Physical Port IP Access List Configuration

Table of Contents

Chapter 1 Configuring Physical Port-based IP Access List

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 and use 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.

1.2 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 *name*	Use name to define a standard IP access list.
deny {*source [source-mask]* | **any**} or **permit** {*source [source-mask]* | **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 *name*	Use a name to define an extensible IP access list.
{**deny | permit**} *protocol source source-mask destination destination-mask* [**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). If the protocol is TCP/UDP, a single port or port 14 in a certain range can be specified. For details, refer to "Extensible Access List Example".
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, it must be applied to the line or the port. Refer to section 1.3 "Applying the Access List to Port".

1.3 Applying the Access List to Port

After the access list is created, you can apply it to one or multiple ports or entries.

Run the following command in port configuration mode:

Run…	To…
ip access-group *name*	Apply the access list to the port.

For the standard entry access list, when the packet is received, the source address of the access list checking packet will be checked. For the extensible access list, the routing switch also checks the destination address. If the access list permits the destination address, the software continues to handle the packet. If the access list denies the destination address, the software drops the packet and returns a message that the ICMP host is unreachable.

If the designated access list does not exist, all packets are allowed to get through.

1.4 Extensible Access List Example

1.4.1 Port-Based IP Access List Supporting Filtration on TCP/UDP Ports

The example is shown as follows:

{**deny | permit**} {tcp | udp}

source source-mask [{ [src_portrange begin-port end-port] | [{gt | lt } port] }]

destination destination-mask [{ [dst_portrange begin-port end-port] | [{gt | lt } port] }]

[**precedence** *precedence*] [**tos** *tos*]

In this case, port l4 of TCP and UDP can be controlled through the access list. Pay attention to the following problems when you configure the access list by defining the port range:

(1) If the access list is configured at the source and destination by specifying the port range, some configuration may fail because lots of sources are occupied during configuration. To solve the problem, you are recommended to specify the port range at one side and the port at the other side.

(2) Using the port range filtration needs a lot of resources. The access list cannot provide strong support to other applications because the port range filtration is used too much.

1.4.2 Port-Based IP Access List Supporting Filtration of Port-Based IP Access List Supporting Filtration of TCP/UDP-Specified Ports

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

```
ip access-list extended aaa
permit tcp any 130.2.1.2 255.255.255.255 eq 25
interface   g0/10
ip access-group aaa
```