IP ACL Application Configuration Commands

Table of contents

CHAPTER 1 IP ACL APPLICATION CONFIGURATION COMMANDS

1.1. IP ACL Application Configuration Commands

IP ACL Application Configuration Commands include:

- ip access-group
- ipv6 access-group

1.1.1. ipv6 access-list

Syntax

To configure the name of access list and enter IPv6 ACL configuration mode, run the following command. To return to the default setting, use the no form of this command.

ipv6 access-list *access-list-name*

no ipv6 access-list *access-list-name*

Parameter

Parameter	Description
access-list-name	access list name

Default value

There is no default access list. There must be configured with access list name.

Command mode

Global configuration mode. The command is used to enter IPv6 access control list configuration mode.

Usage guidelines

1. IPv6 will not use number access list and the number will also be handled as name access list. The access list of IPv4 and IPv6 cannot use the same name, or the port cannot be identified.
2. The default configuration of IPv6 ACL is to enable ND packets of ICMPv6 (equivalent to ARP of IPv4). That's, when using deny configuration rule, add permit any any to the last command. The rules as follows:

permit icmpv6 any any nd-na

permit icmpv6 any any nd-ns

deny ipv6 any any

Example

The following example shows how to create an IPv6 access control list. Use deny to deny packets whose source address prefix is FEC0:0:0:2::/64 and whose destination

address is any. Meanwhile, other packets are permitted and apply the command to gigabit Ethernet interface G1/1.

ipv6 access-list list2

deny FEC0:0:0:2::/64 any

permit ipv6 any any

interface G1/1

ipv6 access-group list2 egress

Related command

deny (IPv6)

permit (IPv6)

ipv6 access-group

show ipv6 access-list

1.1.2. ipv6 access-group

Syntax

To designate an access group, run the ipv6 access-group. To cancel the designated access group, run no ipv6 access-group.

Use it on the interface

[**no**] **ipv6 access-group** *name* **[egress]**

Use it in the global mode

[**no**] **ipv6 access-group** *name* **[vlan {***word* **| add** *word* **| remove** *word***}]**

To apply or delete a created IPv6 ACL on a port or in global mode, run this command.

Parameters

Parameters	Description
name	Name of the IP access control list
egress	THE ACCESS LIST IS APPLIED IN EGRESS.
Vlan	THE ACCESS LIST IS APPLIED IN INGRESS.
Word	VLAN RANGE TABLE
add	ADD VLAN RANGE TABLE
remove	DELETE VLAN RANGE TABLE

Command Mode

Global configuration mode or interface configuration mode

Usage Guidelines

Most rules in the ACL take effect through hardware; those that hardware does not support give no errors but they have no actual effects; a few rules such as time-range take effect through software.

Note:

The IPv6 ACL supports the following rules:

any: means any IP address.

Ipv6-addr/ host *Ipv6-addr:* means IPv6 address match-up.

ip-protocol: means the IPv6 protocol ID.

eq/gt/lt/src-portrange: means TCP/UDP port ID match-up.

dscp/flow-label: means field match-up.

Example

The following example shows how to apply the ACL filter at the ingress direction of interface g0/1.

Switch_config#inter g0/1

Switch_config_g0/1# ipv6 access-group filter

1.1.3. deny/permit

Syntax

To deny certain packets, run the following command. To return to the default setting, use the no form of this command.

deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]

no deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]

deny icmpv6 {*source-ipv6-prefix/prefix-length* | any | host *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | any | host *destination-ipv6-address*} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [dest-option-type [*doh-number* | *doh-type*]] [dscp *value*] [flow-label *value*] [fragments] [log] [log-input] [routing] [sequence *value*] [time-range *name*]

deny tcp {*source-ipv6-prefix/prefix-length* | any | host *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | any | host *destination-ipv6-address*} [*operator* [*port-number*]] [ack] [dest-option-type [*doh-number* | *doh-type*]]

[dscp *value*] [established] [fin] [flow-label *value*] [fragments] [log] [log-input] [neq {*port* | *protocol*}] [psh] [range {*port* | *protocol*}] [routing] [rst] [sequence *value*] [syn] [time-range *name*] [urg]

deny udp {*source-ipv6-prefix*/*prefix-length* | any | host *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | any | host *destination-ipv6-address*} [*operator* [*port-number*]] [dest-option-type [*doh-number* | *doh-type*]] [dscp *value*] [flow-label *value*] [fragments] [log] [log-input] [neq {*port* | *protocol*}] [range {*port* | *protocol*}] [routing] [sequence *value*] [time-range *name*]

Green color: deny fields which protocol, deny icmp, deny tcp and deny udp have.

Red color: deny fields which protocol has but deny icmp, deny tcp or deny udp hasn't; neither permit.

Blue: deny fields which protocol hasn't but deny icmp, deny tcp or deny udp has.

For enabled packets, use command permit and other related setting rule of permit. Use the no form of this command to return to the default setting.

permit *protocol* {*source-ipv6-prefix*/*prefix-length* | any | host *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | any | host *destination-ipv6-address*} [dscp *value*] [flow-label *value*] [fragments] [log] [log-input] [routing] [sequence *value*] [time-range *name*] [undetermined-transport]

no permit protocol {source-ipv6-prefix**/**prefix-length | **any** | **host** source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix**/**prefix-length | **any** | **host** destination-ipv6-address} [**dscp** value] [**flow-label** value] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** value] [**time-range** name] [**undetermined-transport**]

permit icmpv6 {source-ipv6-prefix**/**prefix-length | **any** | **host** source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix**/**prefix-length | **any** | **host** destination-ipv6-address} [icmpv6-type [icmpv6-code] | icmpv6-message] [**dscp** value] [**flow-label** value] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** value] [**time-range** name]

permit tcp {source-ipv6-prefix**/**prefix-length | **any** | **host** source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix**/**prefix-length | **any** | **host** destination-ipv6-address} [operator [port-number]] [**ack**] [**dscp** value] [**established**] [**fin**] [**flow-label** value] [**fragments**] [**log**] [**log-input**] [**neq** {port | protocol}] [**psh**] [**range** {port | protocol}] [**routing**] [**rst**] [**sequence** value] [**syn**] [**time-range** name] [**urg**]

permit udp {source-ipv6-prefix**/**prefix-length | **any** | **host** source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix**/**prefix-length | **any** | **host** destination-ipv6-address} [operator [port-number]] [**dscp** value] [**flow-label** value] [**fragments**] [**log**] [**log-input**] [**neq** {port | protocol}] [**range** {port | protocol}] [**routing**] [**sequence** value] [**time-range** name]

Parameter

Parameter	Description
protocol	Network protocol name or protocol number. The current

	supported protocol name are ahp(51), esp(50), icmpv6(58), ipv6(41), pcp(108), sctp(132), tcp(6) and udp(17).
*source-ipv6-prefix***/***prefixlength*	Source IPv6 prefix/prefix length.
any	Abbreviation of IPv6 prefix ::/0.
host *source-ipv6-address*	Source IPv6 host address.
operator [*port-number*]	(optional) operational character and port number are only effective for tcp and udp protocol. Operator has **lt** (less than), **gt** (greater than), **eq**(equal), **neq**(not equal) and **range**(inclusive range). The operator **range** has two port numbers and other operators only have one port number. The value range of *port-number* is 0 to 65535.
*destination-ipv6-prefix***/***prefix-length*	Destination IPv6 prefix/prefix length
host *destination-ipv6-address*	Destination IPv6 host address
dscp *value*	(optional) differentiated services code point) (dscp, differentiated services code point). It is used for matching IPv6 packet header Traffic Class domain, 0-63. The existed definitions are af11(001010), af12(001100), af13(001110), af21(010010), af22(010100), af23(010110), af31(011010), af32(011100), af33(011110), af41(100010), af42(100100), af43(100110), cs1(001000), cs2(010000), cs3(011000), cs4(100000), cs5(101000), cs6(110000), cs7(111000), ef(101110), default(000000)
flow-label *value*	(optional) Flow label of IPv6 packet header, 1-1048575(1024*1024-1)
fragments	If the fragment header has non-0 offset, it will match the non-initiated fragment header group. Only ***operator* [*port-number*]** does not be claimed, **fragments** are optional.
log	(optional) When grouping match, send log information to the console port. The log information includes access list name, serial number, grouping deny/permit, protocol/protocol number (TCP, UDP, ICMPv6, etc.), source

	address/destination address, source port number/destination port number.
log-input	(optional) It has the same function with log. It also includes packet ingress.
routing	(optional) Matching the route extended header of IPv6 grouping.
sequence *value*	(optional) It is used to designate the serial number of the access list, which is easy for the client to add 1-4294967295 (65536*65536-1). IPv4 access list can only add the rule to the last, while IPv6 can add the rule to any position by make use of sequence. If there is rule on the position of new added sequence number, the rule will be overlapped.
time-range *name*	(optional) Set the time range of the access list. In command **time-range**, apply time rule name to the access list with the key words **absolute/periodic**.
undetermined-transport	(optional) Match grouping which layer-4 protocol cannot distinguish. Only protocol is not claimed, can **undetermined-transport** is optional. If protocol is ipv6, it means that layer-4 protocol of IPv6 is not claimed.
icmpv6-type	(optional) Packet type of ICMPv6, 0-255.
icmpv6-code	(optional) ICMPv6 packet code, 0-255.
icmpv6-message	(optional) pass ICMPv6 packet name (RFC specified packet name and ICMP packet type constituted by the packet code, such as destination unreachable), 0 to 255.
ack	(optional) Used only for TCP packets, acknowledgment (ACK) setting.
fin	(optional) Used only for TCP packets, finish (FIN) matching.
psh	(optional) Used only for TCP packets, push (PSH) set.
rst	(optional) Used only for TCP packets, reset (RST) set.
syn	(optional) Used only for TCP packets, synchronize (SYN) matching set.

urg	Used only for TCP packets, urgent (URG) matching set.
established	(optional) Used only for TCP packets. When ACK or RST of TCP packets are set, it means the match is established. When the rule is used as deny, it is used to deny the connection from external network to inner network, but enables connection from inner network to the external network.
eq{*port* | *protocol*}	(optional) Used only for grouping of designated port number. Protocol is the designated protocol name.
gt{*port* | *protocol*}	(optional) Used only for grouping greater than the designated port number. Protocol is the designated protocol name.
lt {*port* | *protocol*}	(optional) Used only for grouping smaller than the designated port number. Protocol is the designated protocol name.
neq {*port* | *protocol*}	(optional) Only matching with grouping not in the designated port number. Protocol is the designated protocol name.
range {*port* | *protocol*}	(optional) Only matching with grouping in the designated port number. Protocol is the designated protocol name.

Default value

Serial number:

Different with ACL of IPv4, ACL of IPv6 can add in any position of the existed access list with permit, deny and sequence, not only limited to the end of ACL. Therefore, the access list needs to be numbered. If the user does not configure the sequence number of the access list manually, the first default ACL serial No. is 10, add 10 successively; if the user designated sequence number, it will be inserted accordingly; if the user designated sequence number is the same with that of existed ACL, the existed ACL will be overlapped. If the last sequence number designated by the user is not an integral multiple of 10, when ACL rule is added without designating the sequence number, the sequence number will be the sequence number of the last rule plus 10.

Default rule

Similar to IPv4 ACL, if configured ACL name, but without configuring the rule, the access list will not disable any rule.

permit icmpv6 any any nd-na

permit icmpv6 any any nd-ns

permit ipv6 any any

It should be noted that as ICMP of IPv6 is equivalent to ARP of IPv4, the neighbor inform and neighbor request of the neighbor discovery can pass by default. If one rule is configured in IPv6 ACL rule, the implied condition of disqualifying the rule is to enable ICMPv6 packets, but disable all IPv6 packets.

permit icmp any any nd-na

permit icmp any any nd-ns

deny ipv6 any any

Therefore, if enable packets disqualifying the rule is disabled, add to IPv6 ACL one command: permit ipv6 any any.

Command mode

IPv6 access list configuration mode

Usage guidelines

1. Packet name of ICMPv6 as follows:

- beyond-scope
- destination-unreachable
- echo-reply
- echo-request
- header
- hop-limit
- mld-query
- mld-reduction
- mld-report
- nd-na
- nd-ns
- next-header
- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- port-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded

- unreachable

2. Defined protocols on TCP port number:

- bgp(179)
- chargen(19)
- cmd(514)
- daytime(13)
- discard(9)
- domain(53)
- echo(7)
- exec(512)
- finger(79)
- ftp(21)
- ftp-data (20)
- gopher (70)
- hostname (101)
- ident (113)
- irc (194)
- klogin (543)
- kshell (544)
- login (513)
- lpd (515)
- nntp (119)
- pim-auto-rp (496)
- pop2 (109)
- pop3 (110)
- smtp (25)
- sunrpc (111)
- syslog (514)
- talk (517)
- time (37)
- uucp (540)
- whois (43)
- www (80)

3. Defined protocols on UDP port number:

- biff (512)
- bootpc (68)
- bootps (67)
- discard (9)
- dnsix (195)
- domain(53)
- echo(7)

- isakmp (500)
- netbios-dgm (138)
- netbios-ns (137)
- netbios-ss (139)
- ntp (123)
- pim-auto-rp (496)
- rip (520)
- snmp (512)
- snmptrap (162)
- sunrpc (111)
- syslog (514)
- talk (517)
- tftp (69)
- time (37)
- who (513)
- xdmcp (177)

Example

The following example shows how to create an IPv6 access list named “example” and set four rules for it. Rule 1: Deny all tcp connected packets whose port destination port number is bigger than 5000; Rule 2: Deny all udp packets whose source port number is smaller than 5000. Rule 3: Enable all icmpv6 packets; Rule 4: Enable all packets which are not satisfy the rule. Note: When configuring access list, if packets not satisfy the rule are not denied, please add the rule. Lastly, in the interface configuration mode, apply the rule to the egress of Ethernet port g2/1.

```
ipv6 access-list example
deny tcp any any gt 5000
deny udp ::/0 lt 5000 ::/0 log
permit icmpv6 any any
permit any any
int gigaEthernet 2/1
ipv6 access-group example egress
```

Related command

ipv6 access-list

ipv6 access-group

show ipv6 access-list

list

1.1.4. Sequence

Syntax

To insert a new access list or overlap the existed access list in any position, run the following command. To return to the default setting, use the no form of this command.

sequence *value* {**deny | permit**} *protocol* {*source-ipv6-prefix***/***prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix***/***prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** *name*] [**undetermined-transport**]

no sequence *value* {**deny | permit**} *protocol* {*source-ipv6-prefix***/***prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix***/** *prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** *name*] [**undetermined-transport**]

sequence {**deny | permit**} **icmpv6** {*source-ipv6-prefix***/***prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix***/***prefix-length* | **any** | **host** *destination-ipv6-address*} [*icmpv6-type* [*icmpv6-code*] | *icmpv6-message*] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**time-range** *name*]

sequence {**deny | permit**} **tcp** {source-ipv6-prefix**/**prefix-length | **any** | **host** source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix**/**prefix-length | **any** | **host** destination-ipv6-address} [operator [port-number]] [**ack**] [**dscp** value] [**established**] [**fin**] [**flow-label** value] [**fragments**] [**log**] [**log-input**] [**neq** {port | protocol}] [**psh**] [**range** {port | protocol}] [**routing**] [**rst**] [**syn**] [**time-range** name] [**urg**]

sequence {**deny | permit**} **udp** {source-ipv6-prefix**/**prefix-length | **any** | **host** source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix**/**prefix-length | **any** | **host** destination-ipv6-address} [operator [port-number]] [**dscp** value] [**flow-label** value] [**fragments**] [**log**] [**log-input**] [**neq** {port | protocol}] [**range** {port | protocol}] [**routing**] [**time-range** name]

Parameter

Reference to deny/permit in 1.1.3, which only puts the key words of sequence in the front.

Default value

The same with deny/permit in 1.1.3.

Command mode

IPv6 access list configuration mode

Usage guidelines

ACL can be added in any position with permit, deny, remark, evaluate, but not only limited to the end of ACL. Between two existed ingresses add an appropriate ingress number. The default first ACL ingress number is 10 and the subsequent ACL ingress number is 10 increased successively.

Keywords of sequence is used for:

If seq is not designated, the first seq=10, increase successively after that;

If seq is designated, ipv6acl without seq will be added to the end, and add 10 to the last seq;

If seq is designated, ipv6acl with seq will inserted in the middle;

If seq is designated, ipv6acl with seq and seq is the same with the current, renew ipv6acl of the seq;

If directly designate seq XXX, it means seq XXX deny 0 any any;

Guidelines of other commands are the same with deny/permit in 1.1.3.

Example

The following example shows how to configure as 1.1.3 but only adds the sequence number in the front.

ipv6 access-list example

sequence 30 deny tcp any any gt 5000

sequence 70 deny udp ::/0 lt 5000 ::/0 log

sequence 75 permit icmpv6 any any

sequence 76 permit any any

Add a new rule to the existed rule:

deny ipv6 FE80::/64 any log-input

The rule will be added to the end and automatically number the sequence as 76+10=86. If the user designates the sequence number when add the new rule, run the following command:

sequence 50 deny ahp any any

or deny ahp any any sequence 50

The rule will be inserted into rule sequence No.30 and No.70. If the sequence number designated by the user is the same with that of the existed one, run the following command.

sequence 75 deny esp any any log

or deny esp any any log sequence 75

In the existed access list, the rule numbered 75 will be overlapped. Change of the access list adding 3 rules is shown below:

ipv6 access-list example

sequence 30 deny tcp any any gt 5000

sequence 50 deny ahp any any

sequence 70 deny udp ::/0 lt 5000 ::/0 log

sequence 75 deny esp any any log

sequence 76 permit any any

deny ipv6 FE80::/64 any log-input sequence 86

Related command

deny(IPv6)

permit(IPv6)

ipv6 access-list

ipv6 access-group

show ipv6 access-list

list

1.1.5. show ipv6 access-list

To show IPv6 ACL information, run the following command.

show ipv6 access-list [*access-list-name*]

Parameter

Parameter	Description
access-list-name	access list name

Default value

If there is no access list input, all access lists will be shown.

Command mode

Global configuration mode or management mode

Usage guidelines

The command **show ipv6 access-list** is used to show the format of IPv6 access list, which is different with the command **show running** for showing the format of IPv6 ACL. When using the command **show running**, the rule with designated sequence number will be shown in the beginning, otherwise, it will be shown in the end. Reference to example in 1.1.4. When using command **show ipv6 access-list**, whether designated the sequence number, the rule with sequence number will be shown in the end. Refer to example in this section.

Example

The following example shows how to show example 1 and example 2 by entering the command **show ipv6 access-list**.

```
ipv6 access-list example1
  permit ipv6 any any sequence 10
  deny icmpv6 any any 255 255 routing sequence 20
ipv6 access-list example2
  permit icmpv6 12::/0 host 34:: header dscp ef fragments sequence 20
  permit icmpv6 any any header flow-label 987 sequence 30
  deny ahp any any routing log time-range example_TIMER sequence 50
```

deny icmpv6 any any 255 255 sequence 8918

permit any any sequence 8928

Enter command **show ipv6 access-list example1** and show example 1.

ipv6 access-list example1

permit ipv6 any any sequence 10

deny icmpv6 any any 255 255 routing sequence 20

Related command

ipv6 access-list