IP ACL Application Configuration Commands
Table of Contents

IP ACL Application Configuration Commands.................................................................................................................1
Table of Contents ...........................................................................................................................................................I
Chapter 1 IP ACL Application Commands ..................................................................................................................1
  1.1 Configuration Commands for Applying IP ACL..................................................................................................1
    1.1.1 ip access-group ..................................................................................................................................1
    1.1.2 ipv6 access-group ................................................................. 2
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
- ipv6 access-group

1.1.1 ip access-group

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:

```plaintext
[no] ip access-group name [egress]
```

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

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

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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Stands for the name of IP ACL.</td>
</tr>
<tr>
<td>egress</td>
<td>Applies the ACL in an outbound direction.</td>
</tr>
<tr>
<td>Vlan</td>
<td>Applies the ACL in an inbound VLAN.</td>
</tr>
<tr>
<td>Word</td>
<td>Stands for the VLAN range table.</td>
</tr>
<tr>
<td>add</td>
<td>Adds a VLAN range table.</td>
</tr>
<tr>
<td>remove</td>
<td>Cancels a VLAN range table.</td>
</tr>
</tbody>
</table>

Command mode

Global or port configuration mode
Explanation

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 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/offset-zero/don offragment-set/ donotfragment-notset/icmp-type: means field match-up, among which ttl must be set to equal.

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

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

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

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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Stands for the name of IPv6 ACL.</td>
</tr>
<tr>
<td>egress</td>
<td>Applies the IPv6 ACL in an outbound direction.</td>
</tr>
<tr>
<td>Vlan</td>
<td>Applies the IPv6 ACL in an inbound VLAN.</td>
</tr>
<tr>
<td>Word</td>
<td>Stands for the VLAN range table.</td>
</tr>
<tr>
<td>add</td>
<td>Adds the VLAN range table.</td>
</tr>
<tr>
<td>remove</td>
<td>Cancels the VLAN range table.</td>
</tr>
</tbody>
</table>

Command mode

- Global configuration mode or port configuration mode

Explanation

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.
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
```