

IP ACL Application Commands

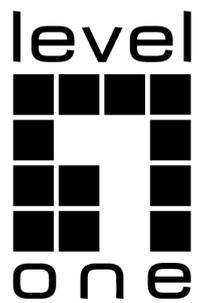


Table of Contents

| | |
|-----------------------------------------------------|---|
| IP ACL Application Configuration Commands..... | 1 |
| Table of Contents | 1 |
| Chapter 1 IP ACL Application Commands | 1 |
| 1.1 Configuration Commands for Applying IP ACL..... | 1 |
| 1.1.1 ip access-group..... | 1 |

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:

- ip access-group

1.1.1 ip access-group

Syntax

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.

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

[no] ip access-group *name* [egress][stat-packet | stat-byte]

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

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

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 |
|--------------------|------------------------------------------------|
| <i>name</i> | Stands for the name of access list. |
| egress | The access list is applied in the egress. |
| Vlan | The access list is applied to the ingress VLAN |
| <i>word</i> | Stands for the VLAN range table. |
| <i>add</i> | Addes VLANID to current configuration list |
| <i>remove</i> | Removes VLANID from current configuration list |
| stat-packet | Statistics based on the number of packets |
| stat-byte | Byte-based statistics |

Command mode

Global or port configuration mode

Usage guidelines

Most of the rules in the ACL are implemented by hardware, and the non-supported rules does not prompt an error, but has no actual effect; a small amount, such as time-range, is implemented by software.

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 ip-mask: means IP address match-up.

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

eq/gt/lt/neq/src-portrange/dst-portrange: *tcp/udp*: means port ID match-up.

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

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

tos: means the tos priority match-up

cos: means the cos priority match-up

precedence: means the precedence priority match-up

time-range: effective time configuration

Example

The following example shows how to apply the ACL filter at the ingress direction of interface g0/0/1.

```
Switch(config)#interface g0/0/1
```

```
Switch(config-g0/0/1)# ip access-group filter
```