IPv6 ACL Configuration

Table of Contents

Chapter 1 IPv6 ACL Configuration

1.1 IPv6 ACL Configuration

1.1.1 Filtering IPv6 Packets

Filtering IPv6 packets helps the control packet run in the network. Such control can limit network transmission and network running by a certain user or device. For enabling or disabling packets from the cross designated port, we provide with ACL. You can use IPv6 ACL as follows:

- Limit of packet transmission on the port
- Limit of virtual terminal line access
- Limit of the route update

This chapter summarizes how to set up IPv6 ACL and how to apply them.

IPv6 ACL is a well-organized set which applies enable/disable of IPv6 address. ROS of the switch will test addresses in ACL accordingly. The first match determines whether the software accept or refuse the address. Because after the first match, the software will stop the match rule, the sequence of the condition is important. If there is no rule to match, the address will be refused.

Steps for using ACL:

(1) Set up ACL by designating ACL name and ACL conditions.

(2) Apply ACL to the port.

1.1.2 Setting up IPv6 ACL

Use a character string to set up IPv6 ACL.

Note:

The standard ACL and the expanded ACL cannot be the same.

In order to set up IPv6 ACL, run the following command in the global configuration mode.

Command	Purpose
IPv6 access-list *name*	Use the name to define an IPv6 ACL.
{**deny** | **permit**} *protocol* {*source-ipv6-prefix*|*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]]	In the configuration mode of IPv6 ACL, designate one or multiple enable/disable conditions. This determines whether to pass

{*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*]	the packet or not. (dscp is used for matching IPv6 grouping header Traffic Class domain, flow-label is used for matching Flow Label tag domain of IPv6 grouping header, fragments is used for matching fragment grouping when the grouping expansion header includes none-0 offset; log means whether to record log, routing is used for the source grouping of the route expansion header of IPv6 grouping header, time-range is used for limit the time range of ACL.)
Exit	Exit from the configuration mode of ACL.

After setting up ACL, any additional parts will be affiliated to the end of the ACL if no sequence is added to the rule deny or permit. In other words, add [**sequence** value] in the front or back of the rule deny/permit, you can add ACL commands in any position of the designated ACL.

Likewise, you can use “no permit” and “no deny” to delete an item in ACL or “no sequence” to delete the rule in a certain position directly.

Note:

When setting up ACL, please remember the end sentence of ACL by default covers the sentence of **deny ipv6 any any.**

The ACL must be applied to the line or port after being set up. Refer to the description of “Apply the ACL to the port”.

1.1.3 Applying ACL to the Ports

ACL can be applied to one or multiple ports or the ingress.

Run this command in the configuration mode.

Command	Purpose
IPv6 access-group *name*	Apply ACL to the port.

For the standard ingress ACL, check the source address of the packet after receiving it. For the expanded ACL, the routing switch also checks the objective address. If the ACL enables the address, the software continues to handle the packet. If ACL does not allow the address, the software will drop the packet and returns one ICMP host unreachable packets.

If there is no designated ACL, all packets will be allowed to pass.

1.1.4 Examples of IPv6 ACL

In the following example, please first enable to connect with the individual destination host of the host A:B:C:D::E and disable the new TCP to connect with SMTP port whose host IPv6 source prefix 255:255:255::/48. The next rule sequence of the final ACL comes before the former rule.

```
Switch_config#ipv6 access-list xxcom
Switch_config_ipv6acl#permit any host A:B:C:D::E sequence 20
Switch_config_ipv6acl#deny tcp any 255:255:255::/48 eq 25 sequence 10
Switch_config_ipv6acl#ex
Switch_config#show ipv6 access-lists xxcom
ipv6 access-list xxcom
    deny tcp any 255:255:255::/48 eq smtp sequence 10
    permit ipv6 any host A:B:C:D::E sequence 20
```