, you have two options, one of which is based on flow ingress with the other one based on flow egress.

3. Simulate Filter

Use filter command to make the access control rule effect or no effect. Default status is no effect. Once command is configured as effect, not only the earlier configuration filter rules will be effect, but also the later configuration filter rule will effect as well.

1.5.1 Application Default Configuration Based on Hardware ACL

None.

1.5.2 Application Configuration Based on Hardware ACL

1、 Application based on switch

Steps	Command	Description
Step 1	Config	Entry into global configuration mode
Step 2	[no] filter (ip-access-list mac-access-list access-list-map) {acllist / all}	Set filter based on switch ip-access-list indicates that the filter uses IP access list mac-access-list indicates that the filter uses MAC access list access-list-map indicates that the filter uses user-defined access list map <i>acllist / all</i> access control list series number, all means all the configured access control lists
Step 3	filter (enable disable)	enable filter function effect enable disable filter function effect disable
Step 4	exit	Exit global configuration mode and enter privileged EXEC mode
Step 5	show filter	Show all filter status

2. Application based on port

Steps	Command	Description
Step 1	config	Entry into global configuration mode

Step 2	[no] filter (ip-access-list mac-access-list access-list-map) {acllist / all} {ingress / egress} port-list {portlist}	<p>Set filter based on port</p> <p>ip-access-list indicates that the filter uses IP access list</p> <p>mac-access-list indicates that the filter uses MAC access list</p> <p>access-list-map indicates that the filter uses user-defined access list map</p> <p>acllist all access control list series number, all means all the configured access control lists</p> <p>ingress egress means to carry out the filtering on ingress egress</p> <p>port-list the filter is applied to port portlist Physical port list range</p>
Step 3	filter (enable disable)	<p>enable filter function effect enable</p> <p>disable filter function effect disable</p>
Step 4	exit	Exit global configuration mode and enter privileged EXEC mode
Step 5	show filter	Show all filter status

3. Based from ingress port to egress port

Steps	Command	Description
Step 1	config	Entry into global configuration mode
Step 2	[no] filter (ip-access-list mac-access-list access-list-map) {all/ acllist} from ingress-port to egress-port	<p>Set the filter based from ingress port to egress port</p> <p>ip-access-list indicates that the filter uses IP access list</p> <p>mac-access-list indicates that the filter uses MAC access list</p> <p>access-list-map indicates that the filter uses user-defined access list map</p> <p>acllist all access control list series number, all means all the configured access control</p>

		<p>lists</p> <p>from to directions</p> <p>ingress-port ingress port</p> <p>egress-port egress port</p>
Step 3	filter (enable disable)	<p>enable filter function effect enable</p> <p>disable filter function effect disable</p>
Step 4	exit	Exit global configuration mode and enter privileged EXEC mode
Step 5	show filter	Show all filter status

4.Application based on VLAN

Steps	Command	Description
Step 1	config	Entry into global configuration mode
Step 2	[no] filter (ip-access-list mac-access-list access-list-map) {all/ acllist} vlan vlanid	<p>Set the filter based on VLAN</p> <p>ip-access-list indicates that the filter uses IP access list</p> <p>mac-access-list indicates that the filter uses MAC access list</p> <p>access-list-map indicates that the filter uses user-defined access list map</p> <p>acllist all access control list series number, all means all the configured access control lists</p> <p>Vlan the filter is applied to VLAN</p> <p>vlanid VLAN ID</p>
Step 3	filter (enable disable)	<p>enable filter fuction effect enable</p> <p>disable filter fuction effect disable</p>
Step 4	exit	Exit global configuration mode and enter privileged EXEC mode
Step 5	show filter	Show all filter status

1.5.3 Monitoring and Maintenance

Check and display all configuration filter status command:

Command	Description
show filter	Display all configuration filter status

1.5.4 Specific Configuration Examples

Example 1:

➤ Destination

The switch does not allow TCP packet to pass through with destination port 80

➤ Set up steps

```
Raisecom#config
```

```
Raisecom(config)# ip-access-list 0 deny tcp any any 80
```

```
Raisecom(config)# filter ip-access-list 0
```

```
Raisecom(config)#filter enable
```

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

Example 2:

➤ Destination

The switch does not allow ARP packets with the MAC address 000e.3842.34ea to pass through on port 2 to 8.

➤ Set up Steps

```
Raisecom#config
```

```
Raisecom(config)# mac-access-list 2 deny arp any 000e.3842.34ea
```

```
Raisecom(config)# filter mac-access-list 2 ingress portlist 2-8
```

```
Raisecom(config)#filter enable
```

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

Example 3:

➤ Destination

The switch allows IP packets with the source address in network segment 10.0.0.0/8 to pass through in VLAN 3

➤ Set up Steps

```
Raisecom#config
```

```
Raisecom(config)# ip-access-list 2 deny ip any any
```

```

Raisecom(config)# ip-access-list 3 permit ip 10.0.0.0 255.0.0.0 any

Raisecom(config)# filter ip-access-list 2,3 vlan 3

Raisecom(config)#filter enable

Raisecom(config)#exit

```

1.6 Configuration Function Based on Software IP ACL

The steps below show how to use software IP ACL on Layer-3 interface:

1) Define access control list

Show in section 1.2

2) ACL Configuration

Filtering rules on a Layer-3 interface can be combined of one or multiple “permit | deny” sentences, every sentence has different specified packet ranges, so matching order problem may happen when matching one packet and ACL rule. The matching order depends on the orders of configured filtering rules, as the order closer to the back, the higher the priority will be. When conflict happens, high priority will be the benchmark.

1.6.1 Application Default Configuration Based on Software IP ACL

None

1.6.2 Layer-3 Interface Protect Configuration Based on IP ACL

Steps	Command	Description
Step 1	config	Entry into global configuration mode
Step 2	interface ip <0-14>	Enter Layer-3 interface configuration mode
Step 3	[no] ip ip-access-list {all/ acllist}	Set Layer-3 interface filter ip-access-list indicates that the filter uses IP access list acllist all access control list series number, all means all the configured access control lists
Step 4	exit	Exit Ethernet Layer-3 interface configuration mode and enter global configuration mode

Step 5	exit	Exit global configuration mode and enter privileged EXEC mode
Step 6	show interface ip ip-access-list	Show filters status for all interfaces

1.6.3 Monitoring and Maintenance

Check and display configuration filter status command:

Command	Description
show interface ip ip-access-list	Show all filters status for Layer-3 interface

1.6.4 Specific Configuration Example

Example 1:

➤ Destination

Switch only allow IP packet with 10.0.0.0/8 access

➤ Set up steps

```
Raisecom#config
```

```
Raisecom(config)# ip-access-list 2 deny ip any any
```

```
Raisecom(config)# ip-access-list 3 permit ip 10.0.0.0 255.0.0.0 any
```

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

```
Raisecom(config-ip)# ip ip-access-list 2,3
```

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

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



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>