Chapter35: Network Protocol Configuration

Table of Contents

Chapter 1 Configuring IP Addressing

1.1 IP Introduction

1.1.1 IP

Internet Protocol (IP) is a protocol in the network to exchange data in the text form. IP has the functions such as addressing, fragmenting, regrouping and multiplexing. Other IP protocols (IP protocol cluster) are based on IP. As a protocol working on the network layer, IP contains addressing information and control information which are used for routing.

Transmission Control Protocol (TCP) is also based on IP. TCP is a connection-oriented protocol which regulates the format of the data and information in data transmission. TCP also gives the method to acknowledge data is successfully reached. TCP allows multiple applications in a system to communicate simultaneously because it can send received data to each of the applications respectively.

The IP addressing, such as Address Resolution Protocol, are to be described in section “Configuring IP Addressing.” IP services such as ICMP, HSRP, IP statistics and performance parameters are to be described in “Configuring IP Services.”

1.2 Configuring IP Address Task List

An essential and mandatory requirement for IP configuration is to configure the IP address on the network interface of the routing switch. Only in this case can the network interface be activated, and the IP address can communicate with other systems. At the same time, you need to confirm the IP network mask.

To configure the IP addressing, you need to finish the following tasks, among which the first task is mandatory and others are optional.

For creating IP addressing in the network, refer to section “IP Addressing Example.” IP address configuration task list:

- Configuring IP address at the network interface
- Configuring multiple IP addresses at the network interface
- Configuring Address Resolution
- Detecting and maintaining IP addressing

1.3 Configuring IP Address

1.3.1 Configuring IP Address at the Network Interface

The IP address determines the destination where the IP message is sent to. Some IP special addresses are reserved and they cannot be used as the host IP address or network address. Table 1 lists the range of IP addresses, reserved IP addresses and available IP addresses.

Type	Address or Range	Status

A	0.0.0.0 1.0.0.0 to 126.0.0.0 127.0.0.0	Reserved Available Reserved
B	128.0.0.0 to 191.254.0.0 191.255.0.0	Available Reserved
C	192.0.0.0 192.0.1.0 to 223.255.254.0 223.255.255.0	Reserved Available Reserved
D	224.0.0.0 to 239.255.255.255	Multicast address
E	240.0.0.0 to 255.255.255.254 255.255.255.255	Reserved Broadcast

The official description of the IP address is in RFC 1166 “Internet Digit”. You can contact the Internet service provider.

An interface has only one primary IP address. Run the following command in interface configuration mode to configure the primary IP address and network mask of the network interface:

Command	Purpose
ip address *ip-address mask*	Configure the main IP address of the interface.

The mask is a part of the IP address, representing the network.

Note:

Our OLT only supports masks which are continuously set from the highest byte according to the network character order.

1.3.2 Configuring Multiple IP Addresses at the Network Interface

Each interface can possess multiple IP addresses, including a primary IP address and multiple subordinate IP addresses. You need to configure the subordinate IP addresses in the following two cases:

If IP addresses in a network segment are insufficient. For example, there are only 254 available IP addresses in a certain logical subnet, however, 300 hosts are needed to connect the physical network. In this case, you can configure the subordinate IP address on the switch or the server, enabling two logical subnets to use the same physical subnet.

Most of early-stage networks which are based on the layer-2 bridge are not divided into multiple subnets. You can divide the early-stage network into multiple route-based subnets by correctly using the subordinate IP addresses. Through the configured subordinate IP addresses, the routing switch in the network can know multiple subnets that connect the same physical network.

If two subnets in one network are physically separated by another network In this case, you can take the address of the network as the subordinate IP address. Therefore, two subnets in a logical network that are physically separated, therefore, are logically connected together.

Note:

If you configure a subordinate IP address for a routing switch in a network segment, you need to do this for other routing switches in the same network segment.

Run the following command in interface configuration mode to configure multiple IP addresses on the network interface.

Command	Purpose
ip address *ip-address mask* **secondary**	Configure multiple IP addresses on the network interface.

Note:

When the IP routing protocol is used to send the route update information, subordinate IP addresses may be treated in different ways.

1.3.3 Configuring Address Resolution

IP can realize functions such as IP address resolution control. The following sections show how to configure address resolution:

1. Creating address resolution

An IP device may have two addresses: local address (local network segment or device uniquely identified by LAN) and network address (representing the network where the device is located). The local address is the address of the link layer because the local address is contained in the message header at the link layer, and is read and used by devices at the link layer. The professionals always call it as the MAC address. This is because the MAC sub layer in the link layer is used to process addresses.

For example, if you want your host to communicate with a device on Ethernet, you must know the 48-bit MAC address of the device or the local address of the link layer. The process on how to obtain the local address of the link layer from the IP address is called as Address Resolution Protocol (ARP). The process on how to obtain the IP address from the local address of the link layer is called as Reverse Address Resolution (RARP).

Our system adopts address resolution in two types: ARP and proxy ARP. The ARP and proxy ARP are defined in RFC 860 and 1027 respectively.

ARP is used to map IP addresses to media or MAC address. When the IP address is known, ARP will find the corresponding MAC address. When the MAC address is known, the mapping relationship between IP address and MAC address is saved in ARP cache for rapid access. The IP message is then packaged in the message at the link layer and at last is sent to the network.

- Defining a static ARP cache

  ARP and other address resolution protocols provide a dynamic mapping between IP address and MAC address. The static ARP cache item is generally not required because most hosts support dynamic address resolution. You can define it in global configuration mode if necessary. The system utilizes the static ARP cache item to translate the 32-bit IP address into a 48-bit MAC address. Additionally, you can specify the routing switch to respond to the ARP request for other hosts.

  You can set the active period for the ARP entries if you do not want the ARP entry to exist permanently. The following two types show how to configure the mapping between the static IP address and the MAC address.

Run one of the following commands in global configuration mode:

Command	Purpose
arp ip-address hardware-address vlan	Globally map an IP address to a MAC address in the ARP cache.
arp ip-address hardware-address vlan **alias**	Specify the routing switch to respond to the ARP request of the designated IP address through the MAC address of the routing switch.

Run the following command in interface configuration mode:

Command	Purpose
arp timeout *seconds*	Set the timeout time of the ARP cache item in the ARP cache.
arp dynamic	Enables arp dynamic learning in the interface

Run show interfaces to display the ARP timeout time of the designated interface. Run the show arp to check the content of the ARP cache. Run clear arp-cache to delete all entries in the ARP cache.

- Configuring free ARP function

  The switch can know whether the IP addresses of other devices collide with its IP address by sending free ARP message. The source IP address and the destination IP address contained by free ARP message are both the local address of the switch. The source MAC address of the message is the local MAC address.

  The switch processes free ARP message by default. When the switch receives free ARP message from a device and finds that the IP address contained in the message collide with its own IP address, it will return an ARP answer to the device, informing the device that the IP addresses collide with each other. At the same time, the switch will inform users by logs that IP addresses collide.

  The switch's function to send free ARP message is disabled by default. Run the following commands to configure the free ARP function on the port of the switch:

Command	Usage Guidelines
arp send-gratuitous	Start up free ARP message transmission on the interface.
arp send-gratuitous interval *value*	Set the interval for sending free ARP message on the interface. The default value is 120 seconds.

- To set the maximum retransmissions of the Re-Detect packets, run the following command.

  The ARP entries (to be tagged with G), which the routing entry gateway depends on, require being re-detected at their aging so that the promptness and correctness of the hardware subnet routing can be guaranteed. The greater the retransmission times, the more likely to re-detect.

Command	Usage Guidelines
arp max-gw-retries *number*	Sets the maximum retransmissions of the Re-Detect packets. The default is 3.

- Sets re-detection when ARP entry is aging.

  By default only ARP depends on routing entry has re-detection when aging. After enable this command, all ARP entries will adopt aging re-detection mechanism.

Command	Usage Guidelines
arp retry-allarp	Sets re-detection when the ARP entry is aging.

2. Mapping host name to IP addres

Any IP address can correspond to a host name. The system has saved a mapping (host name to address) cache which can be telneted or pinged.

To designate a mapping from host name to address, run the following commands in global mode:

Command	Purpose
ip host *name address*	Statically map the host name to the IP address.

1.3.4 Detecting and Maintaining IP Addressing

To detect and maintain the network, run the following command:

1. Clearing cache, list and database

Clearing cache, list and database You can clear all content in a cache, list or the database.

When you think some content is ineffective, you can clear it.

Run the following command in management mode to clear the cache, list and database:

Command	Purpose
clear arp-cache	Clear the IP ARP cache.

2. Displaying statistics data about system and network

The system can display designated statistics data, such as IP routing table, cache and database. All such information helps you know the usage of the systematic resources and solve network problems. The system also can display the reachability of the port and the routes that the message takes when the message runs in the network.

All relative operations are listed in the following table. For how to use these commands, refer to Chapter “IP Addressing Commands”. Run the following commands in management mode:

Command	Purpose
show arp	Display content in the ARP table.

show hosts	Display the cache table about hostname-to-IP mapping.
show ip interface [*type number*]	Displays the state of a port.
ping {**host	address**}	Test the reachability of the network node.

1.4 IP Addressing Example

The following case shows how to configure the IP address on interfaceVLAN11.

interface vlan 11 ip address

202.96.2.3 255.255.255.0

Chapter 2 Configuring DHCP

2.1 Overview

Dynamic Host Configuration Protocol (DHCP) is used to provide some network configuration parameters for the hosts on the Internet, which is described in details in RFC 2131. One of the major functions of DHCP is to distribute IPs on an interface. DHCP supports the following three IP distribution mechanism:

- Automatic distribution

  The DHCP server automatically distributes a permanent IP address to a client.

- Dynamic distribution

  The DHCP server distributes an IP address for a client to use for a certain period of time or until the client does not use it.

- Manual distribution

  The administrator of the DHCP server manually specifies an IP address and through the DHCP protocol sends it to the client.

2.1.1 DHCP Application

DHCP can be applied at the following cases: You can distribute IP address, network segment and related sources (such as relevant gateway) to an Ethernet interface by configuring the DHCP client.

- When an OLT that can access DHCP connects multiple hosts, the OLT can obtain an IP address
- From the DHCP server through the DHCP relay and then distribute the address to the hosts.

2.1.2 Advantages of DHCP

In current software version, the DHCP client or the DHCP client on the Ethernet interface is supported. DHCP has the following strong points:

- Fastening the settings;
- Reducing configuration errors;
- Controlling IP addresses of some device ports through the DHCP server

2.1.3 DHCP Terms

DHCP is based on the server/client mode. So the DHCP server and the DHCP client must exist at the same time:

- DHCP-Server

  It is a device to distribute and recycle the DHCP-related sources such as IP addresses and lease time.

- DHCP-Client

  It is a device to obtain information from the DHCP server for devices of the local system to use, such as IP address information.

In a word, there exists lease time during the process of dynamic DHCP distribution:

- Lease time – it means the effective period of an IP, which starts from the distribution. After the lease time, the DHCP server withdraws the IP. To continue to use this IP, the DHCP client needs to apply it again.

2.2 Configuring DHCP Client

2.2.1 Configuration Task List of DHCP Client

- Obtaining an IP address
- Specifying an address for DHCP server
- Configuring DHCP parameters ● Monitoring DHCP

2.2.2 DHCP Client Configuration Tasks

1. Obtaining an IP address

Run the following command on the VLAN interface to obtain an IP address through the DHCP protocol for an interface.

Command	Function
ip address dhcp	Sets the IP address of an Ethernet interface through DHCP.

2. Specifying an address for DHCP server

If knowing the addresses of some DHCP servers, you can specify these servers' addresses on switch so as to reduce the time of protocol processing. You can run the following command in global mode:

Command	Function
ip dhcp-server *ip-address*	Specifies the IP address of the DHCP server.

The command is optional when you perform operations to "obtain an IP address".

3. Configuring DHCP parameters

To adjust the parameters of DHCP communication according to actual requirements, run the following commands in global mode:

Command	Function
ip dhcp client minlease *seconds*	Specifies the acceptable minimum lease time.

ip dhcp client retransmit *count*	Specifies the retransmission times for DHCP packet.
ip dhcp client select *seconds*	Specify the interval for SELECT.
ip dhcp client class_identifier *WORD*	Specify the classification code of the provider.
ip dhcp client client_identifier hrd_ether	Specify the client ID as the Ethernet type
ip dhcp client timeout_shut	Specify client timeout shutdown of the interface

The command is optional when you perform operations to "obtain an IP address".

4. Monitoring DHCP

To browse related information of the DHCP server, which is discovered by the switch currently, run the following command in EXEC mode:

Command	Function
show dhcp server	Displays related information about the DHCP server, which is known by the switch.

To browse which IP address is currently used by the switch, run the following command in EXEC mode:

Command	Function
show dhcp lease	Displays IP resources, which are currently used by the switch, and related information.

Additionally, if you use DHCP to distribute an IP for an Ethernet interface, you can also run show interface to browse whether the IP address required by the Ethernet interface is successfully acquired.

2.2.3 DHCP Client Configuration Example

DHCP Client configuration example is shown below:

1. Obtaining an IP address

The following example shows interface vlan11 obtains an IP address through DHCP.

```
!
interface vlan 11
ip address dhcp
```

Chapter 3 IP Service Configuration

The section is to describe how to configure optional IP service. For the details of the IP service commands, refer to section “IP Service Commands”.

3.1 Configuring IP Service

Optional IP service configuration tasks are listed as follows:

- Managing IP connection
- Configuring performance parameters
- Detecting and Maintaining IP Network

The above operations are not mandatory. You can perform the operations according to your requirements.

3.1.1 Managing IP Connection

The IP protocol provides a series of services to control and manage IP connections. Most of these services are provided by ICMP. The ICMP message is sent to the host or other routing switches when the routing switch or the access server detects faults in the IP message header. ICMP is mainly defined in RFC 792.

Perform the following different operations according to different IP connection conditions:

1. Sending ICMP unreachable message

If the system receives a message and cannot send it to the destination, such as no routes, the system will send an ICMP-unreachable message to the source host. The function of the system is enabled by default.

If the function is disabled, you can run the following command in interface configuration mode to enable the function.

Command	Purpose
ip unreachables	Enable the function to send an ICMP-unreachable message.

2. Sending ICMP redirection message

Sometimes the host selects an unfavorable route. After a routing switch on the route receives a message from the host, it is to check the routing table and then forward the message through the message-receiving interface to another routing switch that is in the same network segment as the host. In this case, the routing switch notifies the source host of directly sending the message with the destination to another routing switch without winding itself. The redirection message requires the source host to discard the original route and take more direct route suggested in the message. Many host’s operating system adds a host route to its routing table. However, the routing switch is more willing to trust information obtained through the routing protocol. Therefore, the routing switch would not add the host route according to the information.

The function is enabled by default. If the hot standby routing switch protocol is configured on the interface, the function is automatically disabled. However, the function will not be automatically enabled even if the hot standby routing switch protocol is canceled.

To enable the function, run the following command in interface configuration mode:

Command	Purpose
ip redirects	Permit sending the ICMP redirection messafge.

3. Sending ICMP mask response message

Sometimes the host must know the network mask. To get the information, the host can send the ICMP mask request message. If the routing switch can confirm the mask of the host, it will respond with the ICMP mask response message. By default, the routing switch can send the ICMP mask response message.

To send the ICMP mask request message, run the following command in interface configuration mode:

Command	Purpose
ip mask-reply	Send the ICMP mask reply message.

4. Supporting route MTU detection

The system supports the IP route MTU detection mechanism defined by RFC 1191. The IP route MTU detection mechanism enables the host to dynamically find and adjust to the maximum transmission unit (MTU) of different routes. Sometimes the routing switch detects that the received IP message length is larger than the MTU set on the message forwarding interface. The IP message needs to be segmented, but the “unsegmented” bit of the IP message is reset. The message, therefore, cannot be segmented. The message has to be dropped. In this case, the routing switch sends the ICMP message to notify the source host of the reason of failed forwarding, and the MTU on the forwarding interface. The source host then reduces the length of the message sent to the destination to adjust to the minimum MTU of the route.

If a link in the route is disconnected, the message is to take other routes. Its minimum MTU may be different from the original route. The routing switch then notifies the source host of the MTU of the new route. The IP message should be packaged with the minimum MTU of the route as much as possible. In this way, the segmentation is avoided and fewer message is sent, improving the communication efficiency.

Relevant hosts must support the IP route MTU detection. They then can adjust the length of IP message according to the MTU value notified by the routing switch, preventing segmentation during the forwarding process.

5. Setting IP maximum transmission unit (MTU)

All interfaces have a default IP maximum transmission unit (MTU), that is, the transmissible maximum IP message length. If the IP message length exceeds MTU, the routing switch segments the message.

Changing the MTU value of the interface is to affect the IP MTU value. If IP MTU equals to MTU, IP MTU will automatically adjust itself to be the same as new MTU as MTU changes. The change of IP MTU, however, does not affect MTU. IP MTU cannot be bigger than MTU configured on the current interface. Only when all devices connecting the same physical media

must have the same MTU protocol can normal communication be created. To set IP MTU on special interface, run the following command in interface configuration mode:

Command	Purpose
ip mtu *bytes*	Set IP MTU of the interface.

6. Authorizing IP source route

The routing switch checks the IP header of every message. The routing switch supports the IP header options defined by RFC 791: strict source route, relax source route, record route and time stamp. If the OLT detects that an option is incorrectly selected, it will send message about the ICMP parameter problem to the source host and drop the message. If problems occur in the source route, the routing OLT will send ICMP unreachable message (source route fails) to the source host.

IP permits the source host to specify the route of the IP network for the message. The specified route is called as the source route. You can specify it by selecting the source route in the IP header option. The routing switch has to forward the IP message according to the option, or drop the message according to security requirements. The routing switch then sends ICMP unreachable message to the source host. The routing switch supports the source route by default.

If the IP source route is disabled, run the following command in global configuration mode to authorize the IP source route:

Command	Usage Guidelines
ip source-route	Authorizing IP source route.

3.1.2 Configuring Performance Parameters

Run the following command to adjust IP performance.

1. Setting the Wait Time for TCP Connection

When the routing switch performs TCP connection, it considers that the TCP connection fails if the TCP connection is not created during the wait time. The routing switch then notifies the upper-level program of the failed TCP connection. You can set the wait time for TCP connection. The default value of the system is 75 seconds. The previous configuration has no impact on TCP connections that the switch forwards. It only affects TCP connections that are created by the switch itself.

Run the following command in global configuration mode to set the wait time for TCP connections:

Command	Purpose
ip tcp synwait-time *seconds*	Set the wait time for TCP connection.

2. Setting the Size of TCP Windows

The default size of TCP windows is 2000 byte. Run the following command in global configuration mode to change the default window size:

Command	Purpose
ip tcp window-size *bytes*	Set the size of TCP windows.

3.1.3 Detecting and Maintaining IP Network

To detect and maintain the network, run the following command:

1. Clearing Cache, List and Database

You can clear all content in a cache, list or database. All incorrect data in a cache, list or database need be cleared.

Run the following command to clear incorrect data:

Command	Purpose
clear tcp statistics	To clear the statistics data about TCP, run the following command:

2. Clearing TCP Connection

To disconnect a TCP connection, run the following command:

Command	Purpose
clear tcp {**local** host-name port **remote** host-name port | **tcb** address}	Clear the designated TCP connection. TCB refers to TCP control block.

3. Displaying statistics data about system and network

The system can display the content in the cache, list and database. These statistics data can help you know the usage of systematic sources and solve network problems.

Run the following commands in EXEC mode. For details, refer to “IP Service Command”.

Command	Purpose
show ip access-lists *name*	Display the content of one or all access lists.
show ip sockets	Display all socket information about the routing switch.
show ip traffic	Show IP protocol statistics data
show tcp	Show all TCP connection status information
show tcp brief	Briefly display information about TCP connection states.
show tcp statistics	Display the statistics data about TCP
show tcp tcb	Display information about the designated TCP connection state.

4. Displaying debugging information

When problem occurs on the network, you can run debug to display the debugging information.

Run the following command in EXEC mode. For details, refer to “IP Service Command”.

Command	Purpose
debug arp	Display the interaction information about ARP.

debug ip icmp	Display the interaction information about ICMP.
debug ip raw	Display the information about received/transmitted Internet IP message.
debug ip packet	To display the information about IP interaction, run debug ip raw.
debug ip tcp	Display the interaction information about TCP.
debug ip udp	Display the interaction information about UDP.

3.2 Configuring Access List

3.2.1 Filtering IP Packet

Filtering message helps control the movement of packet in the network. The control can limit network transmission and network usage through a certain user or device. To make packets valid or invalid through the crossly designated interface, our routing switch provides the access list. The access list can be used in the following modes:

Controlling packet transmission on the interface

Controlling virtual terminal line access

Limiting route update content

The section describes how to create IP access lists and how to use them.

The IP access list is an orderly set of the permit/forbid conditions for applying IP addresses. The ROS software of our switch tests the address one by one in the access list according to regulations. The first match determines whether the ROS accepts or declines the address. After the first match, the ROS software terminates the match regulations. The order of the conditions is, therefore, important. If no regulations match, the address is declined.

Use the access list by following steps:

(1) Create the access list by designating the access list name and conditions.

(2) Apply the access list to the interface.

3.2.2 Creating Standard and Extensible IP Access List

Use a character string to create an IP access list.

Note:

The standard access list and the extensible access list cannot have the same name.

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

Command	Purpose
ip access-list standard *name*	Use a name to define a standard access list.

deny {*source [source-mask]* | **any**}[**log | location**] or **permit** {*source [source-mask]* | **any**}[**log | location**]	Designate one or multiple permit/deny conditions in standard access list configuration mode. The previous setting decides whether the packet is approved or disapproved.
Exit	Log out from the access list configuration mode.

Run the following command in global configuration mode to create an extensible access list.

Command	Purpose
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*] [**log**][**time-range** time-range] [**location** location] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**totallen eq|gt|lt** lentgh] [**ttl eq|gt|lt** time] [**offset-not-zero**] [**offset-zero**] {**deny | permit**} *protocol* **any any** [**precedence** *precedence*] [**tos** *tos*] [**log**][**time-range** time-range] [**location** location] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**totallen eq|gt|lt** lentgh] [**ttl eq|gt|lt** time] [**offset-not-zero**] [**offset-zero**]	Designate one or multiple permit/deny conditions in extensible access list configuration mode. The previous setting decides whether the packet is approved or disapproved. precedence means the priority of the IP packet; TOS means Type of Service.
Exit	Log out from the access list configuration mode.

After the access list is originally created, any part that is added later can be put at the end of the list. That is to say, 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 access list.

Note:

When you create the access list, the end of the access list includes the implicit deny sentence by default. If the mask is omitted in the relative IP host address access list, 255.255.255.255 is supposed to be the mask.

After the access list is created, the access list must be applied on the route or interface. For details, refer to section 4.2.3 “Applying the Access List to the Interface”.

3.2.3 Applying the Access List to the Interface

After the access list is created, you can apply it to one or multiple interfaces including the in interfaces and out interfaces.

Run the following command in interface configuration mode.

Command	Purpose
ip access-group *name* **{in | out}**	Apply the access list to the interface.

The access control list can be used on the incoming or outgoing interface. After a packet is received, the source address of the packet will be checked according to the standard egress

interface access control list. For the expanded access control list, the routing switch also checks the destination address. If the access control list permits the destination address, the system will continue handling the packet. However, if the access control list forbids the destination address, the system will drop the packet and then returns an ICMP unreachable packet.

For the standard access list of the out interfaces, after a packet is received or routed to the control interface, the software checks the source address of the packet according to the access list. For the extensible access list, the routing switch also checks the access list of the receiving side. If the access list permits the address, the software will send the packet. If the access list does not permit the address, the software drops the packet and returns an ICMP unreachable message.

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

3.2.4 Extensible Access List Example

In the following example, the first line allows any new TCP to connect the destination port after port 1023. The second line allows any new TCP to connect the SMTP port of host

130.2.1.2. ip access-list extended aaa permit

tcp any 130.2.0.0 255.255.0.0 gt 1023 permit

tcp any 130.2.1.2 255.255.255.255 eq 25

interface vlan 10 ip access-group aaa in

Another example to apply the extensible access list is given. Suppose a network connects the Internet, you expect any host in the Ethernet can create TCP connection with the host in the Internet. However, you expect the host in the Internet cannot create TCP connection with the host in the Ethernet unless it connects the SMTP port of the mail host.

SMTP connects with TCP port in one end and the arbituary port number in the other end. During the connection period, the same two port numbers are used. The mail packet from the Internet has a destination port, that is, port 25. The outgoing packet has a contrary port number. In fact, the security system behind the routing switch always receives mails from port 25. That is the exact reason why the incoming service and the outgoing service can be uniquely controlled. The access list can be configured as the outgoing service or the incoming service.

In the following example, the Ethernet is a B-type network with the address 130.20.0.0. The address of the mail host is 130.20.1.2. The keyword established is only used for the TCP protocol, meaning a connection is created. If TCP data has the ACK or RST digit to be set, the match occurs, meaning that the packet belongs to an existing connection.

ip access-list aaa permit tcp any 130.20.0.0

255.255.0.0 established permit tcp any 130.20.1.2

255.255.255.255 eq 25 interface vlan 10 ip

access-group aaa in

3.3 Configuring IP Access List Based on Physical Port

3.3.1 Filtering IP Packet

Filtering message helps control the movement of packet in the network. The control can limit network transmission and network usage through a certain user or device. To make packets valid or invalid through the crossly designated interface, our routing switch provides the access list. The access list can be used in the following modes:

Controlling packet transmission on the interface

Controlling virtual terminal line access

Limiting route update content

The section describes how to create IP access lists and how to use them.

The IP access list is an orderly set of the permit/forbid conditions for applying IP addresses. The ROS software of our switch tests the address one by one in the access list according to regulations. The first match determines whether the ROS accepts or declines the address. After the first match, the ROS software terminates the match regulations. The order of the conditions is, therefore, important. If no regulations match, the address is declined.

Use the access list by following steps:

(1) Create the access list by designating the access list name and conditions.

(2) Applying ACL on a port

3.3.2 Creating Standard and Extensible IP Access List

Use a character string to create an IP access list.

Note:

The standard access list and the extensible access list cannot have the same name.

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

Command	Purpose
ip access-list standard *name*	Use a name to define a standard access list.
deny {*source [source-mask]* | **any**} [**log | location**] or **permit** {*source [source-mask]* | **any**} [**log | location**]	Designate one or multiple permit/deny conditions in standard access list configuration mode. The previous setting decides whether the packet is approved or disapproved.
Exit	Log out from the access list configuration mode.

Run the following command in global configuration mode to create an extensible access list.

Command	Purpose
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*] [**log**] [**time-range** time-range] [**location** location] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**totallen eq|gt|lt** lentgh] [**ttl eq|gt|lt** time] [**offset-not-zero**] [**offset-zero**] {**deny | permit**} *protocol* **any any** [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** time-range] [**location** location] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**totallen eq|gt|lt** lentgh] [**ttl eq|gt|lt** time] [**offset-not-zero**] [**offset-zero**]	Designate one or multiple permit/deny conditions in extensible access list configuration mode. The previous setting decides whether the packet is approved or disapproved. precedence means the priority of the IP packet; TOS means Type of Service. If protocol is TCP/UDP, designate a single or 14 port number in a certain range. For more details, refer to Access List Configuration Example.
Exit	Log out from the access list configuration mode.

After the access list is originally created, any part that is added later can be put at the end of the list. That is to say, 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 access list.

Note:

When you create the access list, the end of the access list includes the implicit deny sentence by default. If the mask is omitted in the relative IP host address access list, 255.255.255.255 is supposed to be the mask.

After ACL is established, it must be applied on the lines or ports. For details, refer to section “Applying the Access List to the Interface”.

3.3.3 Applying ACL on Ports

After an ACL is established, it can be applied on the ingress of one or many interfaces. Run the following command to apply IPv6 ACL on a port:

Command	Purpose
ip access-group *name*	Applying ACL on a port

After a packet is received, the source address of the packet will be checked according to the standard egress interface access control list. For the expanded access control list, the routing switch also checks the destination address. If the access control list permits the destination address, the system will continue handling the packet. However, if the access control list forbids the destination address, the system will drop the packet and then returns an ICMP unreachable packet.

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

3.3.4 Extensible Access List Example

1. Port-based IP access list supporting TCP/UDP port filtration

The format is 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*]

If you configure the access list by defining the port range, pay attention to the following:

(1) If you use the method of designating the port range to configure the access list at the source side and the destination side, some configuration may fail because of massive resource consumption. In this case, you need to use the fashion of designating the port range at one side, and use the fashion of designating the port at another side.

(2) When the port range filtration is performed, too many resources will be occupied. If the port range filtration is used too much, the access list cannot support other programs as well as before.

2. Port-based IP access list supporting TCP/UDP designated port filtration

In the following example, the first line allows any new TCP to connect the SMTP port 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 g0/1 ip access-group aaa