

IP Access List Configuration

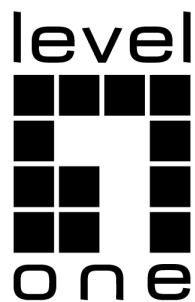


Table of Contents

Chapter 1	Configuring IP Access List.....	1
1.1	Configuring IP Access List	1
1.1.1	Filtering IP Message	1
1.1.2	Creating Standard and Extensible IP Access List.....	1
1.1.3	Extensible Access List Example	2

Chapter 1 Configuring IP Access List

1.1 Configuring IP Access List

1.1.1 Filtering IP Message

Filtering message helps control the running of packets in the network. The control can constrain network transmission or limit network usage through user or device. To enable or disable packets on the crossly specified port, our routing switches provide the access list. The access list can be used through the following methods:

- Controlling packet transmission on the port
- Controlling the access of virtual terminal line
- Limiting routing update content

The section describes how to create the IP access list.

The IP access list is an orderly set IP of applying the allowed and forbidden conditions of IP address. The ROS software of our routing switches is to test the addresses in the access list one by one. The first match decides whether the software to accept or reject the address. Because the ROS software stops the match rules after the first match, the order of conditions is very important. If rule match does not exist, the address is to be rejected.

You need to perform the following steps before using the access list:

- (1) Create the IP access list by specifying the access list name and access conditions.
- (2) Apply the IP access list to the port.

1.1.2 Creating Standard and Extensible IP Access List

Use a character string to create an IP access list.

Note:

The standard IP access list and the extensible IP access list cannot use the same name.

Run the following commands in global configuration mode to create a standard IP access list:

Run...	To...
ip access-list standard <i>name</i>	Use name to define a standard IP access list.
deny { <i>source</i> [<i>source-mask</i>] any } or permit { <i>source</i> [<i>source-mask</i>] any }	Specify one or multiple permit/reject conditions in standard IP access list configuration mode, which decides whether the packet is approved or disapproved.
Exit	Log out from the IP access list configuration mode.

Run the following commands in global configuration mode to create an extensible IP access list:

Run...	To...
ip access-list extended <i>name</i>	Use a name to define an extensible IP access list.

{deny permit} protocol source source-mask src-port destination destination-mask dst-port [precedence precedence] [tos tos] {deny permit} protocol any any	Specify one or multiple deny or permit conditions in extensible access list configuration mode, which decides whether the IP packet is passed or not (precedence means the priority of the IP packet. TOS is the simplified form of Type of Service).
Exit	Log out of the access list configuration mode.

After the access list is originally created, any part added later (may be entered from the terminal) is put at the end of the list, that is, you cannot add the command line to the designated access list. However, you can run **no permit** and **no deny** to delete items from the name access list.

Note:

When you create the access list, remember that the end of the access list contains the invisible **deny** sentence. In another word, if the mask is not specified in relevant IP address access list, 255.255.255.255 is supposed to be the mask.

After the access list is created, refer to section “Applying the Access List to Port” to apply.

1.1.3 Extensible Access List Example

In the following case, the first command line allows the newly coming TCP to connect SMTP of host 130.2.1.2.

```
Switch(config)#ip access-list extended aaa
```

```
Switch(config-aaa)#permit tcp any 130.2.1.2 255.255.255.255 eq 25
```