Content

Chapter 1 Commands for ACL

1.1 absolute-periodic/periodic

Command: [no] absolute-periodic {Monday|Tuesday|Wednesday|Thursday|Friday | Saturday|Sunday}<start_time>to{Monday|Tuesday|Wednesday|Thursday|Friday| Saturday| Sunday} <end_time>

[no]periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday}|daily| weekdays | weekend} <start_time> to <end_time>

Functions: Define the time-range of different commands within one week, and every week to circulate subject to this time.

Parameters:

Friday (Friday)

Monday (Monday)

Saturday (Saturday)

Sunday (Sunday)

Thursday (Thursday)

Tuesday (Tuesday)

Wednesday (Wednesday)

daily (Every day of the week)

weekdays (Monday thru Friday)

weekend (Saturday thru Sunday)

start_time start time ,HH:MM:SS (hour: minute: second)

end_time end time,HH:MM:SS (hour: minute: second)

Remark: time-range polling is one minute per time, so the time error shall be <= one minute.

Command Mode: time-range mode

Default: No time-range configuration.

Usage Guide: Periodic time and date. The definition of period is specific time period of Monday to Saturday and Sunday every week.

day1 hh:mm:ss To day2 hh:mm:ss or {[day1+day2+day3+day4+day5+day6+day7]|weekend|weekdays|daily} hh:mm:ss To hh:mm:ss

Examples: Make configurations effective within the period from9:15:30 to 12:30:00 during Tuesday to Saturday.

Switch(config)#time-range admin_timer

Switch(Config-Time-Range-admin_timer)#absolute-periodic Tuesday 9:15:30 to Saturday 12:30:00

Make configurations effective within the period from 14:30:00 to 16:45:00 on Monday,

Wednesday, Friday and Sunday.
Switch(Config-Time-Range-admin_timer)#periodic Monday Wednesday Friday Sunday 14:30:00 to 16:45:00

1.2 absolute start

Command: [no] absolute start <*start_time*> <*start_data*> [end <*end_time*> <*end_data*>]
Functions: Define an absolute time-range, this time-range operates subject to the clock of this equipment.
Parameters: ***start_time*** **:** start time, HH:MM:SS (hour: minute: second)
end_time **:** end time, HH:MM:SS (hour: minute: second)
start_data **:** start data, the format is, YYYY.MM.DD (year.month.day)
end_data **:** end data, the format is, YYYY.MM.DD (year.month.day)
Remark: time-range is one minute per time, so the time error shall be <= one minute.
Command Mode: Time-range mode
Default: No time-range configuration.
Usage Guide: Absolute time and date, assign specific year, month, day, hour, minute of the start, shall not configure multiple absolute time and date, when in repeated configuration, the latter configuration covers the absolute time and date of the former configuration.
Examples: Make configurations effective from 6:00:00 to 13:30:00 from Oct. 1, 2004 to Jan. 26, 2005.
Switch(config)#Time-range admin_timer
Switch(Config-Time-Range-admin_timer)#absolute start 6:00:00 2004.10.1 end 13:30:00 2005.1.26

1.3 access-list deny-preemption

This command is not supported by the switch.

1.4 access-list (ip extended)

Command: access-list <*num*> {deny | permit} icmp {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]
access-list <*num*> {deny | permit} igmp {{<*slpAddr*> <*sMask*>} | any-source |

{host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list <*num*> {deny | permit} tcp {{ <*slpAddr*> <*sMask*> } | any-source | {host-source <*slpAddr*> }} [s-port { <*sPort*> | range <*sPortMin*> <*sPortMax*> }] {{ <*dlpAddr*> <*dMask*> } | any-destination | {host-destination <*dlpAddr*> }} [d-port { <*dPort*> | range <*dPortMin*> <*dPortMax*> }] [ack+ fin+ psh+ rst+ urg+ syn] [precedence <*prec*>] [tos <*tos*>][time-range <*time-range-name*>]

access-list <num> {*deny* | permit} udp *{{* <slpAddr> <*sMask*> *}* | any-source | {host-source <*slpAddr*> }} [s-port *{* <*sPort*> | range <*sPortMin*> <*sPortMax*>] {{ <dlpAddr> <*dMask*> *}* | any-destination | *{host-destination* <dlpAddr> *}} [d-port* { <dPort> | range <dPortMin> <*dPortMax*> }] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list <*num*> {deny | permit} {eigrp | *gre* | *igrp* | ipinip | ip | ospf | <*protocol-num*> } {{ <*slpAddr*> <sMask> } | any-source | *{*host-source <slpAddr> *}} {{ <dlpAddr*> <dMask> } | *any-destination* | {host-destination <dlpAddr> }} *[precedence* <*prec*>] *[tos* <tos>][time-range <*time-range-name*> *]*

no access-list <*num*>

Functions: Create a numeric extended IP access rule to match specific IP protocol or all IP protocol; if access-list of this coded numeric extended does not exist, thus to create such a access-list.

Parameters: <*num*> is the No. of access-list, 100-299; **<*protocol*>** is the No. of upper-layer protocol of ip, 0-255; **<*slpAddr*>** is the source IP address, the format is dotted decimal notation; **<*sMask* >** is the reverse mask of source IP, the format is dotted decimal notation; **<*dlpAddr*>** is the destination IP address, the format is dotted decimal notation; **<*dMask*>** is the reverse mask of destination IP, the format is dotted decimal notation, attentive position o, ignored position1;**<*igmp-type*>**,the type of igmp, 0-15; **<*icmp-type*>**, the type of icmp, 0-255;**<icmp-code>,** protocol No. of icmp, 0-255;**<prec>**, IP priority, 0-7; **<*tos*>**, to value, 0-15; **<*sPort*>**, source port No., 0-65535; **<*sPortMin*>**, the down boundary of source port; **<*sPortMax*>**, the up boundary of source port; **<*dPortMin*>**, the down boundary of destination port; **<*dPortMax*>**, the up boundary of destination port; **<*dPort*>**, destination port No., 0-65535; **<*time-range-name*>**, the name of time-range.

Command Mode: Global mode

Default: No access-lists configured.

Usage Guide: When the user assign specific **<*num*>** for the first time, ACL of the serial number is created, then the lists are added into this ACL; the access list which marked 200-299 can configure not continual reverse mask of IP address.

<*igmp-type*> represent the type of IGMP packet, and usual values please refer to the following description:

17(0x11): IGMP QUERY packet

18(0x12): IGMP V1 REPORT packet

22(0x16): IGMP V2 REPORT packet

23(0x17): IGMP V2 LEAVE packet

34(0x22): IGMP V3 REPORT packet
19(0x13): DVMR packet
20(0x14): PIM V1 packet
Particular notice: The packet types included here are not the types excluding IP OPTION. Normally, IGMP packet contains OPTION fields, and such configuration is of no use for this type of packet. If you want to configure the packets containing OPTION, please directly use the manner where OFFSET is configured.
Examples: Create the numeric extended access-list whose serial No. is 110. deny icmp packet to pass, and permit udp packet with destination address 192. 168. 0. 1 and destination port 32 to pass.
Switch(config)#access-list 110 deny icmp any any-destination
Switch(config)#access-list 110 permit udp any host-destination 192.168.0.1 d-port 32

1.5 access-list (ip standard)

Command: access-list <*num*> {deny | permit} {{<*slpAddr*> <*sMask* >} | any-source| {host-source <*slpAddr*>}}
no access-list <*num*>
Functions: Create a numeric standard IP access-list. If this access-list exists, then add a rule list; the "**no access-list <*num*>**" operation of this command is to delete a numeric standard IP access-list.
Parameters: <*num*> is the No. of access-list, 100-199; **<*slpAddr*>** is the source IP address, the format is dotted decimal notation; **<*sMask* >** is the reverse mask of source IP, the format is dotted decimal notation.
Command Mode: Global mode
Default: No access-lists configured.
Usage Guide: When the user assign specific **<*num*>** for the first time, ACL of the serial number is created, then the lists are added into this ACL.
Examples: Create a numeric standard IP access-list whose serial No. is 20, and permit date packets with source address of 10.1.1.0/24 to pass, and deny other packets with source address of 10.1.1.0/16.
Switch(config)#access-list 20 permit 10.1.1.0 0.0.0.255
Switch(config)#access-list 20 deny 10.1.1.0 0.0.255.255

1.6 access-list(mac extended)

Command: access-list <*num*> {deny | permit} {any-source-mac | {host-source-mac <*host_smac*>} | {<*smac*> <*smac-mask*>}} {any-destination-mac | {host-destination-mac <*host_dmac*>} | {<*dmac*> <*dmac-mask*>}} [untagged-eth2 | tagged-eth2 | untagged-802-3 | tagged-802-3]
no access-list <*num*>
Functions: Define an extended numeric MAC ACL rule, "**no access-list <*num*>**"

command deletes an extended numeric MAC access-list rule.

Parameters: ***<num>*** is the access-list No. which is a decimal's No. from 1100-1199; **deny** if rules are matching, deny access; **permit** if rules are matching, permit access; ***<any-source-mac>*** any source address; ***<any-destination-mac>*** any destination address; ***<host_smac>, <smac>*** source MAC address; ***<smac-mask>*** mask (reverse mask) of source MAC address; ***<host_dmac> , <dmac>*** destination MAC address; ***<dmac-mask>*** mask (reverse mask) of destination MAC address; **untagged-eth2** format of untagged ethernet II packet; **tagged-eth2** format of tagged ethernet II packet; **untagged-802-3** format of untagged ethernet 802.3 packet; **tagged-802-3** format of tagged ethernet 802.3 packet.

Command Mode: Global mode

Default Configuration: No access-list configured

Usage Guide: When the user assign specific <*num*> for the first time, ACL of the serial number is created, then the lists are added into this ACL.

Examples: Permit tagged-eth2 with any source MAC addresses and any destination MAC addresses and the packets pass.

Switch(config)#access-list 1100 permit any-source-mac any-destination-mac tagged-eth2

1.7 access-list(mac-ip extended)

Command:

access-list<*num*>{deny|permit}{any-source-mac| {host-source-mac<*host_smac*>}| {<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}icmp {{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}| any-destination| {host-destination<*destination-host-ip*>}}[<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list<*num*>{deny|permit}{any-source-mac| {host-source-mac<*host_smac*>}| {<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}igmp {{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}| any-destination| {host-destination<*destination-host-ip*>}} [<*igmp-type*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list <*num*> {deny|permit}{any-source-mac| {host-source-mac <*host_smac*> }|{ <*smac*> <*smac-mask*> }}{any-destination-mac| {host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }}tcp {{ <*source*> <*source-wildcard*> }| any-source| {host-source <*source-host-ip*> }}[s-port{ <*port1*> | range <*sPortMin*> <*sPortMax*> }] {{ <*destination*> <destination-wildcard> } | any-destination | {host-destination <destination-host-ip> }} [d-port { <*port3*> | range <*dPortMin*> <*dPortMax*> }] [ack+fin+psh+rst+urg+syn] [precedence <*precedence*>] [tos <*tos*>] [time-range <*time-range-name*>]

access-list <num> *{deny*|permit}{any-source-mac| *{host-source-mac* <host_smac> *}*|{ <*smac*> <*smac-mask*> }}{any-destination-mac| {host-destination-

mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }}udp {{ <*source*> <*source-wildcard*> }|any-source| {host-source <*source-host-ip*> }}[s-port{ <*port1*> | range <*sPortMin*> <*sPortMax*> }] {{ <destination> <*destination-wildcard*> }|any-destination| *{host-destination* <destination-host-ip> *}}[d-port*{ <port3> | *range* <dPortMin> <*dPortMax*> }] [precedence <*precedence*>] [tos <*tos*>][time-range <*time-range-name*>]

access-list <*num*> {deny|permit}{any-source-mac| {host-source-mac <*host_smac*> }|{ <*smac*> <*smac-mask*> }} {any-destination-mac|{host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }} {eigrp|gre|*igrp*|*ip*|*ipinip*|*ospf*|{ <protocol-num> }} *{{* <source> <*source-wildcard*> }|any-source|{*host-source <source-host-ip> }}* {{ <destination> <*destination-wildcard*> }|any-destination| *{host-destination* <destination-host-ip> }} [precedence <precedence>] [tos <tos> *][time-range* <time-range-name>]

Functions: Define an extended numeric MAC-IP ACL rule, no command deletes a extended numeric MAC-IP ACL access-list rule.

Parameters: num access-list serial No. this is a decimal's No. from 3100-3299; **deny** if rules are matching, deny to access; **permit** if rules are matching, permit to access; **any-source-mac**: any source MAC address; **any-destination-mac**: any destination MAC address; **host_smac , smac**: source MAC address; **smac-mask: mask** (reverse mask) of source MAC address ; **host_dmac , dmas** destination MAC address; **dmac-mask** mask (reverse mask) of destination MAC address; **protocol** No. of name or IP protocol. It can be a key word: eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, or an integer from 0-255 of list No. of IP address. Use key word 'ip' to match all Internet protocols (including ICMP, TCP, AND UDP) list; **source-host-ip, source** No. of source network or source host of packet delivery. Numbers of 32-bit binary system with dotted decimal notation expression; host: means the address is the IP address of source host, otherwise the IP address of network; **source-wildcard**: reverse of source IP. Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask; **destination-host-ip**, destination No. of destination network or host to which packets are delivered. Numbers of 32-bit binary system with dotted decimal notation expression; **host:** means the address is the that the destination host address, otherwise the network IP address; **destination-wildcard**: mask of destination. I Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask; **s-port(optional):** means the need to match TCP/UDP source port; **port1(optional):** value of TCP/UDP source interface No., Interface No. is an integer from 0-65535; **d-port(optional)**: means need to match TCP/UDP destination interface; ***<sPortMin>*,** the down boundary of source port; ***<sPortMax>***, the up boundary of source port; **port3(optional)**: value of TCP/UDP destination interface No., Interface No. is an integer from 0-65535; ***<dPortMin>***, the down boundary of destination port;***<dPortMax>***, the up boundary of destination port; **[ack] [fin] [psh] [rst] [urg] [syn]**,(optional) only for TCP protocol, multi-choices of tag positions are available, and when TCP data reports the configuration of corresponding position, then initialization of TCP data report is enabled to form a match when in connection; **precedence** (optional) packets can be filtered by priority which is a number from 0-7; **tos** (optional) packets can be filtered by service type

which ia number from 0-15; **icmp-type** (optional) ICMP packets can be filtered by packet type which is a number from 0-255; **icmp-code** (optional) ICMP packets can be filtered by packet code which is a number from 0-255; **igmp-type** (optional) ICMP packets can be filtered by IGMP packet name or packet type which is a number from 0-255; **<time-range-name>**, name of time range

Command Mode: Global mode

Default Configuration: No access-list configured.

Usage Guide: When the user assign specific <num> for the first time, ACL of the serial number is created, then the lists are added into this ACL; the access list which marked 3200-3299 can configure not continual reverse mask of IP address.

Examples: Permit the passage of TCP packet with source MAC 00-12-34-45-XX-XX, any destination MAC address, source IP address 100.1.1.0 0.255.255.255, and source port 100.

Switch(config)#access-list 3199 permit 00-12-34-45-67-00 00-00-00-00-FF-FF any-destination-mac tcp 100.1.1.0 0.255.255.255 s-port 100 any-destination

1.8 access-list(mac standard)

Command: access-list <*num*> {deny|permit} {any-source-mac | {host-source-mac <*host_smac*> } | {<*smac*> <*smac-mask*>} }

no access-list <num>

Functions: Define a standard numeric MAC ACL rule, no command deletes a standard numeric MAC ACL access-list rule.

Parameters: <*num*> is the access-list No. which is a decimal's No. from 700-799; **deny** if rules are matching, deny access; **permit** if rules are matching, permit access; **<*host_smac*>**, **<*sumac*>** source MAC address; **<*sumac-mask*>** mask (reverse mask) of source MAC address.

Command Mode: Global mode

Default Configuration: No access-list configured.

Usage Guide: When the user assign specific <*num*> for the first time, ACL of the serial number is created, then the lists are added into this ACL.

Examples: Permit the passage of packets with source MAC address 00-00-XX-XX-00-01, and deny passage of packets with source MAC address 00-00-00-XX-00-ab.

Switch(config)# access-list 700 permit 00-00-00-00-00-01 00-00-FF-FF-00-00

Switch(config)# access-list 700 deny 00-00-00-00-00-ab 00-00-00-FF-00-00

1.9 clear access-group statistic

Command: clear access-group statistic [ethernet <*interface-name*>]

Functions: Empty packet statistics information of the specified interface.

Parameters: <*interface-name*>: Interface name.

Command Mode: Admin mode

Default: None
Examples: Empty packet statistics information of interface.
Switch#clear access-group statistic

1.10 firewall

Command: firewall {enable | disable}
Functions: Enable or disable firewall.
Parameters: enable means to enable of firewall; **disable** means to disable firewall.
Default: It is no use if default is firewall.
Command Mode: Global mode
Usage Guide: Whether enabling or disabling firewall, access rules can be configured. But only when the firewall is enabled, the rules can be used in specific orientations of specific ports. When disabling the firewall, all ACL tied to ports will be deleted.
Examples: Enable firewall.
Switch(config)#firewall enable

1.11 ip access extended

Command: ip access extended <*name*>
no ip access extended <*name*>
Function: Create a named extended IP access list. The no prefix will remove the named extended IP access list including all the rules.
Parameters: <name> is the name of the access list. The name can be formed by non-all-digit characters of length of 1 to 32.
Command Mode: Global Mode.
Default: No access list is configured by default.
Usage Guide: When this command is issued for the first time, an empty access list will be created.
Example: To create a extended IP access list name tcpFlow.
Switch(config)#ip access-list extended tcpFlow

1.12 ip access standard

Command: ip access standard <*name*>
no ip access standard <*name*>
Function: Create a named standard access list. The no prefix will remove the named standard access list including all the rules in the list.
Parameters: <*name*> is the name of the access list. The name can be formed by non-all-digit characters of length of 1 to 32.
Command Mode: Global Mode.

Default: No access list is configured by default.
Usage Guide: When this command is issued for the first time, an empty access list will be created.
Example: To create a standard IP access list name ipFlow.
Switch(config)#ip access-list standard ipFlow

1.13 ipv6 access-list

Command: ipv6 access-list <*num-std*> {deny | permit} {<*sIPv6Prefix/sPrefixlen*> | any-source | {host-source <*sIPv6Addr*>}}
no ipv6 access-list <num-std>
Functions: Creates a numbered standard IP access-list, if the access-list already exists, then a rule will add to the current access-list; the "**no access-list {<*num-std*>|<*num-ext*>}** "command deletes a numbered standard IP access-list.
Parameters: **<*num-std*>** is the list number, list range is between 500 ～ 599; **<*sIPv6Prefix*>** is the prefix of the ipv6 source address; **<*sPrefixlen*>** is the length of prefix of the ipv6 source address, range is between 1～128; **<*sIPv6Addr*>** is the ipv6 source address.
Command Mode: Global Mode.
Default: No access-list configured.
Usage Guide: Creates a numbered 520 standard IP access-list first time, the following configuration will add to the current access-list.
Examples: Creates a numbered 520 standard IP access-list, allow the source packet from 2003:1:2:3::1/64 pass through the net, and deny all the other packet from the source address 2003:1:2::1/48 pass through.
Switch (config)#ipv6 access-list 520 permit 2003:1:2:3::1/64
Switch (config)#ipv6 access-list 520 deny 2003:1:2:::1/48

1.14 ipv6 access standard

Command: ipv6 access-list standard <*name*>
no ipv6 access-list standard <*name*>
Function: Create a name-based standard IPv6 access list; the "**no ipv6 access-list standard<*name*>**"command deletes the name-based standard IPv6 access list (including all entries).
Parameter: **<*name*>** is the name for access list, the character string length is from 1 to 32.
Command Mode: Global Mode.
Default: No access list is configured by default.
Usage Guide: When this command is run for the first time, only an empty access list with no entry will be created.
Example: Create a standard IPv6 access list named ip6Flow.

Switch(config)#ipv6 access-list standard ip6Flow

1.15 ipv6 access extended

Command: ipv6 access-list extended <*name*>
no ipv6 access-list extended <*name*>
Function: Create a name-based extended IPv6 access list; the no command delete the name-based extended IPv6 access list.
Parameter: <*name*> is the name for access list, the character string length is from 1 to 32.
Command Mode: Global Mode.
Default: No IP address is configured by default.
Usage Guide: When this command is run for the first time, only an empty access list with no entry will be created.
Example: Create an extensive IPv6 access list named tcpFlow.
Switch (config)#ipv6 access-list extended tcpFlow

1.16 {ip|ipv6|mac|mac-ip} access-group

Command: {ip|ipv6|mac|mac-ip} access-group <*name*> {in} [traffic-statistic]
no {ip|ipv6|mac|mac-ip} access-group <*name*> {in}
Function: Apply an access-list on some direction of port, and determine if ACL rule is added statistic counter or not by options; the no command deletes access-list binding on the port.
Parameter: <*name*> is the name for access list, the character string length is from 1 to 32.
Command Mode: Port Mode
Default: The entry of port is not bound ACL.
Usage Guide: One port can bind ingress rules
Note: when a ACL has multiple rules, traffic-statistic can't configure.

There are four kinds of packet head field based on concerned: MAC ACL, IP ACL, MAC-IP ACL and IPv6 ACL; to some extent, ACL filter behavior (permit, deny) has a conflict when a data packet matches multi types of four ACLs. The strict priorities are specified for each ACL based on outcome veracity. It can determine final behavior of packet filter through priority when the filter behavior has a conflict.

When binding ACL to port, there are some limits as below:

1. Each port can bind a MAC-IP ACL, a IP ACL, a MAC ACL and a IPv6 ACL.

2. When binding four ACLs and data packet matching the multi ACLs simultaneity, the priority from high to low are shown as below,

Ingress IPv6 ACL
Ingress MAC-IP ACL
Ingress MAC ACL

Ingress IP ACL

Example: Binding AAA access-list to entry direction of port.

Switch(Config-If-Ethernet1/0/5)#ip access-group aaa in

1.17 {ip|ipv6|mac|mac-ip} access-group (Interface Mode)

This command is not supported by switch.

1.18 mac access extended

Command: mac-access-list extended <*name*>

no mac-access-list extended <*name*>

Functions: Define a name-manner MAC ACL or enter access-list configuration mode, "**no mac-access-list extended <*name*>**" command deletes this ACL.

Parameters: <*name*> name of access-list excluding blank or quotation mark, and it must start with letter, and the length cannot exceed 32. (remark: sensitivity on capital or small letter.)

Command Mode: Global mode

Default Configuration: No access-lists configured.

Usage Guide: After assigning this command for the first time, only an empty name access-list is created and no list item included.

Examples: Create an MAC ACL named mac_acl.

Switch(config)# mac-access-list extended mac_acl

Switch(Config-Mac-Ext-Nacl-mac_acl)#

1.19 mac-ip access extended

Command: mac-ip-access-list extended <*name*>

no mac-ip-access-list extended <*name*>

Functions: Define a name-manner MAC-IP ACL or enter access-list configuration mode, "**no mac-ip-access-list extended <*name*>**" command deletes this ACL.

Parameters: <*name*>: name of access-list excluding blank or quotation mark, and it must start with letter, and the length cannot exceed 32 (remark: sensitivity on capital or small letter).

Command Mode: Global Mode.

Default: No named MAC-IP access-list.

Usage Guide: After assigning this command for the first time, only an empty name access-list is created and no list item included.

Examples: Create an MAC-IP ACL named macip_acl.

Switch(config)# mac-ip-access-list extended macip_acl
Switch(Config-MacIp-Ext-Nacl-macip_acl)#

1.20 permit | deny (ip extended)

Command: [no] {deny | permit} icmp {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

[no] {deny | permit} igmp {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

[no] {deny | permit} tcp {{ <*slpAddr*> <*sMask*> } | any-source | {host-source <*slpAddr*> }} [s-port { <*sPort*> | range <*sPortMin*> <*sPortMax*> }] {{ <*dlpAddr*> <*dMask*> } | any-destination | {host-destination <*dlpAddr*> }} [d-port { <*dPort*> | range <*dPortMin*> <*dPortMax*> }] [ack+fin+psh+rst+urg+syn] [precedence <*prec*>] [tos <*tos*>][time-range <*time-range-name*>]

[no] {deny | *permit}* udp {{ <*slpAddr*> <sMask> *}* | any-source **| {host-source <*slpAddr*> }} [s-port *{* <*sPort*> | range <*sPortMin*> <*sPortMax*> }] {{ <dlpAddr> <*dMask*> } | any-destination | *{host-destination* <dlpAddr> *}} [*d-port { <*dPort*> | range <*dPortMin*> <*dPortMax*> }] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]**

[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | <*protocol-num*>} {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

Functions: Create a name extended IP access rule to match specific IP protocol or all IP protocol.

Parameters: <*slpAddr*> is the source IP address, the format is dotted decimal notation; **<*sMask* >** is the reverse mask of source IP, the format is dotted decimal notation; **<*dlpAddr*>** is the destination IP address, the format is dotted decimal notation; **<*dMask*>** is the reverse mask of destination IP, the format is dotted decimal notation, attentive position o, ignored position 1; **<*igmp-type*>**, the type of igmp, 0-15; **<*icmp-type*>**, the type of icmp, 0-255 ; **<icmp-code>,** protocol No. of icmp, 0-255; **<prec>**, IP priority, 0-7; **<*tos*>**, to value, 0-15; **<*sPort*>**, source port No., 0-65535; **<*sPortMin*>**, the down boundary of source port; **<*sPortMax*>**, the up boundary of source port; **<*dPort*>**, destination port No. 0-65535; **<*dPortMin*>**, the down boundary of destination port; **<*dPortMax*>**, the up boundary of destination port; **<*time-range-name*>**, time range name.

Command Mode: Name extended IP access-list configuration mode

Default: No access-list configured.

Examples: Create the extended access-list, deny icmp packet to pass, and permit udp

packet with destination address 192. 168. 0. 1 and destination port 32 to pass.
Switch(config)# access-list ip extended udpFlow
Switch(Config-IP-Ext-Nacl-udpFlow)#deny igmp any any-destination
Switch(Config-IP-Ext-Nacl-udpFlow)#permit udp any host-destination 192.168.0.1 d-port 32

1.21 permit | deny(ip standard)

Command: {deny | permit} {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}}

no {deny | permit} {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}}

Functions: Create a name standard IP access rule, and "**no {deny | permit} {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}}**" action of this command deletes this name standard IP access rule.

Parameters: <*slpAddr*> is the source IP address, the format is dotted decimal notation; **<*sMask* >** is the reverse mask of source IP, the format is dotted decimal notation.

Command Mode: Name standard IP access-list configuration mode

Default: No access-list configured.

Example: Permit packets with source address 10.1.1.0/24 to pass, and deny other packets with source address 10.1.1.0/16.

Switch(config)# access-list ip standard ipFlow
Switch(Config-Std-Nacl-ipFlow)# permit 10.1.1.0 0.0.0.255
Switch(Config-Std-Nacl-ipFlow)# deny 10.1.1.0 0.0.255.255

1.22 permit | deny(ipv6 extended)

Command: [no] {deny | permit} icmp {{<*slPv6Prefix/*sPrefixlen>} | any-source | {*host-source* <slPv6Addr>}} *{*<*dlPv6Prefix/*dPrefixlen> | any-destination | {*host-destination* <dlPv6Addr>}} *[*<icmp-type> *[*<icmp-code>]] [*dscp* <dscp>] [*flow-label* <fl>][*time-range* <*time-range-name*>]

[no] {deny | permit} tcp { <*slPv6Prefix*/*sPrefixlen*> | any-source | {host-source <*slPv6Addr*> }} [s-port { <*sPort*> | range <*sPortMin*> <sPortMax> }] { <*dlPv6Prefix/dPrefixlen*> | any-destination | {host-destination <dlPv6Addr> }} [d-port { <*dPort*> | range <*dPortMin*> <*dPortMax*> }] [syn | ack | urg | rst | fin | psh] [dscp <*dscp*>] [flow-label <*fl*>][time-range <*time-range-name*>]

[no] {deny | *permit}* udp { <*slPv6Prefix/sPrefixlen*> | *any-source* | {host-source <*slPv6Addr*> }} [s-port *{* <*sPort*> | *range* <*sPortMin*> <sPortMax> }] { <*dlPv6Prefix/dPrefixlen*> | any-destination | *{host-destination* <dlPv6Addr> *}}* [d-port { <*dPort*> | range <*dPortMin*> <dPortMax> }] [dscp <*dscp*>] [flow-label <*fl*>] [time-range <*time-range-name*>]

[no] {deny | permit} <next-header> *{*<*slPv6Prefix/*sPrefixlen> | *any-source* |

{host-source *<sIPv6Addr>*}} {<dIPv6Prefix/*dPrefixlen*> | any-destination | *{host-destination <dIPv6Addr>*}} [dscp <*dscp>]* [flow-label <fl>*][*time-range <*time-range-name>]*

[no*]* {deny | *permit}* {<sIPv6Prefix/*sPrefixlen*> | *any-source* | {host-source <sIPv6Addr>*}}* {<dIPv6Prefix/dPrefixlen> | any-destination | *{host-destination* <dIPv6Addr>}} [dscp <*dscp*>] [flow-label <*fl*>] [time-range<*time-range-name*>]

Function: Create an *extended* nomenclature IPv6 access control *rule for* specific IPv6 protocol.

Parameter: <*sIPv6Addr*> is the source IPv6 address; **<sPrefixlen>** is the length of the IPv6 address prefix, the range is 1～128; **<dIPv6Addr>** is the destination IPv6 address; **<*dPrefixlen*>** is the length of the IPv6 address prefix, the range is 1～128; **<*igmp-type*>**, type of the IGMP; **<*icmp-type*>**, icmp type; **<*icmp-code*>**, icmp protocol number; **<*dscp*>**, IPv6 priority ,the range is 0～63; **<*flowlabel*>**, value of the flow label, the range is 0～1048575; **syn**,**ack**,**urg**,**rst**,**fin**,**psh**,**tcp** label position; **<*sPort*>**, source port number, the range is 0～65535; **<*sPortMin*>**, the down boundary of source port; **<sPortMax>*,*** the up boundary of source port; **<dPort>,** destination port number, the range is 0～65535; **<*dPortMin*>**, the down boundary of destination port; **<*dPortMax*>**, the up boundary of destination port. **<*next-header*>***,*** the IPv6 next-header. **<*time-range-name*>**, time range name.

Command Mode: IPv6 nomenclature extended access control list mode

Default: No access control list configured.

Example: Create an extended access control list named udpFlow, denying the igmp packets while allowing udp packets with destination address 2001:1:2:3::1 and destination port 32.

Switch(config)#ipv6 access-list extended udpFlow

Switch(Config-IPv6-Ext-Nacl-udpFlow)#deny igmp any any-destination

Switch(Config-IPv6-Ext-Nacl-udpFlow)#permit udp any-source host-destination 2001:1:2:3::1 dPort 32

1.23 permit | deny(ipv6 standard)

Command: [no] {deny | permit} {{<*sIPv6Prefix*/*sPrefixlen*>} | any-source | {host-source <*sIPv6Addr*>}}

Function: Create a standard nomenclature IPv6 access control rule; the no form of this command deletes the nomenclature standard IPv6 access control rule.

Parameter: <*sIPv6Prefix*> is the prefix of the source IPv6 address, **<*sPrefixlen*>** is the length of the IPv6 address prefix, the valid range is 1~128. **<*sIPv6Addr*>** is the source IPv6 address.

Command Mode: Standard IPv6 nomenclature access list mode

Default: No access list configured by default.

Usage Guide:

Example: Permit packets with source address of 2001:1:2:3::1/64 while denying those with source address of 2001:1:2:3::1/48.

Switch(config)#ipv6 access-list standard ipv6Flow
Switch(Config-IPv6-Std-Nacl-ipv6Flow)# permit 2001:1:2:3::1/64
Switch(Config-IPv6-Std-Nacl-ipv6Flow)# deny 2001:1:2:3::1/48

1.24 permit | deny(mac extended)

Command:

[no]{deny|permit} {any-source-mac|{host-source-mac <*host_smac*> }|{ <*smac*> <*smac-mask*> }} {any-destination-mac|{host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }} [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]] [ethertype <*protocol*> [<*protocol-mask*>]]

[no]{deny|permit} {any-source-mac|{host-source-mac <*host_smac*> }|{ <*smac*> <*smac-mask*> }} {any-destination-mac|{host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }} [untagged-eth2 [ethertype <*protocol*> [protocol-mask]]]

[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*> }|{ <*smac*> <*smac-mask*> }} {any-destination-mac|{host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }} [untagged-802-3]

[no]{deny|permit} {any-source-mac|{host-source-mac <*host_smac*> }|{ <*smac*> <*smac-mask*> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac> <*dmac-mask*> }} [tagged-eth2 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]] [ethertype <*protocol*> [<*protocol-mask*>]]]

[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*> }|{ <*smac*> <*smac-mask*> }} {any-destination-mac|{host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }} [tagged-802-3 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]]]

Functions: Define an extended name MAC ACL rule, and no command deletes this extended name IP access rule.

Parameters: any-source-mac: any source of MAC address; **any-destination-mac**: any destination of MAC address; **host_smac**, **smac**: source MAC address; **smac-mask**: mask (reverse mask) of source MAC address; **host_dmac**, **dmas** destination MAC address; **dmac-mask** mask (reverse mask) of destination MAC address; **untagged-eth2** format of untagged ethernet II packet; **tagged-eth2** format of tagged ethernet II packet; **untagged-802-3** format of untagged ethernet 802.3 packet; **tagged-802-3** format of tagged ethernet 802.3 packet; **cos-val:** cos value, 0-7; **cos-bitmask:** cos mask, 0-7reverse mask and mask bit is consecutive; **vid-value:** VLAN No, 1-4094; **vid-bitmask:** VLAN mask, 0-4095, reverse mask and mask bit is consecutive; **protocol:** specific Ethernet protocol No., 1536-65535; **protocol-bitmask:** protocol mask, 0-65535, reverse mask and mask bit is consecutive.

Notice: mask bit is consecutive means the effective bit must be consecutively effective from the first bit on the left, no ineffective bit can be added through. For example: the reverse mask format of one byte is: 00001111b; mask format is 11110000; and this is not permitted: 00010011.
Command Mode: Name extended MAC access-list configuration mode
Default configuration: No access-list configured.
Example: The forward source MAC address is not permitted as 00-12-11-23-XX-XX of 802.3 data packet.
Switch(config)# mac-access-list extended macExt
Switch(Config-Mac-Ext-Nacl-macExt)#deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac untagged-802-3
Switch(Config-Mac-Ext-Nacl-macExt)#deny 00-12-11-23-00-00 00-00-00-00-ff-ff any tagged-802

1.25 permit | deny(mac-ip extended)

Command:
[no] {deny|permit} {any-source-mac|{host-source-mac<*host_smac*>}| {<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} icmp{{<*source*><*source-wildcard*>}| any-source|{host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination|{host-destination <*destination-host-ip*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

[no]{deny|permit}
{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}
igmp{{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}}
{{<*destination*><*destination-wildcard*>}|any-destination|{host-destination <*destination-host-ip*>}} [<*igmp-type*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*> }| { <*smac*> <*smac-mask*> }}{any-destination-mac|{host-destination-mac <*host_dmac*> }|{ <*dmac*> <*dmac-mask*> }}tcp{{ <*source*> <*source-wildcard*> }|any-source| {host-source <*source-host-ip*> }}[s-port { <*port1*> | range <*sPortMin*> <*sPortMax*> }] {{ <*destination*> <*destination-wildcard*> } | any-destination| {host-destination <*destination-host-ip*> }} [d-port { <*port3*> | range <*dPortMin*> <*dPortMax*> }] [ack＋fin＋psh＋rst＋urg＋syn] [precedence <*precedence*>] [tos <*tos*>][time-range <*time-range-name*>]

[no]{deny|*permit}{any-source-mac*|{host-source-mac <*host_smac*> }|{ <*smac*>

<*smac-mask*> }}{any-destination-mac|{host-destination-mac <*host_dmac*> }| { <*dmac*> <*dmac-mask*> }}udp{{ <*source*> <*source-wildcard*> }|any-source| {host-source <*source-host-ip*> }}[s-port{ <*port1*> | range <*sPortMin*> <*sPortMax*> }] {{ <destination> <*destination-wildcard*> }|any-destination| *{host-destination* <destination-host-ip> *}} [d-port* { <port3> | range <dPortMin> <*dPortMax*> }] [precedence <*precedence*>] [tos <*tos*>][time-range <*time-range-name*>]

[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*> <*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}| {<*dmac*><*dmac-mask*>}}{eigrp|gre|igrp|ip|ipinip|ospf|{<*protocol-num*>}} {{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination|{host-destination <*destination-host-ip*>}} [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

Functions: Define an extended name MAC-IP ACL rule, no form deletes one extended numeric MAC-IP ACL access-list rule.

Parameters: num access-list serial No. this is a decimal's No. from 3100-3199; **deny** if rules are matching, deny to access; **permit** if rules are matching, permit to access; **any-source-mac**: any source MAC address; **any-destination-mac**: any destination MAC address; **host_smac**, smac: source MAC address; smac-mask: mask (reverse mask) of source MAC address ; **host_dmac** , dmas destination MAC address; **dmac-mask** mask (reverse mask) of destination MAC address; **protocol** No. of name or IP protocol. It can be a key word: eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, or an integer from 0-255 of list No. of IP address. Use key word 'ip' to match all Internet protocols (including ICMP, TCP, AND UDP) list; **source-host-ip**, source No. of source network or source host of packet delivery. Numbers of 32-bit binary system with dotted decimal notation expression; **host**: means the address is the IP address of source host, otherwise the IP address of network; **source-wildcard**: reverse of source IP. Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask; **destination-host-ip**, destination No. of destination network or host to which packets are delivered. Numbers of 32-bit binary system with dotted decimal notation expression; **host**: means the address is that the destination host address, otherwise the network IP address; **destination-wildcard**: mask of destination. I Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask; **s-port(optional)**: means the need to match TCP/UDP source port; **port1(optional):** value of TCP/UDP source interface No., Interface No. is an integer from 0-65535; ***<sPortMin>***, the down boundary of source port; ***<sPortMax>***, the up boundary of source port; **d-port(optional):** means need to match TCP/UDP destination interface; **port3(optional)**: value of TCP/UDP destination interface No., Interface No. is an integer from 0-65535; ***<dPortMin>***, the down boundary of destination port; ***<dPortMax>***, the up boundary of destination port; **[ack] [fin] [psh] [rst] [urg] [syn]**, (optional) only for TCP protocol, multi-choices of tag positions are available, and when TCP data reports the configuration of corresponding position, then initialization of TCP data report is enabled to form a match when in connection; **precedence (optional)** packets can be filtered by priority which is a

number from 0-7; **tos (optional)** packets can be filtered by service type which ia number from 0-15; **icmp-type (optional)** ICMP packets can be filtered by packet type which is a number from 0-255; **icmp-code (optional)** ICMP packets can be filtered by packet code which is a number from 0-255; **igmp-type (optional)** ICMP packets can be filtered by IGMP packet name or packet type which is a number from 0-255; ***<time-range-name>***, name of time range.

Command Mode: Name extended MAC-IP access-list configuration mode

Default: No access-list configured.

Examples: Deny the passage of UDP packets with any source MAC address and destination MAC address, any source IP address and destination IP address, and source port 100.

Switch(config)# mac-ip-access-list extended macIpExt

Switch(Config-MacIp-Ext-Nacl-macIpExt)# deny any-source-mac any-destination-mac udp any-source s-port 100 any-destination

1.26 show access-lists

Command: show access-lists [<*num*>|<*acl-name*>]

Functions: Reveal ACL of configuration.

Parameters: <*acl-name*>, specific ACL name character string; ***<num>,*** specific ACL No.

Default: None.

Command Mode: Admin Mode

Usage Guide: When not assigning names of ACL, all ACL will be revealed, used x time（s）indicates the times of ACL to be used.

Examples:

Switch#show access-lists

access-list 10(used 0 time(s))

access-list 10 deny any-source

access-list 100(used 1 time(s))

access-list 100 deny ip any any-destination

access-list 100 deny tcp any any-destination

access-list 1100(used 0 time(s))

access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800

Displayed information	Explanation
access-list 10(used 1 time(s))	Number ACL10, 0 time to be used
access-list 10 deny any-source	Deny any IP packets to pass
access-list 100(used 1 time(s))	Nnumber ACL100, 1 time to be used
access-list 100 deny ip any-source any-	Deny IP packet of any source IP address

destination	and destination address to pass
access-list 100 deny tcp any-source any-destination	Deny TCP packet of any source IP address and destination address to pass
access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800	Permit tagged-eth2 with any source MAC addresses and any destination MAC addresses and the packets whose 15th and 16th byte is respectively 0x08 , 0x0 to pass.

1.27 show access-group

Command: show access-group in (interface {Ethernet | Ethernet IFNAME})
Functions: Display the ACL binding status on the port.
Parameters: IFNAME, Port name.
Default: None.
Command Mode: Admin and Configuration Mode.
Usage Guide: When not assigning interface names, all ACL tied to port will be revealed.
Examples:
Switch#show access-group
interface name: Ethernet 1/0/1
IP Ingress access-list used is 100, traffic-statistics Disable.
interface name: Ethernet1/0/2
IP Ingress access-list used is 1, packet(s) number is 11110.

Displayed information	Explanation
interface name: Ethernet 1/0/1	Tying situation on port Ethernet1/0/1
IP Ingress access-list used is 100	No. 100 numeric expansion ACL tied to entrance of port Ethernet1/0/1
packet(s) number is 11110	Number of packets matching this ACL rule

1.28 show firewall

Command: show firewall
Functions: Reveal configuration information of packet filtering functions.
Parameters: None.
Default: None.
Command Mode: Admin and Configuration Mode.
Examples:
Switch#show firewall
Firewall status: Enable.

Displayed information	Explanation
fire wall is enable	Packet filtering function enabled

1.29 show ipv6 access-lists

Command: show ipv6 access-lists [<*num*>|<*acl-name*>]
Function: Show the configured IPv6 access control list.
Parameter:<num> is the number of specific access control list, the valid range is 500～699, amongst 500～599 is digit standard IPv6 ACL number, 600～699 is the digit extended IPv6 ACL number; <acl-name> is the nomenclature character string of a specific access control list, lengthening within 1～32.
Default: None.
Command Mode: Admin and Configuration Mode.
Usage Guide: When no access control list is specified, all the access control lists will be displayed; in used x time（s） is shown the times the ACL had been quoted.
Example:

```
Switch #show ipv6 access-lists
ipv6 access-list 500(used 1 time(s))
  ipv6 access-list 500 deny any-source

ipv6 access-list 510(used 1 time(s))
  ipv6 access-list 510 deny ip any-source any-destination
  ipv6 access-list 510 deny tcp any-source any-destination

ipv6 access-list 520(used 1 time(s))
  ipv6 access-list 520 permit ip any-source any-destination
```

1.30 show time-range

Command: show time-range <*word*>
Functions: Reveal configuration information of time range functions.
Parameters: ***word*** assign name of time-range needed to be revealed.
Default: None.
Command Mode: Admin Mode
Usage Guide: When not assigning time-range names, all time-range will be revealed.
Examples:

```
Switch#show time-range
time-range timer1 (inactive, used 0 times)
      absolute-periodic Saturday 0:0:0 to Sunday 23:59:59
time-range timer2 (inactive, used 0 times)
```

absolute-periodic Monday 0:0:0 to Friday 23:59:59

1.31 time-range

Command: [no] time-range <*time_range_name*>
Functions: Create the name of time-range as time range name, enter the time-range mode at the same time.
Parameters: ***time_range_name***, time range name must start with letter or number, and the length cannot exceed 32 characters long.
Command Mode: Global mode
Default: No time-range configuration.
Usage Guide: None
Examples: Create a time-range named admin_timer.
Switch(config)#Time-range admin_timer

Chapter 2 Commands for Self-defined ACL

2.1 userdefined-access-list standard offset

Command: userdefined-access-list standard offset [window1 { l3start | l4start} <*offset*>] [window2 { l3start | l4start } <*offset*>] [window3 { l3start | l4start } <*offset*>] [window4 { l3start | l4start } <*offset*>] [window5 { l3start | l4start } <*offset*>] [window6 { l3start | l4start } <*offset*>] [window7 { l3start | l4start } <*offset*>] [window8 { l3start | l4start } <*offset*>] [window9 { l3start | l4start } <*offset*>] [window10 { l3start | l4start } <*offset*>] [window11 { l3start | l4start } <*offset*>] [window12 { l3start | l4start } <*offset*>]

no userdefined-access-list standard offset [window1] [window2] [window3] [window4] [window5] [window6] [window7] [window8] [window9] [window10] [window11] [window12]

Function: Create a standard self-defined ACL template. If the template exists, the corresponding window of the template can be modified; the no command deletes the window of the standard self-defined ACL template. If the window is not specified, the standard self-defined ACL template will be deleted.

Parameter:

window1-window12 self-defined window 1 to 12

l3start The start offset position is start of layer3 (It can be effective only when the start of layer3 exists)

l4start The start offset position is start of layer4 (It can be effective only when the start of layer4 exists)

offset The configured offset is from 0 to 178 (unit is 2Bytes)

Command Mode: Global Mode

Default: No Configuration Template

Usage Guide: {l2endoftag | l3start | l4start}: used to configure the start offset position of a window, <*offset*>: used to the offset of a window, the range is <*0-178*>, unit is 2Bytes, namely, 0 means 0Bytes offset and 1 means 2Bytes offset. Standard self-defined ACL template can configure the start offset position and offset for 12 window at most. One standard self-defined ACL template can be shared in global mode. The window cannot be modified if the standard self-defined ACL rule is configured with this window. But if the standard self-defined ACL rule is not configured, the window configuration can be modified with this command.

The no command can delete one or more offset configuration of the window in the template or delete the whole template. The window in the template can be deleted

successfully when it is not used by the self-defined ACL rule.

Ipv6 only supports window1-6, the biggest offset of l3start includes the head of L2, the biggest offset of l4start includes the head of L2 and L3.

Example: Create a global template with 7 windows (3-9) to configure the start offset position and the offset:

Switch(config)#userdefined-access-list standard offset window3 l2 0 window4 l2 2 window5 l3 0 window6 l3 1 window7 l3 2 window8 l4 1 window9 l4 2

2.2 userdefined-access-list extended offset

This command is not supported by switch.

2.3 userdefined-access-list standard

Command: userdefined-access-list standard <1200-1299> {permit|deny} {window1| window2|window3|window4|window5|window6|window7|window8|window9| window10|window11|window12}

no userdefined-access-list standard <1200-1299> {permit|deny} {window1| window2|window3|window4|window5|window6|window7|window8|window9| window10|window11|window12}

Function: Create a numbered standard self-defined ACL. If the standard self-defined ACL exists, then a rule will be added to the ACL. The no command deletes a numbered standard self-defined ACL.

Parameter: <*num*> is the access-list No. from 1200 to 1299 in decimal notation; **deny** if rules are matching, deny access; **permit** if rules are matching, permit access; <value> and <mask> of each window is a 2 bits Hexadecimal number.

Command Mode: Global Mode

Default: No any access-list configured

Usage Guide: When users specify the specified <*num*> for the first time, create the ACL with this serial number, then add the entry into this ACL.

Example: Permit the second bytes of the start of l3 is 0x4501. Permit the packets that the forth byte of the start of l4 is 0xFF.

Switch(config)#userdefined-access-list standard offset window1 l3 0 window2 l4 1

Switch(config)#userdefined-access-list standard 1200 permit window1 4501 FFFF window2 00FF 00FF. Configure a rule in the same list to deny the packets that the fifth and the sixth bytes of the start of l3 is 0xFFAA.

Switch(config)#userdefined-access-list standard offset window3 l3 2

Switch(config)#userdefined-access-list standard 1200 deny any-source-mac any-destination-mac untagged-eth2 window3 FFAA FFFF

2.4 userdefined-access-list extended

This command is not supported by switch.

2.5 userdefined access-group

Command: userdefined access-group <*name*> {in} [traffic-statistic]
no userdefined access-group <*name*> {in}
Function: Apply userdefined-access-list to one direction of the port. Decide whether the statistical counter should be added to the ACL according to the options. The no command deletes the configuration bound to the port.
Parameter: <*name*> is the access-list name from 1200-1399 in decimal notation.
Command Mode: Physical Port Configuration Mode.
Default: userdefined-access-list is not bound to the port
Usage Guide: A self-defined access-list can be bound to the ingress of a port and can be configured at the ingress of the same port with other access-lists at the same time. The deny rule is precedent when different access-lists are matching, that means if there is a access-lists match the deny rule, the deny rule must be executed, the permit rule will be executed oppositely.
Example: The configured self-defined access-list is shown in the following:
Switch(config)#userdefined-access-list standard offset window1 l3 0 window2 l4 1 window3 l3 1
Switch(config)#userdefined-access-list standard 1300 permit window1 4501 FFFF window2 00FF 00FF
Switch(config)#userdefined-access-list standard 1300 deny window1 FFAA0000 FFFF0000
Bind the self-defined access-list to Ethernet1/1:
Switch(config)#interface ethernet1/1
Switch(config-if-ethernet1/1)#userdefined access-group 1300 in

2.6 vacl userdefined access-group

Command: vacl userdefined access-group <*name*> {in} vlan <*vlanId*> [traffic-statistic]
no vacl userdefined access-group <*name*> {in} vlan <*vlanId*>
Function: Apply userdefined-access-list to one direction of the specified VLAN, decide whether the statistical counter should be added to the ACL according to the options or. Theno command deletes the configuration bound to the specified VLAN.
Parameter: <*name*> is the access-list name from 1200 to 1399 in decimal notation; <*vlanId*> the bound VLAN， the range is 1-4095.

Command Mode: Global Mode
Default: userdefined-access-list is not bound to any VLAN
Usage Guide: A self-defined access-list can be bound to the ingress of a VLAN and can be configured at the ingress of the same VLAN with other access-lists at the same time. The deny rule is precedent when different access-lists are matching, that means if there is a access-lists match the deny rule, the deny rule must be executed, the permit rule will be executed oppositely.
Example: The configured self-defined access-list is shown in the following:
Switch(config)#userdefined-access-list standard offset window1 l3 0 window2 l4 1 window3 l3 1
Switch(config)#userdefined-access-list standard 1300 permit window1 4501 FFFF window2 00FF 00FF
Switch(config)#userdefined-access-list standard 1300 deny window1 FFAA0000 FFFF0000
Bind the self-defined access-list to VLAN1:
Switch(config)#vacl userdefined access-group 1300 in vlan 1.

Chapter 3 Commands for 802.1x

3.1 debug dot1x detail

Command: debug dot1x detail {pkt-send | pkt-receive | internal | all | userbased} interface [ethernet] <*interface-name*>

no debug dot1x detail { pkt-send | pkt-receive | internal | all | userbased} interface [ethernet] <*interface-name*>

Function: Enable the debug information of dot1x details; the no operation of this command will disable that debug information.

Parameters: pkt-send: Enable the debug information of dot1x about sending packets;

pkt-receive: Enable the debug information of dot1x about receiving packets;

internal: Enable the debug information of dot1x about internal details;

all: Enable the debug information of dot1x about all details mentioned above;

userbased: user-based authentication;

<*interface-name*>: the name of the interface.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of dot1x details, users can check the detailed processes of the Radius protocol operation, which might help diagnose the cause of faults if there is any.

Example: Enable all debug information of dot1x details on interface1/0/1.

Switch#debug dot1x detail all interface ethernet1/0/1

3.2 debug dot1x error

Command: debug dot1x error

no debug dot1x error

Function: Enable the debug information of dot1x about errors; the no operation of this command will disable that debug information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of dot1x about errors, users can check the information of errors that occur in the processes of the Radius protocol operation, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of dot1x about errors.

Switch#debug dot1x error

3.3 debug dot1x fsm

Command: debug dot1x fsm {all | aksm | asm | basm | ratsm} interface <interface-name>

no debug dot1x fsm {all | aksm | asm | basm | ratsm} interface <interface-name>

Function: Enable the debug information of dot1x state machine; the no operation of this command will disable that debug information.

Command Mode: Admin Mode.

Parameters: all: Enable the debug information of dot1x state machine;

aksm: Enable the debug information of Authenticator Key Transmit state machine;

asm: Enable the debug information of Authenticator state machine;

basm: Enable the debug information of Backend Authentication state machine;

ratsm: Enable the debug information of Re-Authentication Timer state machine;

***<interface-name>*:** the name of the interface.

Usage Guide: By enabling the debug information of dot1x, users can check the negotiation process of dot1x protocol, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of dot1x state machine.

Switch#debug dot1x fsm asm interface ethernet1/0/1

3.4 debug dot1x packet

Command: debug dot1x packet {all | receive | send} interface <*interface-name*>

no debug dot1x packet {all | receive | send} interface <*interface-name*>

Function: Enable the debug information of dot1x about messages; the no operation of this command will disable that debug information.

Command Mode: Admin Mode.

Parameters: send: Enable the debug information of dot1x about sending packets;

receive: Enable the debug information of dot1x about receiving packets;

all: Enable the debug information of dot1x about both sending and receiving packets;

***<interface-name>*:** The name of the interface.

Usage Guide: By enabling the debug information of dot1x about messages, users can check the negotiation process of dot1x protocol, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of dot1x about messages.

Switch#debug dot1x packet all interface ethernet1/0/1

3.5 dot1x accept-mac

Command: dot1x accept-mac <*mac-address*> [interface <*interface-name*>]

no dot1x accept-mac <*mac-address*> [interface <*interface-name*>]

Function: Add a MAC address entry to the dot1x address filter table. If a port is specified, the entry added applies to the specified port only. If no port is specified, the entry added applies to all the ports. The “no dot1x accept-mac <mac-address> [interface <interface-name>]” command deletes the entry from dot1x address filter table.

Parameters: *<mac-address>* stands for MAC address;

<interface-name> for interface name and port number.

Command mode: Global Mode.

Default: N/A.

Usage Guide: The dot1x address filter function is implemented according to the MAC address filter table, dot1x address filter table is manually added or deleted by the user. When a port is specified in adding a dot1x address filter table entry, that entry applies to the port only; when no port is specified, the entry applies to all ports in the switch. When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted, the rest will be rejected.

Example: Adding MAC address 00-01-34-34-2e-0a to the filter table of Ethernet 1/0/5.

Switch(config)#dot1x accept-mac 00-01-34-34-2e-0a interface ethernet 1/0/5

3.6 dot1x eapor enable

Command: dot1x eapor enable

no dot1x eapor enable

Function: Enables the EAP relay authentication function in the switch; the “no dot1x eapor enable” command sets EAP local end authentication.

Command mode: Global Mode.

Default: EAP relay authentication is used by default.

Usage Guide: The switch and RADIUS may be connected via Ethernet or PPP. If an Ethernet connection exists between the switch and RADIUS server, the switch needs to authenticate the user by EAP relay (EAPoR authentication); if the switch connects to the RADIUS server by PPP, the switch will use EAP local end authentication (CHAP authentication). The switch should use different authentication methods according to the connection between the switch and the authentication server.

Example: Setting EAP local end authentication for the switch.

Switch(config)#no dot1x eapor enable

3.7 dot1x enable

Command: dot1x enable

no dot1x enable

Function: Enables the 802.1x function in the switch and ports: the "**no dot1x enable**" command disables the 802.1x function.

Command mode: Global Mode and Port Mode.

Default: 802.1x function is not enabled in global mode by default; if 802.1x is enabled under Global Mode, 802.1x will not be enabled for the ports by default.

Usage Guide: The 802.1x authentication for the switch must be enabled first to enable 802.1x authentication for the respective ports. If Spanning Tree or MAC binding is enabled on the port, or the port is a Trunk port or member of port aggregation group, 802.1x function cannot be enabled for that port unless such conditions are removed.

Example: Enabling the 802.1x function of the switch and enable 802.1x for port1/0/12.

Switch(config)#dot1x enable

Switch(config)#interface ethernet 1/0/12

Switch(Config-If-Ethernet1/0/12)#dot1x enable

3.8 dot1x ipv6 passthrough

Command: dot1x ipv6 passthrough

no dot1x ipv6 passthrough

Function: Enable IPv6 passthrough function on a switch port, only applicable when access control mode is userbased; the no operation of this command will disable the function.

Command Mode: Port Configuration Mode.

Default Settings: IPv6 passthrough function is disabled on the switch by default.

Usage Guide: The function can only be enabled when 802.1x function is enabled both globally and on the port, with userbased being the control access mode. After it is enabled, users can send IPv6 messages without authentication.

Examples: Enable IPv6 passthrough function on port Ethernet1/0/12.

Switch(config)#dot1x enable

Switch(config)#interface ethernet 1/0/12

Switch(Config-If-Ethernet1/0/12)#dot1x enable

Switch(Config-If-Ethernet1/0/12)#dot1x ipv6 passthrough

3.9 dot1x guest-vlan

Command: dot1x guest-vlan <*vlanid*>

no dot1x guest-vlan

Function: Set the guest-vlan of the specified port; the "**no dot1x guest-vlan**" command is used to delete the guest-vlan.
Parameters: ***<vlanid>*** the specified VLAN id, ranging from 1 to 4094.
Command Mode: Port Mode.
Default Settings: There is no 802.1x guest-vlan function on the port.
User Guide: The access device will add the port into Guest VLAN if there is no supplicant getting authenticated successfully in a certain stretch of time because of lacking exclusive authentication supplicant system or the version of the supplicant system being too low.
In Guest VLAN, users can get 802.1x supplicant system software, update supplicant system or update some other applications (such as anti-virus software, the patches of operating system). When a user of a port within Guest VLAN starts an authentication, the port will remain in Guest VLAN in the case of a failed authentication. If the authentication finishes successfully, there are two possible results:

- ☞ The authentication server assigns an Auto VLAN, causing the port to leave Guest VLAN to join the assigned Auto VLAN. After the user gets offline, the port will be allocated back into the specified Guest VLAN.
- ☞ The authentication server assigns an Auto VLAN, then the port leaves Guest VLAN and joins the specified VLAN. When the user becomes offline, the port will be allocated to the specified Guest VLAN again.

Attention:

- ☞ There can be different Guest VLAN set on different ports, while only one Guest VLAN is allowed on one port.
- ☞ Only when the access control mode is portbased, the Guest VLAN can take effect. If the access control mode of the port is macbased or userbased, the Guest VLAN can be successfully set without taking effect.

Examples： Set Guest-VLAN of port Ethernet1/0/3 as VLAN 10.
Switch(Config-If-Ethernet1/0/3)#dot1xguest-vlan 10

3.10 dot1x macfilter enable

Command: dot1x macfilter enable
no dot1x macfilter enable
Function: Enables the dot1x address filter function in the switch; the "**no dot1x macfilter enable**" command disables the dot1x address filter function.
Command mode: Global Mode
Default: dot1x address filter is disabled by default.
Usage Guide: When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted.
Example: Enabling dot1x address filter function for the switch.
Switch(config)#dot1x macfilter enable

3.11 dot1x macbased guest-vlan

Command: dot1x macbased guest-vlan <vlanid>

no dot1x macbased guest-vlan

Function: Configure to appoint the port's guest-vlan based on the mac authentication; the no command deletes this guest-vlan.

Parameters: <vlanid>: the configured vlan id, the range is from 1 to 4094.

Command mode: Port Mode.

Default: Do not configure 802.1x macbased guest-vlan.

Usage Guide: If there is no dedicated authentication client or the client version was too low, and it makes no clients authenticate successfully on the port in some time, then the access device will make this user join to the guest VLAN. User can get the 802.1x client software in guest VLAN, update the client or do other updating things (such as anti-virus software, system patches and etc.) When the user under the port in Guest VLAN issues the authentication, this port will be stay in guest VLAN if the authentication failed; if it was successful, there are two situations as below:

1. The authentication server issues an auto VLAN, in this time, the user left the guest VLAN and joined to the auto VLAN. After the user was downline, this user will be assigned to the configured guest VLAN again.

2. The authentication server did not issue the VLAN, in this time, the user left the guest VLAN and joined to the configured native VLAN. After the user was downline, this user will be assigned to the configured guest VLAN again.

Notice:

1. dot1x macbased guest-vlan can be configured only on the port based on mac authentication and in HYBRID mode.

2. Different macbased guestVLAN can be configured on different ports, but only one macbased guestVLAN can be configured on one port.

Example: Configure the guest-vlan of Ethernet1/0/3 as Vlan 10.

Switch(Config-If-Ethernet1/0/3)#dot1x macbased guest-vlan 10

3.12 dot1x macbased port-down-flush

Command: dot1x macbased port-down-flush

no dot1x macbased port-down-flush

Function: Enables this command, when the dot1x certification according to mac is down, delete the user who passed the certification of the port; The no command does not make the down operation.

Command mode: Global Mode

Default: The command is not enabled by default.

Usage Guide: When users who passed the certification according to mac changed among different ports, delete the user for the new certification. The command should be enable to delete the user.

Example: When the dot1x certification according to mac is down, delete the user who passed the certification of the port.
Switch(config)#dot1x macbased port-down-flush

3.13 dot1x max-req

Command: dot1x max-req <*count*>
no dot1x max-req
Function: Sets the number of EAP request/MD5 frame to be sent before the switch re-initials authentication on no supplicant response; the "no dot1x max-req" command restores the default setting.
Parameters: <*count*> is the times to re-transfer EAP request/ MD5 frames, the valid range is 1 to 10.
Command mode: Global Mode.
Default: The default maximum for retransmission is 2.
Usage Guide: The default value is recommended in setting the EAP request/ MD5 retransmission times.
Example: Changing the maximum retransmission times for EAP request/ MD5 frames to 5 times.
Switch(config)#dot1x max-req 5

3.14 dot1x user allow-movement

Command: dot1x user allow-movement
no dot1x user allow-movement
Function: Enable the authentication function after the user moves the port, the no command disables the function.
Command Mode: Global mode
Default: Disable the authentication function after the user moves the port.
Usage Guide: Enable the authentication function after the user moves the port, so the switch allows user to process this authentication. In the condition that the switch connects with hub, when the user will be moved to other port, dot1x user allow-movement command should be enabled.
Example: Enable the authentication function after the user moves the port.
Switch(config)#dot1x user allow-movement

3.15 dot1x user free-resource

Command: dot1x user free-resource <*prefix*> <*mask*>
no dot1x user free-resource
Function: To configure 802.1x free resource; the no form command closes this function.

Parameter: <*prefix*> is the segment for limited resource, in dotted decimal format;
<*mask*> is the mask for limited resource, in dotted decimal format.
Command Mode: Global Mode.
Default: There is no free resource by default.
Usage Guide: This command is available only if user based access control is applied. If user based access control has been applied, this command configures the limited resources which can be accessed by the un-authenticated users. For port based and MAC based access control, users could access no network resources before authentication.

If TrustView management system is available, the free resource can be configured in TrustView server, and the TrustView server will distribute the configuration to the switches.

To be noticed, only one free resource can be configured for the overall network.
Example: To configure the free resource segment as 1.1.1.0, the mask is 255.255.255.0.
Switch(Config)#dot1x user free-resource 1.1.1.0 255.255.255.0

3.16 dot1x max-user macbased

Command: dot1x max-user macbased <*number*>
no dot1x max-user macbased
Function: Sets the maximum users allowed connect to the port; the “no dot1x max-user” command restores the default setting.
Parameters: <*number*> is the maximum users allowed, the valid range is 1 to 256.
Command mode: Port configuration Mode.
Default: The default maximum user allowed is 1.
Usage Guide: This command is available for ports using MAC-based access management, if MAC address authenticated exceeds the number of allowed user, additional users will not be able to access the network.
Example: Setting port 1/0/3 to allow 5 users.
Switch(Config-If-Ethernet1/0/3)#dot1x max-user macbased 5

3.17 dot1x max-user userbased

Command: dot1x max-user userbased <number>
no dot1x max-user userbased
Function: Set the upper limit of the number of users allowed access the specified port when using user-based access control mode; the no command is used to reset the default value.
Parameters: <*number*> the maximum number of users allowed to access the network, ranging from 1 to 1~256.
Command Mode: Port Mode.
Default Settings: The maximum number of users allowed to access each port is 10 by

default.

User Guide: This command can only take effect when the port adopts user-based access control mode. If the number of authenticated users exceeds the upper limit of the number of users allowed access the network, those extra users can not access the network.

Examples: Setting port 1/0/3 to allow 5 users.

Switch(Config-If-Ethernet1/0/3)#dot1x max-user userbased 5

3.18 dot1x portbased mode single-mode

Command: dot1x portbased mode single-mode

no dot1x portbased mode single-mode

Function: Set the single-mode based on portbase authentication mode; the no command disables this function.

Parameters: None.

Command mode: Port Mode

Default: Disable the single-mode.

Usage Guide: This command takes effect when the access mode of the port is set as portbase only. Before configuring the single-mode, if the port has enabled dot1x port-method portbased command and exist online users, the switch will enforce all users of this port are offline. After that, this port only allows a user to pass the authentication, the user can access the specified network resource, but other authentication users of this port will be denied and can not access the network. After disabling the single-mode, the switch also enforce the authenticated user is offline.

Example:

Switch(Config-If-Ethernet1/0/1)#dot1x portbased mode single-mode

3.19 dot1x port-control

Command: dot1x port-control {auto | force-authorized | force-unauthorized}

no dot1x port-control

Function: Sets the 802.1x authentication status; the “no dot1x port-control” command restores the default setting.

Parameters: auto enable 802.1x authentication, the port authorization status is determined by the authentication information between the switch and the supplicant; **force-authorized** sets port to authorized status, unauthenticated data is allowed to pass through the port; **force-unauthorized** will set the port to non-authorized mode, the switch will not provide authentication for the supplicant and prohibit data from passing through the port.

Command mode: Port configuration Mode

Default: When 802.1x is enabled for the port, **auto** is set by default.

Usage Guide: If the port needs to provide 802.1x authentication for the user, the port

authentication mode should be set to auto.

Example: Setting port1/0/1 to require 802.1x authentication mode.

Switch(config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#dot1x port-control auto

3.20 dot1x port-method

Command: dot1x port-method {macbased | portbased | userbased {standard | advanced}}

no dot1x port-method

Function: To configure the access control method of appointed interface. The no form command restores the default access control method.

Parameter: macbased means the access control method based on MAC address

portbased means the access control method based on port

userbased means the access control method based on user, it can be divided into two types, one is standard access control method, and the other is advanced access control method

Command mode: Port Configuration Mode.

Default: Advanced access control method based on user is used by default.

Usage Guide: This command is used to configure the dot1x authentication method for the specified port. When port based authentication is applied, only one host can authenticate itself through one port. And after authentication, the host will be able to access all the resources. When MAC based authentication is applied, multiple host which are connected to one port can access all the network resources after authentication. When either of the above two kinds of access control is applied, un-authenticated host cannot access any resources in the network.

When user based access control is applied, un-authenticated users can only access limited resources of the network. The user based access control falls into two kinds – the standard access control and the advanced access control. The standard user based access control does not limit the access to the limited resources when the host is not authenticated yet. While the user based advanced access control can control the access to the limited resources before authentication is done.

Notes: For standard control method based on user, the 802.1x free resource must be configured first, and it needs to be used with dot1x privateclient enable.

Example: To configure the access control method based on port for Etherent1/0/4.

Switch(Config-If-Ethernet1/0/4)#dot1x port-method portbased

3.21 dot1x privateclient enable

Command: dot1x privateclient enable

no dot1x privateclient enable

Function: To configure the switch to force the authentication client to use private 802.1x

authentication protocol. The no prefix will disable the command and allow the authentication client to use the standard 802.1x authentication protocol.
Command Mode: Global Mode.
Default: Private 802.1x authentication packet format is disabled by default.
Usage Guide: To implement integrated solution, the switch must be enabled to use private 802.1x protocol, or many applications will not be able to function. For detailed information, please refer to DCBI integrated solution. If the switch forces the authentication client to use private 802.1x protocol, the standard client will not be able to work.
Example: To force the authentication client to use private 802.1x authentication protocol.
Switch(config)#dot1x privateclient enable

3.22 dot1x privateclient protect enable

Command: dot1x privateclient protect enable
no dot1x privateclient protect enable
Function: Enable the privateclient protect function of the switch, the no command disables the protect function.
Parameter: None.
Command mode: Global Mode
Default: Disable the privateclient protect function.
Usage Guide: Support the partial encryption of the privateclient protocol to advance the security of the privateclient.
Example: Enable the privateclient protect function of the switch.
Switch(config)#dot1x privateclient protect enable

3.23 dot1x re-authenticate

Command: dot1x re-authenticate [interface <*interface-name*>]
Function: Enables real-time 802.1x re-authentication (no wait timeout requires) for all ports or a specified port.
Parameters: **<*interface-name*>** stands for port number, omitting the parameter for all ports.
Command mode: Global Mode.
Usage Guide: This command is a Global Mode command. It makes the switch to re-authenticate the client at once without waiting for re-authentication timer timeout. This command is no longer valid after authentication.
Example: Enabling real-time re-authentication on port1/0/8.
Switch(config)#dot1x re-authenticate interface ethernet 1/0/8

3.24 dot1x re-authentication

Command: dot1x re-authentication
no dot1x re-authentication
Function: Enables periodical supplicant authentication; the “no dot1x re-authentication” command disables this function.
Command mode: Global Mode.
Default: Periodical re-authentication is disabled by default.
Usage Guide: When periodical re-authentication for supplicant is enabled, the switch will re-authenticate the supplicant at regular interval. This function is not recommended for common use.
Example: Enabling the periodical re-authentication for authenticated users.
Switch(config)#dot1x re-authentication

3.25 dot1x timeout quiet-period

Command: dot1x timeout quiet-period <*seconds*>
no dot1x timeout quiet-period
Function: Sets time to keep silent on supplicant authentication failure; the “**no dot1x timeout quiet-period**” command restores the default value.
Parameters: <*seconds*> is the silent time for the port in seconds, the valid range is 1 to 65535.
Command mode: Global Mode.
Default: The default value is 10 seconds.
Usage Guide: Default value is recommended.
Example: Setting the silent time to 120 seconds.
Switch(config)#dot1x timeout quiet-period 120

3.26 dot1x timeout re-authperiod

Command: dot1x timeout re-authperiod <*seconds*>
no dot1x timeout re-authperiod
Function: Sets the supplicant re-authentication interval; the “**no dot1x timeout re-authperiod**” command restores the default setting.
Parameters: <*seconds*> is the interval for re-authentication, in seconds, the valid range is 1 to 65535.
Command mode: Global Mode.
Default: The default value is 3600 seconds.
Usage Guide: dot1x re-authentication must be enabled first before supplicant re-authentication interval can be modified. If authentication is not enabled for the switch, the supplicant re-authentication interval set will not take effect.

Example: Setting the re-authentication time to 1200 seconds.
Switch(config)#dot1x timeout re-authperiod 1200

3.27 dot1x timeout tx-period

Command: dot1x timeout tx-period *<seconds>*
no dot1x timeout tx-period
Function: Sets the interval for the supplicant to re-transmit EAP request/identity frame; the "**no dot1x timeout tx-period**" command restores the default setting.
Parameters: *<seconds>* is the interval for re-transmission of EAP request frames, in seconds; the valid range is 1 to 65535.
Command mode: Global Mode.
Default: The default value is 30 seconds.
Usage Guide: Default value is recommended.
Example: Setting the EAP request frame re-transmission interval to 1200 seconds.
Switch(config)#dot1x timeout tx-period 1200

3.28 dot1x unicast enable

Command: dot1x unicast enable
no dot1x unicast enable
Function: Enable the 802.1x unicast passthrough function of switch; the no operation of this command will disable this function.
Command mode: Global Configuration Mode.
Default: The 802.1x unicast passthrough function is not enabled in global mode.
Usage Guide: The 802.1x unicast passthrough authentication for the switch must be enabled first to enable the 802.1x unicast passthrough function, then the 802.1x function is configured.
Example: Enabling the 802.1x unicast passthrough function of the switch and enable the 802.1x for port 1/0/1.
Switch(config)#dot1x enable
Switch(config)# dot1x unicast enable
Switch(config)#interface ethernet1/0/1
Switch(Config-If-Ethernet1/0/1)#dot1x enable

3.29 dot1x web authentication enable

This command is not supported by switch.

3.30 dot1x web authentication ipv6 passthrough

This command is not supported by switch.

3.31 dot1x web redirect

This command is not supported by switch.

3.32 dot1x web redirect enable

This command is not supported by switch.

3.33 show dot1x

Command: show dot1x [interface <*interface-list*>]
Function: Displays dot1x parameter related information, if parameter information is added, corresponding dot1x status for corresponding port is displayed.
Parameters: ***<interface-list>*** is the port list. If no parameter is specified, information for all ports is displayed.
Command mode: Admin and Configuration Mode.
Usage Guide: The dot1x related parameter and dot1x information can be displayed with "show dot1x" command.
Example:
1. Display information about dot1x global parameter for the switch.

```
Switch#show dot1x
Global 802.1x Parameters
  reauth-enabled        no
  reauth-period         3600
  quiet-period          10
  tx-period             30
  max-req               2
  authenticator mode    passive

Mac Filter Disable
MacAccessList :
dot1x-EAPoR Enable
dot1x-privateclient Disable
dot1x-unicast Disable
```

802.1x is enabled on ethernet Ethernet1/0/1
Authentication Method:Port based
Max User Number:1
  Status Authorized
  Port-control Auto
  Supplicant 00-03-0F-FE-2E-D3

Authenticator State Machine
  State Authenticated
Backend State Machine
  State Idle
Reauthentication State Machine
  State Stop

Displayed information	Explanation
Global 802.1x Parameters	Global 802.1x parameter information
reauth-enabled	Whether re-authentication is enabled or not
reauth-period	Re-authentication interval
quiet-period	Silent interval
tx-period	EAP retransmission interval
max-req	EAP packet retransmission interval
authenticator mode	Switch authentication mode
Mac Filter	Enables dot1x address filter or not
MacAccessList	Dot1x address filter table
dot1x-EAPoR	Authentication method used by the switch (EAP relay, EAP local end)
dot1x-privateclient	Whether the switch supports the privateclient
802.1x is enabled on ethernet Ethernet1/0/1	Indicates whether dot1x is enabled for the port
Authentication Method:	Port authentication method (MAC-based, port-based, user-based)
Status	Port authentication status
Port-control	Port authorization status
Supplicant	Authenticator MAC address
Authenticator State Machine	Authenticator state machine status
Backend State Machine	Backend state machine status
Reauthentication State Machine	Re-authentication state machine status

3.34 user-control limit

This command is not supported by switch.

3.35 user-control limit ipv6

This command is not supported by switch.

Chapter 4 Commands for the Number Limitation Function of MAC and IP in Port, VLAN

4.1 debug ip arp count

Command: debug ip arp count
no debug ip arp count
Function: When the number limitation function debug of ARP in the VLAN, if the number of dynamic ARP and the number of ARP in the VLAN is larger than the max number allowed, users will see debug information." **no debug ip arp count**" command is used to disable the number limitation function debug of ARP in the VLAN.
Parameters: None.
Command Mode: Admin Mode.
Default Settings: None.
Usage Guide: Display the debug information of the number of dynamic ARP in the VLAN.
Examples:
Switch#debug vlan mac count
%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the maximum limit in vlan 1!!
%Jun 14 16:04:40 2007Arp learning will be stopped and some arp will be delete !!

4.2 debug ipv6 nd count

Command: debug ipv6 nd count
no debug ipv6 nd count
Function: When the number limitation function debug of neighbor in the VLAN, if the number of dynamic neighbor and the number of neighbor in the VLAN is larger than the max number allowed, users will see debug information. "**no debug ip neighbor count**" command is used to disable the number limitation function debug of neighbor in the VLAN.
Parameters: None.
Command Mode: Admin Mode.
Default Settings: None.
Usage Guide: Display the debug information of the number of dynamic neighbor in the VLAN.
Examples:

Switch#debug vlan mac count
%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the maximum limit in vlan 1!!

4.3 debug switchport arp count

Command: debug switchport arp count
no debug switchport arp count
Function: When the number limitation function debug of ARP on the port, if the number of dynamic ARP and the number of ARP on the port is larger than the max number allowed, users will see debug information." **no debug switchport arp count**" command is used to disable the number limitation function debug of ARP on the port.
Parameters: None
Command Mode: Admin Mode
Default Settings: None
Usage Guide: Display the debug information of the number of dynamic ARP on the port.
Examples:
Switch#debug switchport arp count
%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the maximum limit in port Ethernet3/1
!!%Jun 14 16:04:40 2007 Arp learning will be stopped and some mac will be delete !!

4.4 debug switchport mac count

Command: debug switchport mac count
no debug switchport mac count
Function: When the number limitation function debug of MAC on the port, if the number of dynamic MAC and the number of MAC on the port is larger than the max number allowed, users will see debug information. "**no debug switchport mac count**" command is used to disable the number limitation function debug of MAC on the port.
Parameters: None
Command Mode: Admin Mode
Default Settings: None
Usage Guide: Display the debug information of the number of dynamic MAC on the port.
Examples:
Switch#debug switchport mac count
%Jun 14 16:04:40 2007 Current mac count 21 is more than or equal to the maximum limit in port Ethernet3/1
!!%Jun 14 16:04:40 2007 Mac learning will be stopped and some mac will be delete !!

4.5 debug switchport nd count

Command: debug switchport nd count

no debug switchport nd count

Function: When the number limitation function debug of ND on the port, if the number of dynamic ND and the number of ND on the port is larger than the max number allowed, users will see debug information. "**no debug switchport nd count**" command is used to disable the number limitation function debug of ND on the port.

Parameters: None

Command Mode: Admin Mode

Default Settings: None

Usage Guide: Display the debug information of the number of dynamic ND on the port

Examples:

Switch#debug switchport arp count

%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the maximum limit in port Ethernet3/1

!!%Jun 14 16:04:40 2007 Neighbor learning will be stopped and some mac will be delete !!

4.6 ip arp dynamic maximum

Command: ip arp dynamic maximum <*value*>

no ip arp dynamic maximum

Function: Set the max number of dynamic ARP allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic ARP in the VLAN; "**no ip arp dynamic maximum**" command is used to disable the number limitation function of dynamic ARP in the VLAN.

Parameters: <*value*> upper limit of the number of dynamic ARP in the VLAN, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic ARP in the VLAN is disabled.

Command Mode: Interface Configuration Mode.

Usage Guide: When configuring the max number of dynamic ARP allowed in the VLAN, if the number of dynamically learnt ARP in the VLAN is already larger than the max number to be set, the extra dynamic ARP will be deleted.

Examples:

Enable the number limitation function of dynamic ARP in VLAN 1, the max number to be set is 50.

Switch(config)#interface ethernet

Switch(Config-if-Vlan1)# ip arp dynamic maximum 50

Disable the number limitation function of dynamic ARP in VLAN 1.

Switch(Config-if-Vlan1)#no ip arp dynamic maximum

4.7 ipv6 nd dynamic maximum

Command: ipv6 nd dynamic maximum <*value*>
no ipv6 nd dynamic maximum

Function: Set the max number of dynamic NEIGHBOR allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic NEIGHBOR in the VLAN; "**no ipv6 nd dynamic maximum**" command is used to disable the number limitation function of dynamic NEIGHBOR in the VLAN.

Parameters: <*value*> upper limit of the number of dynamic NEIGHBOR in the VLAN, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic NEIGHBOR in the VLAN is disabled.

Command Mode: Interface Configuration Mode.

Usage Guide: When configuring the max number of dynamic NEIGHBOR allowed in the VLAN, if the number of dynamically learnt NEIGHBOR in the VLAN is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted.

Examples:

Enable the number limitation function of dynamic NEIGHBOR in VLAN 1, the max number to be set is 50.

Switch(config)#interface ethernet

Switch(Config-if-Vlan1)# ipv6 nd dynamic maximum 50

Disable the number limitation function of dynamic NEIGHBOR in VLAN 1.

Switch(Config-if-Vlan1)#no ipv6 nd dynamic maximum

4.8 show arp-dynamic count

Command: show arp-dynamic count {(vlan <1-4096>)| interface ethernet <*portName*>}

Function: Display the number of dynamic ARP of corresponding port and VLAN.

Parameters: <*vlan-id*> is the specified vlan ID.

<*portName*> is the name of layer-2 port.

Command Mode: Admin and Configuration Mode.

Usage Guide: Use this command to display the number of dynamic ARP of corresponding port and VLAN.

Examples: Display the number of dynamic ARP of the port and VLAN which are configured with number limitation function of ARP.

Switch(config)# show arp-dynamic count interface ethernet 1/0/3

Port	MaxCount	CurrentCount

```
 Ethernet1/0/3          5              1
-------------------------------------------------------------------------------------------------
Switch(config)# show arp-dynamic count vlan 1
  Vlan          MaxCount          CurrentCount
-------------------------------------------------------------------------------------------------
 1              55              15
-------------------------------------------------------------------------------------------------
```

4.9 show mac-address dynamic count

Command: show mac-address dynamic count { (vlan <1-4096>)| interface ethernet *<portName>*}

Function: Display the number of dynamic MAC of corresponding port and VLAN.

Parameters: <*vlan-id*> display the specified VLAN ID.

<*portName*> is the name of layer-2 port.

Command Mode: Any mode

Usage Guide: Use this command to display the number of dynamic MAC of corresponding port and VLAN.

Examples: Display the number of dynamic MAC of the port and VLAN which are configured with number limitation function of MAC.

```
Switch(config)# show mac-address dynamic count interface ethernet 1/0/3
  Port          MaxCount          CurrentCount
-------------------------------------------------------------------------------------------------
 Ethernet1/0/3          5              1
-------------------------------------------------------------------------------------------------
 Switch(config)# show mac-address dynamic count vlan 1
  Vlan          MaxCount          CurrentCount
-------------------------------------------------------------------------------------------------
 1              55              15
-------------------------------------------------------------------------------------------------
```

4.10 show nd-dynamic count

Command: show nd-dynamic count {(vlan <1-4096>)| interface ethernet *<portName>*}

Function: Display the number of dynamic ND of corresponding port and VLAN.

Parameters: <*vlan-id*> is play the specified vlan ID. **<*portName*>** is the name of layer-2 port.

Command Mode: Admin and Configuration Mode.

Usage Guide: Use this command to display the number of dynamic ND of corresponding port and VLAN.

Examples: Display the number of dynamic ND of the port and VLAN which are

configured with number limitation function of ND.

```
Switch(config)# show nd-dynamic count interface ethernet 1/0/3
  Port          MaxCount          CurrentCount
-------------------------------------------------------------------------------------------------
 Ethernet1/0/3          5              1
-------------------------------------------------------------------------------------------------
Switch(config)# show nd-dynamic count vlan 1
  Vlan          MaxCount          CurrentCount
-------------------------------------------------------------------------------------------------
 1              55             15
-------------------------------------------------------------------------------------------------
```

4.11 switchport arp dynamic maximum

Command: switchport arp dynamic maximum <*value*>

no switchport arp dynamic maximum

Function: Set the max number of dynamic ARP allowed by the port, and, at the same time, enable the number limitation function of dynamic ARP on the port; "**no switchport arp dynamic maximum**" command is used to disable the number limitation function of dynamic ARP on the port.

Parameters: <*value*> upper limit of the number of dynamic ARP of the port, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic ARP on the port is disabled.

Command Mode: Port mode.

Usage Guide: When configuring the max number of dynamic ARP allowed by the port, if the number of dynamically learnt ARP on the port is already larger than the max number to be set, the extra dynamic ARP will be deleted. TRUNK ports do not supports this function.

Examples:

Enable the number limitation function of dynamic ARP in port 1/0/2 mode, the max number to be set is 20

```
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)# switchport arp dynamic maximum 20
```

Disable the number limitation function of dynamic ARP in port 1/0/2 mode

```
Switch(Config-If-Ethernet1/0/2)#no switchport arp dynamic maximum
```

4.12 switchport mac-address dynamic maximum

Command: switchport mac-address dynamic maximum <*value*>

no switchport mac-address dynamic maximum

Function: Set the max number of dynamic MAC address allowed by the port, and, at the same time, enable the number limitation function of dynamic MAC address on the port; "**no switchport mac-address dynamic maximum**" command is used to disable the number limitation function of dynamic MAC address on the port.

Parameters: <*value*> upper limit of the number of dynamic MAC address of the port, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic MAC address on the port is disabled.

Command Mode: Port mode.

Usage Guide: When configuring the max number of dynamic MAC address allowed by the port, if the number of dynamically learnt MAC address on the port is already larger than the max number of dynamic MAC address to be set, the extra dynamic MAC addresses will be deleted. This function is mutually exclusive to functions such as dot1x, MAC binding, if the functions of dot1x, MAC binding or TRUNK are enabled on the port, this function will not be allowed.

Examples:

Enable the number limitation function of dynamic MAC address in port 1/0/2 mode, the max number to be set is 20

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)# switchport mac-address dynamic maximum 20

Disable the number limitation function of dynamic MAC address in port 1/0/2 mode

Switch(Config-If-Ethernet1/0/2)#no switchport mac-address dynamic maximum

4.13 switchport mac-address violation

Command: switchport mac-address violation {protect | shutdown} [recovery <5-3600>]

no switchport mac-address violation

Function: Set the violation mode of the port, the no command restores the violation mode to **protect**.

Parameters: protect: protect mode

shutdown: shutdown mode

recovery: Configure the border port to automatically restore after execute **shutdown** violation mode

<5-3600>: Recovery time, do not restore by default

Command Mode: Port mode

Default: protect mode

Usage Guide: The port sets the violation mode after enable the number limit function of MAC only. If the violation mode is **protect**, the port only disable the dynamic MAC address learning function when the MAC address number of the port exceeds the upper limit of secure MAC. If the violation mode is **shutdown**, the port will be disabled when the MAC address number exceeds the upper limit of secure MAC, and the user can enable the port by configuring **no shutdown** command manually or the automatic recovery

timeout.

Example: Set the violation mode as shutdown, the recovery time as 60s for port1.

Switch(config)#interface Ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#switchport mac-address violation shutdown recovery 60

4.14 switchport nd dynamic maximum

Command: switchport nd dynamic maximum <*value*>

no switchport nd dynamic maximum

Function: Set the max number of dynamic NEIGHBOR allowed by the port, and, at the same time, enable the number limitation function of dynamic NEIGHBOR on the port; "**no switchport nd dynamic maximum**" command is used to disable the number limitation function of dynamic NEIGHBOR on the port.

Parameters: <*value*> upper limit of the number of dynamic NEIGHBOR of the port, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic ARP on the port is disabled.

Command Mode: Port mode.

Usage Guide: When configuring the max number of dynamic NEIGHBOR allowed by the port, if the number of dynamically learnt NEIGHBOR on the port is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted. TRUNK ports do not supports this function.

Examples:

Enable the number limitation function of dynamic NEIGHBOR in port 1/0/2 mode, the max number to be 20.

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)# switchport nd dynamic maximum 20

Disable the number limitation function of dynamic NEIGHBOR in port 1/0/2 mode

Switch(Config-If-Ethernet1/0/2)#no switchport nd dynamic maximum

4.15 vlan mac-address dynamic maximum

Command: vlan mac-address dynamic maximum <*value*>

no vlan mac-address dynamic maximum

Function: Set the max number of dynamic MAC address allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic MAC address in the VLAN; "**no ip mac-address dynamic maximum**" command is used to disable the number limitation function of dynamic MAC address in the VLAN.

Parameters: <*value*> upper limit of the number of MAC address in the VLAN, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic MAC address in the VLAN is disabled.

Command Mode: VLAN Configuration Mode.

Usage Guide: When configuring the max number of dynamic MAC allowed in the VLAN, if the number of dynamically learnt MAC address in the VLAN is already larger than the max number to be set, the extra dynamic MAC addresses will be deleted. After enabling number limitation function of dynamic MAC in the VLAN, the number limitation of MAC is only applied to general access port, the number of MAC on TURNK ports and special ports which has enabled dot1x, MAC binding function will not be limited or counted.

Examples: Enable the number limitation function of dynamic MAC address in VLAN 1, the max number to be set is 50.

Switch(config)#vlan1

Switch(Config-if-Vlan1)#vlan mac-address dynamic maximum 50

Enable the number limitation function of dynamic MAC address in VLAN 1.

Switch(Config-if-Vlan1)#no vlan mac-address dynamic maximum

Chapter 5 Commands for AM Configuration

5.1 am enable

Command: am enable
no am enable
Function: Globally enable/disable AM function.
Parameters: None.
Default: AM function is disabled by default.
Command Mode: Global Mode.
Usage Guide: None.
Example: Enable AM function on the switch.
Switch(config)#am enable
Disable AM function on the switch.
Switch(config)#no am enable

5.2 am port

Command: am iport
no am port
Function: Enable/disable AM function on port.
Parameters: None.
Default: AM function is disabled on all port.
Command Mode: Port Mode.
Example: Enable AM function on interface 1/0/3 of the switch.
Switch(Config-If-Ethernet 1/0/3)#am port
Disable AM function on interface 1/0/3 of the switch.
Switch(Config-If-Ethernet 1/0/3)#no am port

5.3 am ip-pool

Command: am ip-pool <*ip-address*> <*num*>
no am ip-pool <*ip-address*> <*num*>
Function: Set the AM IP segment of the interface, allow/deny the IP messages or APR messages from a source IP within that segment to be forwarded via the interface.
Parameters: ***<ip-address>*** the starting address of an address segment in the IP address pool; ***<num>*** is the number of consecutive addresses following ip-address, less

than or equal with 32.
Default: IP address pool is empty.
Command Mode: Port Mode.
Usage Guide: None.
Example: Configure that interface 1/0/3 of the switch will forward data packets from an IP address which is one of 10 consecutive IP addresses starting from 10.10.10.1.
Switch(Config-If-Ethernet 1/0/3)#am ip-pool 10.10.10.1 10

5.4 am mac-ip-pool

Command: am mac-ip-pool <*mac-address*> <*ip-address*>
no am mac-ip-pool <*mac-address*> <*ip-address*>
Function: Set the AM MAC-IP address of the interface, allow/deny the IP messages or APR messages from a source IP within that segment to be forwarded via the interface.
Parameter: <*mac-address*> is the source MAC address; **<*ip-address*>** is the source IP address of the packets, which is a 32 bit binary number represented in four decimal numbers.
Default: MAC-IP address pool is empty.
Command Mode: Port Mode.
Usage Guide: None.
Example: Configure that the interface 1/0/3 of the switch will allow data packets with a source MAC address of 11-22-22-11-11-11 and a source IP address of 10.10.10.1 to be forwarded.
Switch(Config-If-Ethernet1/0/3)#am mac-ip-pool 11-22-22-11-11-11 10.10.10.1

5.5 no am all

Command: no am all [ip-pool | mac-ip-pool]
Function: Delete MAC-IP address pool or IP address pool or both pools configured by all users.
Parameters: ip-pool is the IP address pool; **mac-ip-pool** is the MAC-IP address pool; no parameter means both address pools.
Default: Both address pools are empty at the beginning.
Command Mode: Global Mode
Usage Guide: None.
Example: Delete all configured IP address pools.
Switch(config)#no am all ip-pool

5.6 show am

Command: show am [interface <*interface-name*>]

Function: Display the configured AM entries.

Parameters: ***<interface-name>*** is the name of the interface of which the configuration information will be displayed. No parameter means to display the AM configuration information of all interfaces.

Command Mode: Admin and Configuration Mode.

Example: Display all configured AM entries.

```
Switch#show am
AM is enabled

Interface Ethernet1/0/3
        am interface
        am ip-pool 30.10.10.1  20
Interface Ethernet1/0/5
   am port
   am ip-pool 50.10.10.1  30
   am mac-ip-pool  00-02-04-06-08-09 20.10.10.5
   am ip-pool 50.20.10.1  20
Interface Ethernet1/0/6
   am port
Interface Ethernet1/0/1
        am interface
        am ip-pool 10.10.10.1  20
        am ip-pool 10.20.10.1  20
```

Display the AM configuration entries of ehternet1/0/5 of the switch.

```
Switch#show am interface ethernet 1/0/5
AM is enabled

Interface Etherne1/0/5
        am interface
        am ip-pool 50.10.10.1  30
        am mac-ip-pool  00-02-04-06-08-09 20.10.10.5
   am ip-pool 50.20.10.1  20
```

Chapter 6 Commands for Security Feature

6.1 dosattack-check srcip-equal-dstip enable

Command: [no] dosattack-check srcip-equal-dstip enable
Function: Enable the function by which the switch checks if the source IP address is equal to the destination IP address; the “no” form of this command disables this function.
Parameter: None
Default: Disable the function by which the switch checks if the source IP address is equal to the destination IP address.
Command Mode: Global Mode
Usage Guide: By enabling this function, data packet whose source IP address is equal to its destination address will be dropped.
Example: Drop the data packet whose source IP address is equal to its destination address.l
Switch(config)# dosattack-check srcip-equal-dstip enable

6.2 dosattack-check ipv4-first-fragment enable

This command is not supported by switch.

6.3 dosattack-check tcp-flags enable

Command: [no] dosattack-check tcp-flags enable
Function: Enable the function by which the switch will check the unauthorized TCP label function; the “no” form of this command will disable this function.
Parameter: None
Default: This function disable on the switch by default
Command Mode: Global Mode
Usage Guide: With this function enabled, the switch will be able to drop follow four data packets containing unauthorized TCP label: SYN=1 while source port is smaller than 1024;TCP label positions are all 0 while its serial No. =0;FIN=1,URG=1,PSH=1 and the TCP serial No.=0;SYN=1 and FIN=1. This function can be used associating the “dosattack-check ipv4-first-fragment enable” command.
Example: Drop one or more types of above four packet types.
Switch(config)#dosattack-check tcp-flags enable

6.4 dosattack-check srcport-equal-dstport enable

Command: dosattack-check srcport-equal-dstport enable
no dosattack-check srcport-equal-dstport enable
Function: Enable the function by which the switch will check if the source port is equal to the destination port; the no command disables this function.
Parameter: None
Default: Disable the function by which the switch will check if the source port is equal to the destination port.
Command Mode: Global Mode
Usage Guide: With this function enabled, the switch will be able to drop TCP and UDP data packet whose destination port is equal to the source port. This function can be used associating the “dosattack-check ipv4-first-fragment enable” function so to block the IPv4 fragment TCP and UDP data packet whose destination port is equal to the source port.
Example: Drop the non-fragment TCP and UDP data packet whose destination port is equal to the source port.
Switch(config)#dosattack-check srcport-equal-dstport enable

6.5 dosattack-check tcp-fragment enable

This command is not supported by switch.

6.6 dosattack-check tcp-segment

This command is not supported by switch.

6.7 dosattack-check icmp-attacking enable

Command: [no] dosattack-check icmp-attacking enable
Function: Enable the ICMP fragment attack checking function on the switch; the “no” form of this command disables this function.
Parameter: None
Default: Disable the ICMP fragment attack checking function on the switch
Command Mode: Global Mode
Usage Guide: With this function enabled the switch will be protected from the ICMP fragment attacks, dropping the fragment ICMPv4/v6 data packets whose net length is smaller than the specified value.
Example: Enable the ICMP fragment attack checking function.
Switch(config)#dosattack-check icmp-attacking enable

6.8 dosattack-check icmpV4-size

Command: dosattack-check icmpV4-size <64-1023>

Function: Configure the max net length of the ICMPv4 data packet permitted by the switch.

Parameter: <64-1023> is the max net length of the ICMPv4 data packet permitted by the switch.

Default: The value is 0x200 by default

Command Mode: Global Mode

Usage Guide: To use this function you have to enable “dosattack-check icmp-attacking enable” first.

Example: Set the max net length of the ICMPv4 data packet permitted by the switch to 100.

Switch(config)#dosattack-check icmp-attacking enable

Switch(config)#dosattack-check icmpV4-size 100

6.9 dosattack-check icmpv6-size

This command is not supported by switch.

Chapter 7 Commands for TACACS+

7.1 tacacs-server authentication host

Command: tacacs-server authentication host <*ip-address*> [port <*port-number*>] [timeout <*seconds*>] [key {0 | 7} <*string*>] [primary]

no tacacs-server authentication host <*ip-address*>

Function: Configure the IP address, listening port number, the value of timeout timer and the key string of the TACACS+ server; the no form of this command deletes TACACS+ authentication server.

Parameter: ***<ip-address>*** is the IP address of the server; ***<port-number>*** is the listening port number of the server, the valid range is 0~65535, amongst 0 indicates it will not be an authentication server; ***<seconds>*** is the value of TACACS+ authentication timeout timer, shown in seconds and the valid range is 1~60; ***<string>*** is the key string, If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters; **primary** indicates it's a primary server.

Command Mode: Global Mode

Default: No TACACS+ authentication configured on the system by default.

Usage Guide: This command is for specifying the IP address, port number, timeout timer value and the key string of the TACACS+ server used on authenticating with the switch. The parameter port is for define an authentication port number which must be in accordance with the authentication port number of specified TACACS+ server which is 49 by default. The parameters key and timeout is used to configure the self-key and self-timeout, if the switch is not configure the timeout<*seconds*> and key<string>, it will use the global value and key by command tacacs-server timeout<*seconds*> and tacacs-server key <string>. This command can configure several TACACS+ servers communicate with the switch. The configuration sequence will be used as authentication server sequence. And in case **primary** is configured on one TACACS+ server, the server will be the primary server.

Example: Configure the TACACS+ authentication server address to 192.168.1.2, and use the global configured key.

Switch(config)#tacacs-server authentication host 192.168.1.2

7.2 tacacs-server key

Command: tacacs-server key {0 | 7} <*string*>

no tacacs-server key

Function: Configure the key of TACACS+ authentication server; the "**no tacacs-server key**" command deletes the TACACS+ server key.

Parameter: <*string*> is the key string of the TACACS+ server. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters.
Command Mode: Global Mode
Usage Guide: The key is used on encrypted packet communication between the switch and the TACACS+ server. The configured key must be in accordance with the one on the TACACS+ server or else no correct TACACS+ authentication will be performed. It is recommended to configure the authentication server key to ensure the data security.
Example: Configure test as the TACACS+ server authentication key.
Switch(config)#tacacs-server key 0 test

7.3 tacacs-server nas-ipv4

Command: tacacs-server nas-ipv4 <ip-address>
no tacacs-server nas-ipv4
Function: Configure the source IP address of TACACS+ packet sent by the switch; the "**no tacacs-server nas-ipv4**" command deletes the configuration.
Parameter: <ip-address> is the source IP address of TACACS+ packet, in dotted decimal notation, it must be a valid unicast IP address.
Default: No specific source IP address for TACACS+ packet is configured, the IP address of the interface from which the TACACS+ packets are sent is used as source IP address of TACACS+ packet.
Command Mode: Global Mode
Usage Guide: The source IP address must belongs to one of the IP interface of the switch, otherwise an failure message of binding IP address will be returned when the switch send TACACS+ packet. We suggest using the IP address of loopback interface as source IP address, it avoids that the packets from TACACS+ server are dropped when the interface link-down.
Example: Configure the source ip address of TACACS+ packet as 192.168.2.254.
Switch#tacacs-server nas-ipv4 192.168.2.254

7.4 tacacs-server timeout

Command: tacacs-server timeout <*seconds*>
no tacacs-server timeout
Function: Configure a TACACS+ server authentication timeout timer; the "**no tacacs-server timeout**" command restores the default configuration.
Parameter: <*seconds*> is the value of TACACS+ authentication timeout timer, shown in seconds and the valid range is 1~60.
Command Mode: Global Mode
Default: 3 seconds by default.
Usage Guide: The command specifies the period the switch wait for the authentication

through TACACS+ server. When connected to the TACACS+, and after sent the authentication query data packet to the TACACS+ server, the switch waits for the response. If no replay is received during specified period, the authentication is considered failed.

Example: Configure the timeout timer of the tacacs+ server to 30 seconds.

Switch(config)#tacacs-server timeout 30

7.5 debug tacacs-server

Command: debug tacacs-server

no debug tacacs-server

Function: Open the debug message of the TACACS+; the "**no debug tacacs-server**" command closes the TACACS+ debugging messages.

Command Mode: Admin Mode

Parameter: None.

Usage Guide: Enable the TACACS+ debugging messages to check the negotiation process of the TACACS+ protocol which can help detecting the failure.

Example: Enable the debugging messages of the TACACS+ protocol.

Switch#debug tacacs-server

Chapter 8 Commands for RADIUS

8.1 aaa enable

Command: aaa enable
no aaa enable
Function: Enables the AAA authentication function in the switch; the "no AAA enable" command disables the AAA authentication function.
Command mode: Global Mode.
Parameters: No.
Default: AAA authentication is not enabled by default.
Usage Guide: The AAA authentication for the switch must be enabled first to enable IEEE 802.1x authentication for the switch.
Example: Enabling AAA function for the switch.
Switch(config)#aaa enable

8.2 aaa-accounting enable

Command: aaa-accounting enable
no aaa-accounting enable
Function: Enables the AAA accounting function in the switch: the "no aaa-accounting enable" command disables the AAA accounting function.
Command mode: Global Mode
Default: AAA accounting is not enabled by default.
Usage Guide: When accounting is enabled in the switch, accounting will be performed according to the traffic or online time for port the authenticated user is using. The switch will send an “accounting started” message to the RADIUS accounting server on starting the accounting, and an accounting packet for the online user to the RADIUS accounting server every five seconds, and an “accounting stopped” message is sent to the RADIUS accounting server on accounting end. Note: The switch send the “user offline” message to the RADIUS accounting server only when accounting is enabled, the “user offline” message will not be sent to the RADIUS authentication server.
Example: Enabling AAA accounting for the switch.
Switch(config)#aaa-accounting enable

8.3 aaa-accounting update

Command: aaa-accounting update {enable | disable}
Function: Enable or disable the AAA update accounting function.

Command Mode: Global Mode.
Default: Enable the AAA update accounting function.
Usage Guide: After the update accounting function is enabled, the switch will sending accounting message to each online user on time.
Example: Disable the AAA update accounting function for switch.
Switch(config)#aaa-accounting update disable

8.4 debug aaa packet

Command: debug aaa packet {send | receive | all} interface {ethernet <*interface-number*> | <*interface-name*>}
no debug aaa packet {send | receive | all} interface {ethernet <*interface-number*> | <*interface-name*>}
Function: Enable the debug information of AAA about receiving and sending packets; the no operation of this command will disable such debug information.
Parameters: send: Enable the debug information of AAA about sending packets.
receive: Enable the debug information of AAA about receiving packets.
all: Enable the debug information of AAA about both sending and receiving packets.
<*interface-number*>: the number of interface.
<*interface-name*>: the name of interface.
Command Mode: Admin Mode.
Usage Guide: By enabling the debug information of AAA about sending and receiving packets, users can check the messages received and sent by Radius protocol, which might help diagnose the cause of faults if there is any.
Example: Enable the debug information of AAA about sending and receiving packets on interface1/0/1.
Switch#debug aaa packet all interface Ethernet 1/0/1

8.5 debug aaa detail attribute

Command: debug aaa detail attribute interface {ethernet <*interface-number*> | <*interface-name*>}
no debug aaa detail attribute interface {ethernet <*interface-number*> | <*interface-name*>}
Function: Enable the debug information of AAA about Radius attribute details; the no operation of this command will disable that debug information.
Parameters: <*interface-number*>: the number of the interface.
<*interface-name*>: the name of the interface.
Command Mode: Admin Mode.
Usage Guide: By enabling the debug information of AAA about Radius attribute details, users can check Radius attribute details of Radius messages, which might help diagnose

the cause of faults if there is any.

Example: Enable the debug information of aaa about Radius attribute details on interface 1/0/1.

Switch#debug detail attribute interface Ethernet 1/0/1

8.6 debug aaa detail connection

Command: debug aaa detail connection

no debug aaa detail connection

Function: Enable the debug information of aaa about connection details; the no operation of this command will disable that debug information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of aaa about connection details, users can check connection details of aaa, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of aaa about connection details.

Switch#debug aaa detail connection

8.7 debug aaa detail event

Command: debug aaa detail event

no debug detail event

Function: Enable the debug information of aaa about events; the no operation of this command will disable that debug information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of aaa about events, users can check the information of all kinds of event generated in the operation process of Radius protocol, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of aaa about events.

Switch#debug aaa detail event

8.8 debug aaa error

Command: debug aaa error

no debug error

Function: Enable the debug information of aaa about errors; the no operation of this command will disable that debug information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of aaa about errors, users can check the information of all kinds of errors that occurs in the operation process of Radius protocol, which might help diagnose the cause of faults if there is any.
Example: Enable the debug information of aaa about errors.
Switch#debug aaa error

8.9 radius nas-ipv4

Command: radius nas-ipv4 <*ip-address*>
no radius nas-ipv4
Function: Configure the source IP address for RADIUS packet sent by the switch. The "**no radius nas-ipv4**" command deletes the configuration.
Parameter: ***<ip-address>*** is the source IP address of the RADIUS packet, in dotted decimal notation, it must be a valid unicast IP address.
Default: No specific source IP address for RADIUS packet is configured, the IP address of the interface from which the RADIUS packets are sent is used as source IP address of RADIUS packet.
Command mode: Global Mode.
Usage guide: The source IP address must belongs to one of the IP interface of the switch, otherwise an failure message of binding IP address will be returned when the switch send RADIUS packet. We suggest using the IP address of loopback interface as source IP address, it avoids that the packets from RADIUS server are dropped when the interface link-down.
Example: Configure the source ip address of RADIUS packet as 192.168.2.254.
Switch#radius nas-ipv4 192.168.2.254

8.10 radius nas-ipv6

Command: radius nas-ipv6 <ipv6-address>
no radius nas-ipv6
Function: Configure the source IPv6 address for RADIUS packet sent by the switch. The no command deletes the configuration.
Parameter: ***<ipv6-address>*** is the source IPv6 address of the RADIUS packet, it must be a valid unicast IPv6 address.
Default: No specific source IPv6 address for RADIUS packet is configured, the IPv6 address of the interface from which the RADIUS packets are sent is used as source IPv6 address of RADIUS packet.
Command mode: Global Mode.
Usage guide: The source IPv6 address must belongs to one of the IPv6 interface of the switch, otherwise a failure message of binding IPv6 address will be returned when the switch send RADIUS packet. We suggest using the IPv6 address of loopback interface as source IPv6 address, it avoids that the packets from RADIUS server are dropped

when the interface link-down.

Example: Configure the source ipv6 address of RADIUS packet as 2001:da8:456::1.

Switch#radius nas-ipv6 2001:da8:456::1

8.11 radius-server accounting host

Command: radius-server accounting host {<*ipv4-address*> | <*ipv6-address*>} [port <*port-number*>] [key {0 | 7} <*string*>] [primary]

no radius-server accounting host {<*ipv4-address*> | <*ipv6-address*>}

Function: Specifies the IPv4/IPv6 address and the port number, whether be primary server for RADIUS accounting server; the no command deletes the RADIUS accounting server.

Parameters: ***<ipv4-address> | <ipv6-address>*** stands for the server IPv4/IPv6 address;

<port-number> for server listening port number from 0 to 65535;

<string> is the key string. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters;

primary for primary server. Multiple RADIUS sever can be configured and would be available. RADIUS server will be searched by the configured order if **primary** is not configured, otherwise, the specified RADIUS server will be used first.

Command Mode: Global Mode

Default: No RADIUS accounting server is configured by default.

Usage Guide: This command is used to specify the IPv4/IPv6 address and port number of the specified RADIUS server for switch accounting, multiple command instances can be configured. The ***<port-number>*** parameter is used to specify accounting port number, which must be the same as the specified accounting port in the RADIUS server; the default port number is 1813. If this port number is set to 0, accounting port number will be generated at random and can result in invalid configuration. This command can be used repeatedly to configure multiple RADIUS servers communicating with the switch, the switch will send accounting packets to all the configured accounting servers, and all the accounting servers can be backup servers for each other. If **primary** is specified, then the specified RADIUS server will be the primary server. It only configures a RADIUS primary server whether the server use IPv4 address or IPv6 address.

Example: Sets the RADIUS accounting server of IPv6 address to 2004:1:2:3::2, as the primary server, with the accounting port number as 3000.

Switch(config)#radius-server accounting host 2004:1:2:3::2 port 3000 primary

8.12 radius-server authentication host

Command: radius-server authentication host {*<ipv4-address> | <ipv6-address>*} [port <port-number>] [key *{0* | 7} <string>] [primary] [access-mode {dot1x | telnet}]

no radius-server authentication host {*<ipv4-address>* | *<ipv6-address>*}

Function: Specifies the IPv4 address or IPv6 address and listening port number, cipher key, whether be primary server or not and access mode for the RADIUS server; the no command deletes the RADIUS authentication server.

Parameters: ***<ipv4-address>* | *<ipv6-address>*** stands for the server IPv4/IPv6 address;

<port-number> for listening port number, from 0 to 65535, where 0 stands for non-authentication server usage;

<string> is the key string. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters;

primary for primary server. Multiple RADIUS Sever can be configured and would be available. RADIUS Server will be searched by the configured order if **primary** is not configured, otherwise, the specified RADIUS server will be used last.

[access-mode {dot1x|telnet}] designates the current RADIUS server only use 802.1x authentication or telnet authentication, all services can use current RADIUS server by default.

Command mode: Global Mode

Default: No RADIUS authentication server is configured by default.

Usage Guide: This command is used to specify the IPv4 address or IPv6 address and port number, cipher key string and access mode of the specified RADIUS server for switch authentication, multiple command instances can be configured. The port parameter is used to specify authentication port number, which must be the same as the specified authentication port in the RADIUS server, the default port number is 1812. If this port number is set to 0, the specified server is regard as non-authenticating. This command can be used repeatedly to configure multiple RADIUS servers communicating with the switch, the configured order is used as the priority for the switch authentication server. When the first server has responded (whether the authentication is successed or failed), switch does not send the authentication request to the next. If **primary** is specified, then the specified RADIUS server will be the primary server. It will use the cipher key which be configured by **radius-server key <string>** global command if the current RADIUS server not configure key<string>. Besides, it can designate the current RADIUS server only use 802.1x authentication or telnet authentication via access-mode option. It is not configure access-mode option and all services can use current RADIUS server by default.

Example: Setting the RADIUS authentication server address as 2004:1:2:3::2.

Switch(config)#radius-server authentication host 2004:1:2:3::2

8.13 radius-server dead-time

Command: radius-server dead-time <*minutes*>

no radius-server dead-time

Function: Configures the restore time when RADIUS server is down; the "**no radius-server dead-time**" command restores the default setting.
Parameters: ***<minute>*** is the down -restore time for RADIUS server in minutes, the valid range is 1 to 255.
Command mode: Global Mode
Default: The default value is 5 minutes.
Usage Guide: This command specifies the time to wait for the RADIUS server to recover from inaccessible to accessible. When the switch acknowledges a server to be inaccessible, it marks that server as having invalid status, after the interval specified by this command; the system resets the status for that server to valid.
Example: Setting the down-restore time for RADIUS server to 3 minutes.
Switch(config)#radius-server dead-time 3

8.14 radius-server key

Command: radius-server key {0 | 7} <*string*>
no radius-server key
Function: Specifies the key for the RADIUS server (authentication and accounting); the "no radius-server key" command deletes the key for RADIUS server.
Parameters: ***<string>*** is a key string for RADIUS server, If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters.
Command mode: Global Mode
Usage Guide: The key is used in the encrypted communication between the switch and the specified RADIUS server. The key set must be the same as the RADIUS server set, otherwise, proper RADIUS authentication and accounting will not perform properly.
Example: Setting the RADIUS authentication key to be "test".
Switch(config)#radius-server key 0 test

8.15 radius-server retransmit

Command: radius-server retransmit <*retries*>
no radius-server retransmit
Function: Configures the re-transmission times for RADIUS authentication packets; the "**no radius-server retransmit**" command restores the default setting.
Parameters: ***<retries>*** is a retransmission times for RADIUS server, the valid range is 0 to 100.
Command mode: Global Mode
Default: The default value is 3 times.
Usage Guide: This command specifies the retransmission time for a packet without a RADIUS server response after the switch sends the packet to the RADIUS server. If authentication information is missing from the authentication server, AAA authentication

request will need to be re-transmitted to the authentication server. If AAA request retransmission count reaches the retransmission time threshold without the server responding, the server will be considered to as not work, the switch sets the server as invalid.

Example: Setting the RADIUS authentication packet retransmission time to five times.

Switch(config)#radius-server retransmit 5

8.16 radius-server timeout

Command: radius-server timeout <*seconds*>

no radius-server timeout

Function: Configures the timeout timer for RADIUS server; the "**no radius-server timeout**" command restores the default setting.

Parameters: <*seconds*> is the timer value (second) for RADIUS server timeout, the valid range is 1 to 1000.

Command mode: Global Mode

Default: The default value is 3 seconds.

Usage Guide: This command specifies the interval for the switch to wait RADIUS server response. The switch waits for corresponding response packets after sending RADIUS Server request packets. If RADIUS server response is not received in the specified waiting time, the switch resends the request packet or sets the server as invalid according to the current conditions.

Example: Setting the RADIUS authentication timeout timer value to 30 seconds.

Switch(config)#radius-server timeout 30

8.17 radius-server accounting-interim-update timeout

Command: radius-server accounting-interim-update timeout <*seconds*>

no radius-server accounting-interim-update timeout

Function: Set the interval of sending fee-counting update messages; the no operation of this command will reset to the default configuration.

Parameters: <*seconds*> is the interval of sending fee-counting update messages, in seconds, ranging from 60 to 3600.

Command Mode: Global Mode.

Default: The default interval of sending fee-counting update messages is 300 seconds.

User Guide: This command set the interval at which NAS sends fee-counting update messages. In order to realize the real time fee-counting of users, from the moment the user becomes online, NAS will send a fee-counting update message of this user to the RADIUS server at the configured interval.

The interval of sending fee-counting update messages is relative to the maximum number of users supported by NAS. The smaller the interval, the less the maximum number of the users supported by NAS; the bigger the interval, the more the maximum

number of the users supported by NAS. The following is the recommended ratio of interval of sending fee-counting update messages to the maximum number of the users supported by NAS:

Table 8-1 The recommended ratio of the interval of sending fee-counting update messages to the maximum number of the users supported by NAS

The maximum number of users	The interval of sending fee-counting update messages(in seconds)
1~299	300（default value）
300~599	600
600~1199	1200
1200~1799	1800
≥1800	3600

Example: The maximum number of users supported by NAS is 700, the interval of sending fee-counting update messages 1200 seconds.

Switch(config)#radius-server accounting-interim-update timeout 1200

8.18 show aaa authenticated-user

Command: show aaa authenticated-user

Function: Displays the authenticated users online.

Command mode: Admin and Configuration Mode.

Usage Guide: Usually the administrator concerns only information about the online user, the other information displayed is used for troubleshooting by technical support.

Example:

Switch#show aaa authenticated-user

---------- authenticated users ----------

UserName Retry RadID Port EapID ChapID OnTime UserIP MAC

---------- total: 0 ----------

8.19 show aaa authenticating-user

Command: show aaa authenticating-user

Function: Display the authenticating users.

Command mode: Admin and Configuration Mode.

Usage Guide: Usually the administrator concerns only information about the authenticating user, the other information displays is used for troubleshooting by the technical support.

Example:

Switch#show aaa authenticating-user

---------- authenticating users ----------
User-name Retry-time Radius-ID Port Eap-ID Chap-ID Mem-Addr State
---

---------- total: 0 ----------

8.20 show aaa config

Command: show aaa config
Function: Displays the configured commands for the switch as a RADIUS client.
Command mode: Admin and Configuration Mode.
Usage Guide: Displays whether aaa authentication, accounting are enabled and information for key, authentication and accounting server specified.
Example:
Switch#show aaa config（For Boolean value, 1 stands for TRUE and 0 for FALSE）

---------- AAA config data ----------

Is Aaa Enabled = 1 :1 means AAA authentication is enabled, 0 means is not enabled
Is Account Enabled= 1 :1 means AAA account is enabled, 0 means is not enabled
MD5 Server Key = yangshifeng : Authentication key
authentication server sum = 2 :Configure the number of authentication server
authentication server[0].sock_addr = 2:100.100.100.60.1812 :The address protocol group, IP and interface number of the first authentication server
.Is Primary = 1 :Is the primary server
.Is Server Dead = 0 :The server whether dead
.Socket No = 0 :The local socket number lead to this server
authentication server[1].sock_addr = 10:2004:1:2::2.1812
.Is Primary = 0
.Is Server Dead = 0
.Socket No = 0
accounting server sum = 2 :Configure the number of the accounting server
accounting server[0].sock_addr = 2:100.100.100.65.1813 :The address protocol group, IP and interface number of the accounting server
.Is Primary = 1 :Is primary server
.Is Server Dead = 0 :This server whether dead
.Socket No = 0 :The local socket number lead to this server
accounting server[1].sock_addr = 10:2004::7.1813
.Is Primary = 1
.Is Server Dead = 0
.Socket No = 0

Time Out = 5s :After send the require packets, wait for response time out
Retransmit = 3 :The number of retransmit
Dead Time = 5min :The tautology interval of the dead server
Account Time Interval = 0min :The account time interval

8.21 show radius authenticated-user count

Command: show radius authenticated-user count
Function: Show the number of on-line users who have already passed the authentication.
Parameter: None.
Command mode: Admin and configuration mode
Default: None.
Usage guide: None.
Example:
Switch#show radius authenticated-user count
The authenticated online user num is: 105

8.22 show radius authenticating-user count

Command: show radius authenticating-user count
Function: Show the number of the authenticating-user.
Parameter: None.
Command mode: Admin and configuration mode.
Default: None.
Usage Guide: None.
Example:
Switch#show radius authenticating-user count
The authenticating user num is: 10

8.23 show radius count

Command: show radius {authenticated-user|authenticating-user} count
Function: Displays the statistics for users of RADIUS authentication.
Parameters: **authenticated-user** displays the authenticated users online; **authenticating-user** displays the authenticating users.
Command mode: Admin and Configuration Mode.
Usage Guide: The statistics for RADIUS authentication users can be displayed with the "**show radius count**" command.
Example:
1. Display the statistics for RADIUS authenticated users.

Switch#show radius authenticated-user count
The authenticated online user num is: 0
2. Display the statistics for RADIUS authenticated users and others.
Switch#show radius authenticating-user count

Chapter 9 Commands for SSL Configuration

9.1 ip http secure-server

Command: ip http secure-server
no ip http secure-server
Function: Enable/disable SSL function.
Parameter: None.
Command Mode: Global Mode.
Default: Disabled.
Usage Guide: This command is used for enable and disable SSL function. After enable SSL function, the users visit the switch through https client, switch and client use SSL connect, can form safety SSL connect channel. After that, all the data which transmit of the application layer will be encrypted, then ensure the privacy of the communication.
Example: Enable SSL function.
Switch(config)#ip http secure-server

9.2 ip http secure-port

Command: ip http secure-port *<port-number>*
no ip http secure-port
Function: Configure/delete port number by SSL used.
Parameter: ***<port-number>*** means configured port number, range between 1025 and 65535. 443 is for default.
Command Mode: Global Mode.
Default: Not configure.
Usage Guide: If this command is used to configure the port number, then the configured port number is used to monitor. If the port number for https is changed, when users try to use https to connect, must use the changed one. For example: https://device:port_number. SSL function must reboot after every change.
Example: Configure the port number is 1028.
Switch(config)#ip http secure-port 1028

9.3 ip http secure- ciphersuite

Command: ip http secure-ciphersuite {des-cbc3-sha|rc4-128-sha| des-cbc-sha}
no ip http secure-ciphersuite

Function: Configure/delete secure cipher suite by SSL used.
Parameter: **des-cbc3-sha** encrypted algorithm DES_CBC3, summary algorithm SHA.
rc4-128-sha encrypted algorithm RC4_128, summary algorithm SHA.
des-cbc-sha encrypted algorithm DES_CBC, summary algorithm SHA.
default use is **rc4-md5**.
Command Mode: Global Mode.
Default: Not configure.
Usage Guide: If this command is used to configure the secure cipher suite, specified encryption method will be used. The SSL should be restarted to take effect after changes on configuration. When des-cbc-sha is configured, IE 7.0 or above is required.
Example: Configure the secure cipher suite is rc4-128-sha.
Switch(config)# ip http secure- ciphersuite rc4-128-sha

9.4 show ip http secure-server status

Command: show ip http secure-server status
Function: Show the status for the configured SSL.
Parameter: None.
Command Mode: Admin and Configuration Mode.
Example:
Switch# show ip http secure-server status
HTTP secure server status: Enabled
HTTP secure server port: 1028
HTTP secure server ciphersuite: rc4-128-sha

9.5 debug ssl

Command: debug ssl
no debug ssl
Function: Show the configured SSL information, the no command closes the DEBUG.
Parameter: None.
Command Mode: Admin Mode.
Example:
Switch# debug ssl
%Jan 01 01:02:05 2006 ssl will to connect to web server 127.0.0.1:9998
%Jan 01 01:02:05 2006 connect to http security server success!

Chapter 10 Commands for IPv6 Security RA

10.1 ipv6 security-ra enable

Command: ipv6 security-ra enable
no ipv6 security-ra enable
Function: Globally enable IPv6 security RA function, all the RA advertisement messages will not be forwarded through hardware, but only sent to CPU to handle. The no operation of this command will globally disable IPv6 security RA function.
Parameters: None.
Command Mode: Global Configuration Mode.
Default: The IPv6 security RA function is disabled by default.
Usage Guide: Only after enabling the global security RA function, the security RA on a port can be enabled. Globally disabling security RA will clear all the configured security RA ports. The global security RA function and the global IPv6 SAVI function are mutually exclusive, so they can not be enabled at the same time.
Example: Globally enable IPv6 security RA.
Switch(config)#ipv6 security-ra enable

10.2 ipv6 security-ra enable

Command: ipv6 security-ra enable
no ipv6 security-ra enable
Function: Enable IPv6 security RA on a port, causing this port not to forward the received RA message. The **no ipv6 security-ra enable** will disable the IPv6 security RA on a port.
Parameters: None.
Command Mode: Port Configuration Mode.
Default: IPv6 security RA function is disabled by default.
Usage Guide: Only after globally enabling the security RA function, can the security RA on a port be enabled. Globally disabling security RA will clear all the configured security RA ports.
Example: Enable IPv6 security RA on a port.
Switch(Config-If-Ethernet1/0/2)#ipv6 security-ra enable

10.3 show ipv6 security-ra

Command: show ipv6 security-ra [interface <*interface-list*>]
Function: Display all the interfaces with IPv6 RA function enabled.
Parameters: No parameter will display all distrust ports, entering a parameter will display the corresponding distrust port.
Command Mode: Admin and Configuration Mode.
Example:
Switch# show ipv6 security-ra
IPv6 security ra config and state information in the switch
Global IPv6 Security RA State: Enable
Ethernet1/0/1
IPv6 Security RA State: Yes
Ethernet1/0/3
IPv6 Security RA State: Yes

10.4 debug ipv6 security-ra

Command: debug ipv6 security-ra
no debug ipv6 security-ra
Function: Enable the debug information of IPv6 security RA; the no operation of this command will disable the debug information of IPv6 security RA.
Command Mode: Admin Mode.
Parameters: None.
Usage Guide: Users can check the proceeds of message handling of IPv6 security RA, which will help investigate the causes to problems if there is any.
Example: Enable the debug information of IPv6 security RA.
Switch#debug ipv security-ra

Chapter 11 Commands for MAB

11.1 authentication mab

Command: authentication mab {radius|local} (none|)
no authentication mab

Function: Configure the authentication mode and priority of MAC address authentication, the no command restores the default authentication mode.

Parameters: radius means RADIUS authentication mode; local means the local authentication; none means the authentication is needless.

Default: Using RADIUS authentication mode.

Command Mode: Global mode

Usage Guide: none option is used to the fleeing function of MAC address authentication. If all configured RADIUS servers don't respond, switch will adopt none authentication mode to allow that MAC address authentication users access the network directly. The option of local is used for the local authentication of MAC address, it authenticates through the local user name and password. If configured as the method of **authentication mab radius local none**, judge if configured the user name and password used in mab authentication in local when the radius server has no response. If it has been configured, use the local authentication, if not, use the backup none authentication.

Example: Configure the local authentication and the fleeing function of MAC address authentication.

Switch(config)#authentication mab radius local none

11.2 clear mac-authentication-bypass binding

Command: clear mac-authentication-bypass binding {mac WORD | interface (ethernet IFNAME | IFNAME) | all}

Function: Clear MAB binding information.

Parameters: MAC: Delete MAB binding of the specified MAC address
IFNAME: Delete MAB binding of the specified port
all: Delete all MAB binding

Command Mode: Admin Mode

Default: None.

Usage Guide: None.

Example: Delete all MAB binding.

Switch#clear mac-authentication-bypass binding all

11.3 debug mac-authentication-bypass

Command: debug mac-authentication-bypass {packet | event | binding}
Function: Enable the debugging of the packet information, event information or binding information for MAB authentication.
Parameters: packet: Enable the debugging of the packet information for MAB authentication.
event: Enable the debugging of the event information for MAB authentication.
binding: Enable the debugging of the binding information for MAB authentication.
Command Mode: Admin Mode
Default: None.
Usage Guide: None.
Example: Enable the debugging of the packet information for MAB authentication.
Switch#debug mac-authentication-bypass packet

11.4 mac-authentication-bypass binding-limit

Command: mac-authentication-bypass binding-limit *<1-100>*
no mac-authentication-bypass binding-limit
Function: Set the max binding number of MAB. The no command will restore the default binding number as 3.
Parameters: *<1-100>* the max binding number of MAB, ranging from 1 to 100.
Command Mode: Port Mode
Default: The max binding number of MAB is 3.
Usage Guide: Set the max binding number of MAB. When the binding number reaches to the max value, the port will stop binding, if the max binding number is less than the current binding number of the port, the setting will be unsuccessful.
Example: Configure the max binding number as 10.
Switch(Config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#mac-authentication-bypass binding-limit 10

11.5 mac-authentication-bypass enable

Command: mac-authentication-bypass enable
no mac-authentication-bypass enable
Function: Enable the global and port MAB function. The no command disables MAB function.
Parameters: None.
Command Mode: Global Mode and Port Mode

Default: Disable the global and port MAB function.
Usage Guide: To process MAB authentication of a port, enable the global MAB function first, and then, enable the MAB function of the corresponding port.
Example: Enable the global and port Eth1/0/1 MAB function.
Switch(Config)#mac-authentication-bypass enable
Switch(Config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#mac-authentication-bypass enable

11.6 mac-authentication-bypass guest-vlan

Command: mac-authentication-bypass guest-vlan <*1-4094*>
no mac-authentication-bypass guest-vlan
Function: Set guest vlan of MAB authentication. The no command deletes guest vlan.
Parameters: <*1-4094*>: guest vlan ID, ranging from 1 to 4094.
Command Mode: Port Mode
Default: None.
Usage Guide: Set guest vlan of MAB authentication, only Hybrid port use this command, it is not take effect on access port. After MAB authentication is failing, if the existent guest vlan is configured by the port connecting to the MAB user, the MAB user can join and access guest vlan.
Example: Configure guest vlan of MAB authentication for port 1/0/1
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#mac-authentication-bypass guest-vlan 10

11.7 mac-authentication-bypass spoofing-garp-check

Command: mac-authentication-bypass spoofing-garp-check enable
no mac-authentication-bypass spoofing-garp-check enable
Function: Enable the spoofing-garp-check function, MAB function will not deal with spoofing-garp any more; the no command disables the function.
Parameters: None.
Command Mode: Global Mode
Default: Disable spoofing-garp-check function.
Usage Guide: When the terminal of Windows operating system detects the address conflict, it will sends a gratuitous ARP to correct the error ARP entries generated by gratuitous ARP of the conflict detection. This command is used to detect the spoofing-garp when occuring the address conflict, MAB function is not deal with the packet any more. Notice: when enabling the check function, all ARP will be processed the software check, it will add switch's load.
Example: Enable spoofing-garp-check function.
Switch(Config)#mac-authentication-bypass spoofing-garp-check enable

11.8 mac-authentication-bypass timeout linkup-period

Command: mac-authentication-bypass timeout linkup-period <*0-30*>
no mac-authentication-bypass timeout linkup-period
Function: Set the interval between down and up when VLAN binding in a port is changing to assure the user can obtain IP again.
Parameters: <*0-30*>: After the port is shutdown automatically, the interval before it up again, the unit is second, 0 means there is no down/up operation.
Command Mode: Global Mode
Default: The interval is 0.
Usage Guide: When MAB authentication is successful, belong to vlan according to auto-vlan setting, when MAB authentication is failing, belong to vlan according to guest-vlan setting. After linkup-period is set, when VLAN binding of a port is changing, the port will be shutdown automatically, and will be up again after linkup-period to assure the client obtain IP.
Example: Configure down/up time as 12s.
Switch(Config)#mac-authentication-bypass timeout linkup-period 12

11.9 mac-authentication-bypass timeout offline-detect

Command: mac-authentication-bypass timeout offline-detect (0 | <60-7200>)
no mac-authentication-bypass timeout offline-detect
Function: Configure offline-detect time. The no command restores the default value.
Parameters: (0 | <60-7200>): offline-detect time, the range is 0 or 60 to 7200s.
Command Mode: Global Mode
Default: offline-detect time is 180s.
Usage Guide: When offline-detect time is 0, the switch does not detect MAB binding, when offline-detect time is 60s to 7200s, the switch timely detects the flow corresponding to the MAB binding. If there is no flow in the period of offline-detect time, it will delete this binding and forbid the flow to pass.
Example: Configure offline-detect time as 200s.
Switch(Config)#mac-authentication-bypass timeout offline-detect 200

11.10 mac-authentication-bypass timeout quiet-period

Command: mac-authentication-bypass timeout quiet-period <1-60>
no mac-authentication-bypass timeout quiet-period
Function: Set quiet-period of MAB authentication. The no command restores quiet-period as the default value.
Parameters: <*1-60*>: quiet-period, ranging from 1 to 60s.
Command Mode: Global Mode

Default: quiet-period is 30s.
Usage Guide: If MAB authentication is failing, within the quiet-period the switch will not respond the authentication request of this MAC, after quiet-period, it will respond the request again.
Example: Configure quiet-period of MAB authentication as 60s.
Switch(Config)#mac-authentication-bypass timeout quiet-period 60

11.11 mac-authentication-bypass timeout reauth-period

Command: mac-authentication-bypass timeout reauth-period *<1-3600>*
no mac-authentication-bypass timeout reauth-period
Function: Set the reauthentication interval at failing authentication state. The no command restores the default value.
Parameters: *<1-3600>*: reauthentication interval, ranging from 1 to 3600s.
Command Mode: Global Mode
Default: reauthentication interval is 30s.
Usage Guide: At failing authentication state, the user processes the reauthentication timely until the authentication is successful; at the successful state, the user can access the network resources.
Example: Configure reauthentication time as 20s.
Switch(Config)#mac-authentication-bypass timeout reauth-period 20

11.12 mac-authentication-bypass timeout stale-period

Command: mac-authentication-bypass timeout stale-period <0-60>
no mac-authentication-bypass timeout stale-period
Function: Set the time that delete the binding user after MAB port is down. The no command restores the default value.
Parameters: *<1-60>*: The time that delete the binding, ranging from 0 to 60s.
Command Mode: Global Mode
Default: 30s.
Usage Guide: If the time that delete the binding as 0, delete all user binding of this port as soon as the MAB port is down, if the time is bigger than 0, delete the user binding with a delay after the MAB port is down.
Example: Configure the deletion time as 40s.
Switch(Config)#mac-authentication-bypass timeout stale-period 40

11.13 mac-authentication-bypass username-format

Command: mac-authentication-bypass username-format {mac-address | {fixed username WORD password WORD}}
Function: Set the authenticate method of MAB authentication.
Parameters: mac-address: Use MAC address of MAB user as username and password to authenticate.
fixed username WORD password WORD: Use the specified username and password to authenticate, the length of username and password ranges between 1 and 32 characters.
Command Mode: Global Mode
Default: Use MAC address of MAB user as username and password to authenticate.
Usage Guide: There are two methods for MAB authentication: use MAC address of MAB user as username and password to authenticate or use the specified username and password to authenticate. If there is no specified username and password, the device uses the first method to authenticate by default.
Example: All MAB users use the same username and password to authenticate, the username is mab-user, the password is mab-pwd.
Switch(Config)#mac-authentication-bypass username-format fixed username mab-user password mab-pwd

11.14 show mac-authentication-bypass

Command: show mac-authentication-bypass {interface {ethernet IFNAME | IFNAME) |}
Function: Show the binding information of MAB authentication.
Parameters: interface {ethernet IFNAME|IFNAME}: The port name.
Command Mode: Admin Mode
Default: None.
Usage Guide: None.
Example: Show the binding information of all MAB users.
Switch#show mac-authentication-bypass

The Number of all binding is 5

MAC	Interface	Vlan ID	State
05-0a-eb-6a-7f-88	Ethernet1/0/1	1	MAB_QUIET
04-0a-eb-6a-7f-88	Ethernet1/0/1	1	MAB_QUIET
03-0a-eb-6a-7f-88	Ethernet1/0/1	1	MAB_QUIET
02-0a-eb-6a-7f-88	Ethernet1/0/1	1	MAB_AUTHENTICATED

00-0a-eb-6a-7f-8e Ethernet1/0/1 1 MAB_AUTHENTICATED

Displayed information	Explanation
The Number of all binding	The binding number of all MAB users, include the successful authentication user and the failing authentication user at quiet-period state
MAC	MAC address
Interface	The binding port
Vlan	The VLAN that MAB user belongs
State	Authentication state

Switch(config)#show mac-authentication-bypass int e1/0/1

Interface Ethernet1/0/1 user config:

MAB enable: Enable

Binding info: 1

MAB Binding built at SUN JAN 01 01:14:48 2006

VID 1, Port: Ethernet1/1

Client MAC: 00-0a-eb-6a-7f-8e

Binding State: MAB_AUTHENTICATED

Binding State Lease: 164 seconds left

Displayed information	Explanation
MAB enable	MAB function enabled or not
Binding info	The MAB binding number of the specified port
MAB Binding built at	The time when the user binding was created
VID	The VLAN that MAB user belongs
Port	The binding port
Client MAC	MAC address
Binding State	Authentication state
Binding State Lease	Remain time before the binding release

Chapter 12 Commands for PPPoE Intermediate Agent

12.1 debug pppoe intermediate agent packet {receive | send} interface ethernet <interface-name>

Command: debug pppoe intermediate agent packet (receive | send|) interface ethernet <interface-name>

no debug pppoe intermediate agent packet (receive | send|) interface ethernet <interface-name>

Function: Enable PPPoE packet debug for the specified port, the no command disables it.

Parameter: receive: Enable the debug that receive PPPoE packet.

send: Enable the debug that send PPPoE packet.

ehernet: Physical port

interface-name: Port name

Command Mode: Admin mode

Default: Disable PPPoE packet debug for the specified port.

Usage Guide: Enable PPPoE packet debug for the specified port to show PPPoE packet received and sent by this port.

Example: Enable PPPoE intermediate debug for port ethernet1/0/2.

Switch#debug pppoe intermediate agent packet send interface ethernet 1/0/2

12.2 pppoe intermediate-agent

Command: pppoe intermediate-agent

no pppoe intermediate-agent

Function: Enable global PPPoE intermediate agent function. The no command disables global PPPoE intermediate agent function.

Parameter: None.

Command Mode: Global mode.

Default: Disable global PPPoE intermediate agent function.

Usage Guide: After enable global PPPoE IA function, process the packet of PPPoE discovery stage according to the related configuration.

Example: Enable global PPPoE intermediate agent function.

Switch(config)#pppoe intermediate agent

12.3 pppoe intermediate-agent (Port)

Command: pppoe intermediate-agent
no pppoe intermediate-agent
Function: Enable PPPoE intermediate agent function of the port. The no command disables PPPoE intermediate agent function of the port.
Parameter: None.
Command Mode: Port mode
Default: Disable PPPoE intermediate agent function of the port.
Usage Guide: After enable PPPoE IA function of the port, add vendor tag for PPPoE packet of the port.
Note: 1. It must enable global pppoe intermediate-agent function.
2. At least one port is connected to PPPoE server, and the port mode is trust.
Example: Enable PPPoE intermediate agent function of the port ethernet 1/0/2.
Switch(config-if-ethernet1/0/2)#pppoe intermediate agent

12.4 pppoe intermediate-agent circuit-id

Command: pppoe intermediate-agent circuit-id <string>
no pppoe intermediate-agent circuit-id <string>
Function: Configure circuit ID of the port, the no command cancels this configuration.
Parameter: <string>: circuit-id, the max character number is 63 bytes.
Command Mode: Port mode
Default: This configuration is null.
Usage Guide: This command configures circuit-id alone for each port, the priority is higher than pppoe intermediate-agent identifier-string command.
Example: Configure circuit-id as abcd/efgh on port ethernet1/0/3 of vlan3.
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent circuit-id abcd/efgh
After port ethernet1/0/3 of vlan3 receives PPPoE packet, circuit-id value of the added vendor tag as ”abcd/efgh”.

12.5 pppoe intermediate-agent delimiter

Command: pppoe intermediate-agent delimiter <WORD>
no pppoe intermediate-agent delimiter
Function: Configure the delimiter among the fields in circuit-id and remote-id, the no command cancels the configuration.
Parameter: <WORD>: the delimiter, its range is (#|.|,|;|:|/|space).
Command Mode: Global mode

Default: The fields is comparted with '\0'.

Usage Guide: After configuring the delimiter, the added fields of circuit-id and remote-id use the configured delimiter to compart. Notice: The global **pppoe intermediate-agent** function must be enabled.

Example: Configure the delimiter.

Switch(config)#pppoe intermediate-agent delimiter space

12.6 pppoe intermediate-agent format

Command: pppoe intermediate-agent format (circuit-id | remote-id) (hex | ascii)
no pppoe intermediate-agent format (circuit-id | remote-id)

Function: Configure the format with hex or ASCII for circuit-id and remote-id, the no command cancels the configuration.

Parameter: hex: hexadecimal
ascii: ASCII code

Command Mode: Global mode

Default: This configuration is null.

Usage Guide: Encapsulation circuit-id and remote-id with hex ASCII format to vendor tag. Notice: The global **pppoe intermediate-agent** function must be enabled.

Example: Configure the trust port 1/0/1 to enable vendor-tag strip function.

Switch(config)#pppoe intermediate-agent format remote-id ascii

12.7 pppoe intermediate-agent remote-id

Command: pppoe intermediate-agent remote-id <string>
no pppoe intermediate-agent remote-id <string>

Function: Configure remote-id of the port, the no command cancels this configuration.

Parameter: <string>: remote-id, the max character number is 63 bytes.

Command Mode: Port mode

Default: This configuration is null.

Usage Guide: Configure remote-id for each port, if there is no configuration, use switch's MAC as remote-id value.

Example: Configure remote-id as abcd on port ethernet1/0/2.

Switch(config-if-ethernet1/0/2)# pppoe intermediate-agent remote-id abcd

12.8 pppoe intermediate-agent trust

Command: pppoe intermediate-agent trust
no pppoe intermediate-agent trust

Function: Configure the port as trust port, the no command configures the port as untrust port.

Parameter: None.
Command Mode: Port mode
Default: Untrust port.
Usage Guide: The port which connect to server must be configured as trust port. Note: At least one trust port is connected to PPPoE server.
Example: Configure port ethernet1/0/1 as trust port.
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust

12.9 pppoe intermediate-agent type self-defined circuit-id

Command: pppoe intermediate-agent type self-defined circuit-id {vlan | port | id (switch-id (mac | hostname) | remote-mac) | string WORD}
no pppoe intermediate-agent type self-defined circuit-id
Function: Configure the self-defined circuit-id, the no command cancels the configuration.
Parameter: vlan: VLAN ID
port: Port ID
id switch-id mac: the local MAC address
id switch-id hostname: the local host name
id remote-mac: the remote MAC address
string WORD: the specified keyword
Command Mode: Global mode
Default: This configuration is null.
Usage Guide: This configuration and type tr-101 circuit-id are mutually exclusive, it will clear the corresponding configuration of type tr-101 circuit-id.
Example: Configure the self-defined circuit-id as vlan port id switch-id hostname.
Switch(config)#pppoe intermediate-agent type self-defined circuit-id vlan port id switch-id hostname

12.10 pppoe intermediate-agent type self-defined remoteid

Command: pppoe intermediate-agent type self-defined remoteid {mac | vlan-mac | hostname | string WORD}
no pppoe intermediate-agent type self-defined remote-id
Function: Configure the self-defined remote-id, the no command cancels the configuration.
Parameter: mac: Ethernet port MAC address
vlan-mac: IP interface MAC address

hostname: the local host name

string WORD: the specified keyword

Command Mode: Global mode

Default: This configuration is null.

Usage Guide: Configuration order of this command according to the fields order in remote-id.

Example: Configure the self-defined remote-id as string abcd mac hostname.

Switch(config)#pppoe intermediate-agent type self-defined remote-id string abcd mac hostname

12.11 pppoe intermediate-agent type tr-101 circuit-id access-node-id

Command: pppoe intermediate-agent type tr-101 circuit-id access-node-id <string>

no pppoe intermediate-agent type tr-101 circuit-id access-node-id

Function: Configure access-node-id field value of circuit ID in the added vendor tag with tr-101 standard.

Parameter: <string>: access-node-id, the max character number is 47 bytes.

Command Mode: Global mode

Default: MAC address of the switch

Usage Guide: Use this configuration to create access-node-id of circuit ID in vendor tag. circuit-id value is access-node-id +" eth "+ Slot ID + delimiter + Port Index + delimiter + Vlan ID, access-node-id occupies n bytes (n<48), " eth " is space + e + t + h + space, it occupies 5 bytes, Slot ID occupies 2 bytes, Port Index occupies 3 bytes, Vlan ID occupies 4 bytes, delimiter occupies 1 byte. In default state, access-node-id value of circuit-id is switch's MAC, it occupies 6 bytes. For example: MAC address is "0a0b0c0d0e0f", Slot ID is 12, Port Index is 34, Vlan ID is 567, the default circuit-id value is "0a0b0c0d0e0f eth 12/034:0567".

Example: Configure access-node-id value of circuit ID as abcd in vendor tag.

Switch(config)#pppoe intermediate-agent access-node-id abcd

After port ethernet1/0/3 of vlan3 receives PPPoE packets, circuit-id value of the added vendor tag is "abcd eth 01/003:0003".

12.12 pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter

Command: pppoe intermediate-agent type tr-101 circuit-id identifier-string <string> option {sp | sv | pv | spv} delimiter <WORD> [delimiter <WORD>]

no pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter

Function: Configure circuit-id of the added vendor tag with tr-101 standard, the no command deletes this configuration.

Parameter: <string>: identifier-string, the max character number is 47 bytes.

{sp | sv | pv | spv}: This option can select the combination format for slot, port, vlan, sp means slot and port, sv means slot and vlan, pv means port and vlan, spv means slot, port and vlan.

<WORD>: The delimiter between slot, port and vlan, the range is (# | . | , | ; | : | / | space). Note: There are two delimiter WORDs in spv combo mode, the first between slot and port, the second between port and vlan.

Command Mode: Global mode

Default: This configuration is null.

Usage Guide: This command is used to configure global circuit id, the priority is higher than pppoe intermediate-agent access-node-id command. circuit-id value is access-node-id +" eth "+ Slot ID + delimiter + Port Index + delimiter + Vlan ID, access-node-id occupies n bytes (n<48), " eth " is space + e + t + h + space, it occupies 5 bytes, Slot ID occupies 2 bytes, Port Index occupies 3 bytes, Vlan ID occupies 4 bytes, delimiter occupies 1 byte.

Example: Configure access-node-id as xyz, use spv combination mode, delimiter with "#"between Slot ID and Port ID, delimiter with "/"between Port ID and Vlan ID.

Switch(config)#pppoe intermediate-agent identifier-string xyz option spv delimiter # delimiter /

Switch# show pppoe intermediate-agent identifier-string option delimiter

config identifier string is : xyz

config option is : slot , port and vlan

the first delimiter is : "# "

the second delimiter is : "/ "

After port ethernet1/0/3 of vlan3 receives PPPoE packets, circuit-id value of the added vendor tag is "xyz eth 01#003/0003".

12.13 pppoe intermediate-agent vendor-tag strip

Command: pppoe intermediate-agent vendor-tag strip

no pppoe intermediate-agent vendor-tag strip

Function: Enable vendor-tag strip function of the port, the no command cancels this function.

Parameter: None.

Command Mode: Port mode

Default: Disable vendor-tag strip function of the port.

Usage Guide: If the received packet includes vendor tag from server to client, strip this vendor tag.

Note: 1. Must enable global pppoe intermediate-agent function.

2. It must be configured on trust port.

Example: Trust port ethernet1/0/1 enables vendor tag strip function.

Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent vendor-tag strip

12.14 show pppoe intermediate-agent access-node-id

Command: show pppoe intermediate-agent access-node-id
Function: Show the configured access node ID.
Parameter: None.
Command Mode: Admin mode
Default: The configuration information is null.
Usage Guide: This command is used to show access-node-id configured by user.
Example: Show access-node-id configuration information.
Switch#pppoe intermediate-agent access-node-id abcd
Switch#show pppoe intermediate-agent access-node-id
pppoe intermediate-agent access-node-id is : abcd

12.15 show pppoe intermediate-agent identifier-string option delimiter

Command: show pppoe intermediate-agent identifier-string option delimiter
Function: Show the configured identifier-string, the combination format and delimiter of slot, port and vlan.
Parameter: None.
Command Mode: Admin mode
Default: The configuration information is null.
Usage Guide: Show the configured identifier-string, the combo format and delimiter of slot, port and vlan.
Example: Show the configuration information for pppoe intermediate-agent identifier-string.
Switch#pppoe intermediate-agent identifier-string abcd option spv delimiter # delimiter /
Switch# show pppoe intermediate-agent identifier-string option delimiter
config identifier string is : abcd
config option is : slot , port and vlan
the first delimiter is : "# "
the second delimiter is : "/ "

12.16 show pppoe intermediate-agent info

Command: show pppoe intermediate-agent info [interface ethernet <interface-name>]

Function: Show the related PPPoE IA configuration information of all ports or the specified port.

Parameter: ehernet: physical port

interface-name: port name

Command Mode: Admin mode

Default: The configuration information is null.

Usage Guide: Check the configuration information of the corresponding port, show whether the port is trust port, strip function is enabled, rate limit is enabled, show the configured circuit ID and remote ID.

Example: Show pppoe intermediate-agent configuration information of port ethernet1/0/2.

Switch# show pppoe intermediate-agent info interface ethernet 1/0/2

Interface	IA	Trusted	vendor Strip	Rate limit	circuit id	remote id
Ethernet1/0/2	yes	no	no	no	test1/port1	host1

Chapter 13 Commands for VLAN-ACL

13.1 clear vacl statistic vlan

Command: clear vacl [in | out] statistic vlan [<*1-4094*>]
Function: This command can clear the statistic information of VACL.
Parameter: in | out: Clear the traffic statistic of the ingress/egress.
vlan <*1-4094*>: The VLAN which needs to clear the VACL statistic information. If do not input VLAN ID, then clear all VLAN statistic information.
Command mode: Admin Mode.
Default: None.
Usage Guide: Egress direction filtering is not supported by switch.
Example:
Clear VACL statistic information of Vlan1.
Switch#clear vacl statistic vlan 1

13.2 show vacl vlan

Command: show vacl [in | out] vlan [<*1-4094*>] | [begin | include | exclude <*regular-expression*>]
Function: This command shows the configuration and the statistic information of VACL.
Parameter: in | out: Show ingress/egress configuration and statistic
vlan <*1-4094*>: The VLAN which needs to show the configuration and the statistic information of VACL. If do not input VLAN ID, then show VACL configuration and statistic information of all VLANs.
begin | include | exclude <*regular-expression*>: the regular expression
. match any characters except the line feed character
^ match the beginning of the row
$ match the end of the row
| match the character string at the left or right of upright line
[0-9] match the number 0 to the number 9
[a-z] match the lowercase a to z
[aeiou] match any letter in “aeiou”
\ Escape Character is used to match the intervocalic character, for example, \$ will match the $ character, but it is not match the end of the character string
\w match the letter, the number or the underline
\b match the beginning or the end of the words
\W match any characters which are not alphabet letter, number and underline
\B match the locations which are not the begin or end of the word

[^x] match any characters except x
[^aeiou] match any characters except including aeiou letters
* repeat zero time or many times
+ repeat one time or many times
(n) repeat n times
(n,) repeat n or more times
(n, m) repeat n to m times

At present, the regular expression used does not support the following syntaxes:
\s match the blank character
\d match the number
\S match any characters except blank character
\D match non-number character
? repeat zero time or one time

Command mode: Admin Mode.
Default: None.
Usage Guide: Egress direction filtering is not supported by switch.
Example:
Switch (config)#show vacl vlan 2
Vlan 2:
IP Ingress access-list used is 100, traffic-statistics Disable.
Switch (config)# show vacl vlan 3
Vlan 3:
IP Ingress access-list used is myacl, packet(s) number is 5.

Displayed Information	Explanation
Vlan 2	The name of VLAN
100, myacl	The name of VACL
traffic-statistics Disable	Disable VACL statistic function
packet(s) number is 5	The sum of out-profile data packets matching this VACL

13.3 vacl ip access-group

Command: vacl ip access-group {<1-299> | WORD} {in | out} [traffic-statistic] vlan WORD
no vacl ip access-group {<1-299> | WORD} {in | out} vlan WORD
Function: This command configure VACL of IP type on the specific VLAN.
Parameter: <1-299> | WORD: Configure the numeric IP ACL (include: standard ACL rule <1-99>, extended ACL rule <100-299>) or the named ACL.
in | out: Filter the ingress/egress traffic.
traffic-statistic: Enable the statistic of matched packets number.
vlan WORD: The VLAN will be bound to VACL.

Command mode: Global Mode.
Default: None.
Usage Guide: Use ";" or "-" to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering is not supported by switch.
Example: Configure the numeric IP ACL and enable the statistic function for Vlan 1-5, 6, 7-9.
Switch(config)#vacl ip access-group 1 in traffic-statistic vlan 1-5; 6; 7-9

13.4 vacl ipv6 access-group

Command: vacl ipv6 access-group (<500-699> | WORD) {in } (traffic-statistic|) vlan WORD

no ipv6 access-group {<500-699> | WORD} {in } vlan WORD

Function: This command configure VACL of IPv6 on the specific VLAN.
Parameter: <500-699> | WORD: Configure the IPv6 numeric standard ACL or IPV6 standard ACL rule.

inFilter the ingress traffic.

traffic-statistic: Enable the statistic of matched packets number.

vlan WORD: The VLAN will be bound to VACL.

Command mode: Global Mode.
Default: None.
Usage Guide: Use ";" or "-" to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering and extended IPv6 is not supported by switch.
Example: Configure the numeric IPv6 ACL for Vlan 5.
Switch(config)#vacl ipv6 access-group 600 in traffic-statistic vlan 5

13.5 vacl mac access-group

Command: vacl mac access-group {<700-1199> | WORD} {in } [traffic-statistic] vlan WORD

no vacl mac access-group {<700-1199> | WORD} {in } vlan WORD

Function: This command configure VACL of MAC type on the specific VLAN.
Parameter: <700-1199> | WORD: Configure the numeric IP ACL (include: <700-799> MAC standard access list, <1100-1199> MAC extended access list) or the named ACL.

in: Filter the ingress traffic.

traffic-statistic: Enable the statistic of matched packets number.

vlan WORD: The VLAN will be bound to VACL.

Command mode: Global Mode.
Default: None.
Usage Guide: Use ";" or "-" to input the VLAN or multi-VLANs, but do not exceed 128,

and CLI length cannot exceed 80 characters. Egress direction filtering is not supported by switch.

Example: Configure the numeric MAC ACL for Vlan 1-5.

Switch(config)#vacl mac access-group 700 in traffic-statistic vlan 1-5

13.6 vacl mac-ip access-group

Command: vacl mac-ip access-group {<3100-3299> | WORD} {in } [traffic-statistic] vlan WORD

no vacl mac-ip access-group {<3100-3299> | WORD} {in } vlan WORD

Function: This command configure VACL of MAC-IP type on the specific VLAN.

Parameter: <3100-3299> | WORD: Configure the numeric MAC-IP ACL or the named ACL.

in: Filter the ingress traffic.

traffic-statistic: Enable the statistic of matched packets number.

vlan WORD: The VLAN will be bound to VACL.

Command mode: Global Mode.

Default: None.

Usage Guide: Use ";" or "-" to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering is not supported by switch.

Example: Configure the numeric MAC-IP ACL for Vlan 1, 2, 5.

Switch(config)#vacl mac-ip access-group 3100 in traffic-statistic vlan 1;2;5

Chapter 14 Commands for SAVI

14.1 Commands for SAVI

14.1.1 ipv6 cps prefix

Command: ipv6 cps prefix <*ipv6-address*> vlan <*vid*>
no ipv6 cps prefix<*ipv6-address*>
Function: Configure IPv6 address prefix of the link manually, no command deletes IPv6 address prefix.
Parameter: ipv6-address: the address prefix of link, like 2001::/64;
vid: vlan ID of the current link.
Command Mode: Global Mode.
Default: None.
Usage Guide: Users should configure local address prefix: fe80::/64 of the link before enable the function of matching address prefix of the link, it accepts the packets of which source addresses are the local addresses of the link.
Example: Configure the address prefix of the link to 2001::/64.
Switch(config)#ipv6 cps prefix 2001::/64

14.1.2 ipv6 cps prefix check enable

Command: ipv6 cps prefix check enable
no ipv6 cps prefix check enable
Function: Enable SAVI address prefix check function, no command will disable this function.
Parameter: None.
Command Mode: Global Mode.
Default: Disable SAVI address prefix check function.
Usage Guide: After enable the prefix check function, if the IPv6 address prefix of the packets does not accord with the link prefix, then do not establish the corresponding IPv6 address binding. If users enable the matched address prefix of the link, configure the local address prefix of fe80::/64 first to accept the packets with the source address as local link address. Disable address prefix check function by default.
Example: Enable SAVI address prefix check function.
Switch(config)#ipv6 cps prefix check enable

14.1.3 ipv6 dhcp snooping trust

Command: ipv6 dhcp snooping trust

no ipv6 dhcp snooping trust

Function: Configure the port as dhcpv6 trust port, it does not establish dynamic DHCPv6 binding again and allows all DHCPv6 protocol packets to pass; no command deletes the port trust function.

Parameter: None.

Command Mode: Port Mode.

Default: Disable.

Usage Guide: Set the port as dhcpv6 trust attribute, enable uplink port of the switch with SAVI function for connecting dhcpv6 server or dhcpv6 relay generally.

Example: Set ethernet1/0/1 to be DHCP trust port.

Switch(config)#interface ethernet1/0/1

Switch(config-if-ethernet1/0/1)#ipv6 dhcp snooping trust

14.1.4 ipv6 nd snooping trust

Command: ipv6 nd snooping trust

no ipv6 nd snooping trust

Function: Configure the port as slaac trust and RA trust port, this port will not establish dynamic slaac binding anymore and forwards RA packets. The no command deletes the port trust function.

Parameter: None.

Command Mode: Port Mode.

Default: Disable port trust function.

Usage Guide: If the port disables ipv6 nd snooping trust function, it is considered to untrust RA packets port and discards all RA packets. Setting the port as trust attribute, enable the uplink port of the switch with SAVI or the conjoint port between switches with SAVI generally.

Example: Set the port ethernet1/0/1 to be nd trust port.

Switch(config)#interface ethernet1/0/1

Switch(config-if-etherne1/0/1)#ipv6 nd snooping trust

14.1.5 savi check binding

Command: savi check binding <*simple* | *probe*> mode

no savi check binding mode

Function: Configure the check mode for conflict binding; the no command deletes the check mode.

Parameter: simple mode: only check the port state for conflict binding, if the state is up, keep the conflict binding and do not set new binding. If the state is down, delete the conflict binding to set a new one

probe mode: besides checking the port state for conflict binding, it will send NS packets to probe the usability of the corresponding user when the port state is up. If receiving the responded NA packets from users, it will keep the current conflict binding

and does not set new binding, otherwise delete the conflict binding to set new one.
Command Mode: Global Mode.
Default: Disable the conflict binding check mode by default. It will adopt the mode that delete the conflict binding directly to set new one.
Usage Guide: It is recommended to configure probe mode to prevent the attack that the spurious address conflict binding deletes the legal user binding.
Example: Configure the conflict binding check mode to probe mode.
Switch(config)#savi check binding probe mode

14.1.6 savi enable

Command: savi enable
no savi enable
Function: Enable the global SAVI function, the no command disables this global function.
Parameter: None.
Command Mode: Global Mode.
Default: Disable the global SAVI function.
Usage Guide: Command configuration can be processed for SAVI function after enabling the global SAVI function. Because SAVI function has already contained security RA function, global SAVI function and security RA function are mutually exclusive in the global mode.
Example: Enable SAVI function.
Switch(config)#savi enable

14.1.7 savi ipv6 binding num

Command: savi ipv6 binding num <*limit-num*>
no savi ipv6 binding num
Function: Configure the number of the corresponding binding with the port, no command restores the default value.
Parameter: limit-num: set the range from 0 to 65535, the default value of the port binding number is 65535.
Command Mode: Port Mode.
Default: 65535.
Usage Guide: The configured binding number only include the dynamic binding type of slaac, dhcp. If the binding sum exceeds the configured number, this port does not create new dynamic binding any more, if the configured number is 0, this port does not create any dynamic binding.
Example: Configure the binding number to be 100 for port ethernet1/0/1.
Switch(config)#interface ethernet1/0/1
Switch(config-if-ethernet1/0/1)# savi ipv6 binding num 100

14.1.8 savi ipv6 check source binding

Command: savi ipv6 check source binding ip <*ip-address*> mac <*mac-address*> interface <*if-name*> {type [slaac | dhcp] lifetime <*lifetime*> | type static}

no savi ipv6 check source binding ip <*ip-address*> interface <*if-name*>

Function: Configure the static or dynamic binding function manually; the no command deletes the configured binding.

Parameter: ip-address: is the unicast IPv6 address, including local link and global unicast address

mac-address: is the mac address of Ethernet

if-name: is the port name, like interface ethernet 1/0/1

slaac|dhcp: slaac means create the dynamic binding for slaac type, **dhcp** means create the dynamic binding for dhcp type

lifetime: configure the lifetime period for the dynamic binding, the unit is second.

static: create the binding of the static type.

Command Mode: Global Mode.

Default: None.

Usage Guide: After the dynamic binding configured by handwork is overtime, the corresponding binding will be deleted but the configuration is still be kept, so the binding still be shown. If the binding needs to take effect again, it should delete it first and configure a new binding again.

When the binding type is static type, do not configure lifetime period, the lifetime period is infinite.

Example: Configure the dynamic binding of slaac type for SAVI manually.

Switch(config)#savi ipv6 check source binding ip 2001::10 mac 00-25-64-BB-8F-04 Interface ethernet1/0/1 type slaac lifetime 2010

Configure the static binding for SAVI manually.

Switch(config)#savi ipv6 check source binding ip 2001::20 mac 00-25-64-BB-8F-04 Interface ethernet1/0/1 type static

14.1.9 savi ipv6 check source ip-address mac-address

Command: savi ipv6 check source [ip-address mac-address | ip-address | mac-address]

no savi ipv6 check source

Function: Enable the control authentication function for the packets of the port, no command disables this function.

Parameter: None.

Command Mode: Port Mode.

Default: Disable the control filtering function of the port.

Usage Guide: The global SAVI function must be enabled before configuring this

command.

Example: Enable the control filtering function of the packets on port ethernet1/0/1.

Switch(config)#interface ethernet1/0/1

Switch(config-if-ethernet1/0/1)# savi ipv6 check source ip-address mac-address

14.1.10 savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

Command: savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

no savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

Function: Enable SAVI application scene function, no command disables the function.

Parameter: dhcp-only: dhcp-only application scene

slaac-only: slaac-only application scene

dhcp-slaac: combination application scene of dhcp-only and slaac-only

Command Mode: Global Mode.

Default: Disable SAVI application scene.

Usage Guide: dhcp-only application scene only detects DHCPv6 packets and DAD NS packets of link-local ipv6 address to be IPv6 address with target field, it does not detect DAD NS packets of non-link-local address. slaac-only application scene detects DAD NS packets of all types. dhcp-slaac combination application scene detects all DHCPv6 and DAD NS packets. Disable all kinds of application scene detection function for SAVI by default.

Example: Enable the specified dhcp-only application scene for SAVI.

Switch(config)#savi ipv6 dhcp-only enable

14.1.11 savi ipv6 mac-binding-limit

Command: savi ipv6 mac-binding-limit <*limit-num*>

no savi ipv6 mac-binding-limit

Function: Configure the dynamic binding number of the same MAC address, no command restores the default value.

Parameter: limit-num: set the ranging from 1 to 10, the default dynamic binding number is 32 for the same MAC address.

Command Mode: Global Mode.

Default: 32.

Usage Guide: This command is used to prevent the exhaust attack of the dynamic binding entry for SAVI.

Example: Set the dynamic binding number to be 5 for the same MAC address.

Switch(config)#isavi ipv6 mac-binding-limit 5

14.1.12 savi max-dad-dalay

Command: savi max-dad-delay <*max-dad-delay*>

no savi max-dad-delay

Function: Configure the dynamic binding at DETECTION state and send lifetime period of DAD NS packet detection, no command restores the default value.

Parameter: max-dad-delay: set the ranging between 1 and 65535 seconds, its default value is 1 second.

Command Mode: Port Mode.

Default: 1 second.

Usage Guide: It is recommended to use the default value.

Example: Set the detection lifetime as 2 seconds.

Switch(config)#savi max-dad-delay 2

14.1.13 savi max-dad-prepare-delay

Command: savi max-dad-prepare-delay <*max-dad-prepare-delay*>

no savi max-dad-prepare-delay

Function: Configure lifetime period of redetection for the dynamic binding, no command restores the default value.

Parameter: max-dad-prepare-delay: set the ranging between 1 and 65535 seconds, its default value is 1 second.

Command Mode: Global Mode.

Default: 1 second.

Usage Guide: It is recommended to user the default value.

Example: Set the redetection lifetime as 2 seconds.

Switch(config)#savi max-dad-prepare-delay 2

14.1.14 savi max-slaac-life

Command: savi max-slaac-life <*max-slaac-life*>

no savi max-slaac-life

Function: Configure lifetime period of slaac dynamic binding at BOUND state, no command restores the default value.

Parameter: max-slaac-life: set the ranging between 1 and 31536000 seconds, its default value is 4 hours.

Command Mode: Global Mode.

Default: 4 hours.

Usage Guide: None.

Example: Configure lifetime period of slaac binding type as 2010 seconds at BOUND state.

Switch(config)#savi max-slaac-life 2010

14.1.15 savi timeout bind-protect

Command: savi timeout bind-protect <*protect-time*>
no savi timeout bind-protect
Function: Configure the bind-protect lifetime period for a port after its state from up to down, no command restores the default value.
Parameter: protect-time: set the ranging between 1 and 300 seconds, its default value is 30 seconds.
Command Mode: Global Mode.
Default: 30 seconds.
Usage Guide: After the configured lifetime period is overtime, the port is still at down state, the binding of this port will be deleted. If the port state is changed from down to up state during the configured lifetime period, the binding of the port will reset it as lifetime period of BOUND state. If the configured parameter is 0 second, all binding of the port will be deleted immediately.
Example: Set bind-protect lifetime period to be 20 seconds.
Switch(config)#savi timeout bind-protect 20

14.2 Commands for Monitor and Debug

14.2.1 Monitor and Debugg

14.2.1.1 debug ipv6 dhcp snooping binding

Command: debug ipv6 dhcp snooping binding
no debug ipv6 dhcp snooping binding
Function: Enable binding debug of dhcp type for SAVI, no command disables the debug.
Parameter: None.
Command Mode: Admin Mode.
Default: None.
Usage Guide: After enable this function, the relative binding of dhcp type or static type create the print information for misarranging. The no command disables this function.
Example: Enable the binding debug of dhcp type.
Switch#debug ipv6 dhcp snooping binding

14.2.1.2 debug ipv6 dhcp snooping event

Command: debug ipv6 dhcp snooping event
no debug ipv6 dhcp snooping event
Function: Enable event debug of dhcp type for SAVI, no command disables the debug.
Parameter: None.
Command Mode: Admin Mode.
Default: None.

Usage Guide: After enable event debug, the relative event information of dhcp type will be print for misarranging. The no command disables this function.
Example: Enable binding event debug of dhcp type.
Switch#debug ipv6 dhcp snooping event

14.2.1.3 debug ipv6 dhcp snooping packet

Command: debug ipv6 dhcp snooping packet
no debug ipv6 dhcp snooping packet
Function: Enable the debug of DHCPv6 packets, no command disables the debug.
Parameter: None.
Command Mode: Admin Mode.
Default: None.
Usage Guide: After enable packets debug, the relative DHCPv6 packtets will be print for misarranging. The no command disables this function.
Example: Enable the debug of DHCPv6 packets.
Switch#debug ipv6 dhcp snooping packet

14.2.1.4 debug ipv6 nd snooping binding

Command: debug ipv6 nd snooping binding
no debug ipv6 nd snooping binding
Function: Enable the binding debug of slaac type for SAVI, no command disables the binding debug.
Parameter: None.
Command Mode: Admin Mode.
Default: None.
Usage Guide: After enable binding debug, the relative binding of slaac type will create the print information for misarranging. The no command disables this function.
Example: Enable binding debug of slaac type.
Switch#debug ipv6 nd snooping binding

14.2.1.5 debug ipv6 nd snooping event

Command: debug ipv6 nd snooping event
no debug ipv6 nd snooping event
Function: Enable the event debug of slaac type for SAVI, no command disables the event debug.
Parameter: None.
Command Mode: Admin Mode.
Default: None.
Usage Guide: After enable event debug, the relative event information of slaac type will be print for misarranging. The no command disables this function.

Example: Enable the event debug of slaac type.
Switch#debug ipv6 nd snooping event

14.2.1.6 debug ipv6 nd snooping packet

Command: debug ipv6 nd snooping packet
no debug ipv6 nd snooping packet
Function: Enable ND packets debug, no command disables ND packets debug.
Parameter: None.
Command Mode: Admin Mode.
Default: None.
Usage Guide: After enable packets debug, the relative ND packets will be print for misarranging. The no command disables this function.
Example: Enable ND packets debug.
Switch#debug ipv6 nd snooping packet

14.2.1.7 show savi ipv6 check source binding

Command: show savi ipv6 check source binding [interface<*if-name*>]
Function: Show the global SAVI binding entry list.
Parameter: if-name: port name such as interface ethernet 1/0/1.
Command Mode: Admin Mode.
Default: None.
Usage Guide: Descriptions of each field are as below:

Field	Description
MAC	The bound MAC address
IP	The bound IP address
Vlan	The binding VLAN belongs to
Port	The binding port belongs to
Type	Binding type
State	Binding state
Expires	The bound lifetime period

Example: Show the global binding state of SAVI.
Switch(config)#show savi ipv6 check source binding

Static binding count: 0
Dynamic binding count: 3
Binding count: 3

MAC IP VLAN Port Type State Expires

```
00-25-64-bb-8f-04  fe80::225:64ff:febb:8f04  1 Ethernet1/0/5 slaac  BOUND  14370
00-25-64-bb-8f-04  2001::13   1    Ethernet1/0/5  slaac   BOUND     14370
00-25-64-bb-8f-04  2001::10   1    Ethernet1/0/5  slaac   BOUND     14370
------------------------------------------------------------------------------------------------------------
```