

IP ACL APPLICATION CONFIGURATION COMMANDS



IP ACL Application Configuration Commands



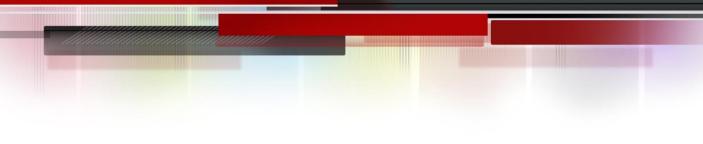


Table of contents

CHAPTE	R 1 IP ACL APPLICATION COMMANDS	3
1.1. Cor	nfiguration Commands for Applying IP ACL	3
1.1.1.	ip access-group	3
1.1.2.	ipv6 access-group	4



IP ACL Application Configuration Commands CHAPTER 1. IP ACL Application Commands

CHAPTER 1 IP ACL APPLICATION COMMANDS

1.1. Configuration Commands for Applying IP ACL

The commands for applying the IP Access Control List (ACL) are shown below:

3

- ip access-group
- ipv6 access-group

1.1.1. ip access-group

Syntax

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

To apply a created IP ACL on a port, run the following command:

[no] ip access-group name [egress]

To apply a created IP ACL globally, run the following command:

[no] ip access-group name [egress | vlan {word | add | remove}]

You can use this command to apply the established IP ACL to an interface or globally or cancel the applied IP ACL on an interface or globally.

Parameter

Parameter	Description
name	Stands for the name of IP ACL.
egress	Applies the ACL in an outbound direction.
Vlan	Applies the ACL in an inbound VLAN.
Word	Stands for the VLAN range table.
add	Adds VLANID.
remove	Cancels VLANID.

Command mode

Global or port 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.

Δ

Note:

The IPv4 standard ACL supports the following rules:

any: means any source IP address.

source-addr source-mask: means matching up the source address.

reverse-mask *source-addr source-mask*: means to use the reverse source address for match-up.

The IPv4 extended ACL supports the following rules:

any: means any IP address.

ip-protocol: means the IP protocol ID.

ip-addr source-mask: means IP address match-up.

Interface *interface-id*: means layer-3 interface match-up.

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

totallen: means the length match-up of IP packets.

established/tos/is-fragment/not-fragment/precedence/ttl/offset-not-zero/offsetzero/donotfragment-set/ donotfragment-notset/*icmp-type*: means field match-up, among which ttl must be set to equal.

time-range: configures effective time

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# ip access-group filter

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**.

To apply a created IPv6 ACL on a port, run the following command:

[no] ipv6 access-group name [egress]

To apply a created IPv6 ACL globally, run the following command:

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

You can use this command to apply the established IPv6 ACL to an interface or globally or cancel the applied IPv6 ACL on an interface or globally.



IP ACL Application Configuration Commands CHAPTER 1. IP ACL Application Commands

Parameter

Parameter	Description
name	Stands for the name of IPv6 ACL.
egress	Applies the IPv6 ACL in an outbound direction.
Vlan	Applies the IPv6 ACL in an inbound VLAN.
Word	Stands for the VLAN range table.
add	Adds the VLANID.
remove	Cancels the VLANID.

5

Command mode

Global configuration mode or port 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 IPv6 address.

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

Ipv6-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.

time-range: configures effective time

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

