Network Protocol Configuration

Table of Contents

Chapter 1 Configuring IP Addressing

1.1 IP Introduction

1.1.1 IP

Internet P (rotocol p iIP) n s t erotocol d i n the f etwork t o xchan 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 connect protocol w r hich t f egulates d a hie ormat d t f he Tata a nd nforma gives the method to acknowledge data is successfully reached applications i a s tnc ystem s o ommunicatec s r imultaneously each of the applications respectively.

The IP addressing, such as Address Resolution Protocol, are to be described i "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 e ssential m nd andatory c equirement t I aor Po onfiguration the network interface of the routing switch. Only in this case can the network interface b 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 I a P ddress t determinesw t I hne estinsation S I s here he P addresses a r rea t esecrved b u andt h heyI a annot n ea sed s he 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 configuration mode to configure the primary IP address and network mask of the netwo 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 I multiple s ubordinate Y n P t addressest s oul a eed i to onfigure following two cases:

If IP addresses in a network segment are insufficient. For example, there a available IP addresses in a certain logical subnet, however, the physical network. In this case, you can configure the 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 divi multiple subnets. You can divide the early-stage network correctly using the subordinate IP addresses. Through the co addresses, the routing switch in the network can know multiple subnets that conn 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. Thus the subordinate a logical network that are physically separated, therefore, are logically connected together.

Note:

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

Run the following command in interface configuration mode addresses on the network interface.

Command	Purpose
ip address *ip-address mask* **secondary**	Configure multiple IP addresses on the 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 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 of the link layer, and 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 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 Addre Resolution Protocol (ARP). The process on how to obtain the IP address from address of the link layer is called as Reverse Address Resolution (RARP).

Our s ystaem a doptps i dtdress A aesolption A T An awo p ypes: RP 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 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 mapp between IP address and MAC address. The static ARP cach generally not required because most hosts support 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 4 M8-bita AAC ddyessc s tdditionally, s t ou an respond to the ARP request for other hosts.

  You c sant a et p he f tctivAe e eriody d norw hte A RP ntries 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 M address in the ARP cache.
a r ip p-address ha **alias**	Specify the routing switch to respond to the an ARP request of the designated IP address through the MAC address of the rou switch.

  Run the following command in interface configuration mode:

Command	Purpose
arp timeout *seconds*	Set t the timeoutt A time i fi he RP ac the ARP cache.
arp dynamic	Enables arp dynamic learning in the interface

  Run show interfaces to display the ARP timeout time of the desig 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 s wicth k w an t nolwa hetheor d he c P w ddresses its I aP ddbress f yA mending T s ree I aRP a etssage.

destination IP address contained by free ARP message are both the local address of the switch. The source MAC address is the MAC address.

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

The switch's function to send free ARP message the following commands to configure the free ARP 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 of sending free ARP on the interface. The default value is 120 seconds.

- To set the maximum retransmissions of the Re-Detect packets, following command.
  The ARP entries (to be tagged with G), which the routing entry gatewa depends on, require being re-detected at their and correctness of the hardware subnet routing can be guaranteed. T 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-detec mechanism.

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

2. Mapping host name to IP addres

Any IP address can correspond to a host name. The system has saved a mapping (h

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
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
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 comman
mode:

Command	Purpose
show arp	Display content in the ARP table.
show hosts	Display the cache table about 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

1.5 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 m afjor ounDctionsi t d f I HCPa i s oD isstribute t f Ps n n nt three IP distribution mechanism:

- Automatic distribution

  The DHCP server automatically distributes a permanent IP address to 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 a dministraotdr D s fm he s HCP a I ærver a anually through the DHCP protocol sends it to the client.

1.5.1 DHCP Application

DHCP c b aan aet f pplied c Yt dhe d ollowinhg a n ases: s ou an is 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 distribut address to the hosts.

1.5.2 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

1.5.3 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 th continue to use this IP, the DHCP client needs to apply it again.

1.6 Configuring DHCP Client

1.6.1 Configuration Task List of DHCP Client

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

1.6.2 DHCP Client Configuration Tasks

1. Obtaining an IP address

Run t f he cdllowing o t Vommiand t o n a lhea LAtN tnteDrface o bt protocol for an interface.

Command	Function
ip address dhcp	Sets t I hae P o adEress i f n thernet nte through DHCP.

2. Specifying an address for DHCP server

If knowing the addresses of some DHCP servers, you can specify these servers’ addresses on s witsh a t r o t s t o o peduce p he Y imce r f f rotocol c rocessing. 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 t r he etransmission D imes or packet.
ip dhcp client select *seconds*	Specify the interval for SELECT.
ip dhcp client class_identifier *WORD*	Specify the classification code 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 t 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 discover currently, run the following command in EXEC mode:

Command	Function
show dhcp server	Displays related information ab 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 Ethern successfully acquired.

1.6.3 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
service commands, refer to section “IP Service Commands”.

1.7 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.

1.7.1 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 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 t hf e unictidon y sc isabled, f cou ani un c he ollowing omma to enable the function.

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

2. Sending ICMP redirection message

Sometimes t h s he a uost elects A a rn nsfavorable t r r oute. fter a message from the host, it is to check the routing table and then forward the me through t m he essage-receiving a r s nterface i t s o n nother outing segment as the host. In this case, the routing switch notifies the source host sending t m he w essage t aith r he s estination w i o Tnother outi redirection message requires the source host to discard the original route and take direct r soute i tuggesnted M hm hoe essage. a a h any t i ost's perat routing t H able. t r owevesr, i m hew otuting i witcho st ore illing 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 automatically enabled even if the h canceled.

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

Command	Purpose
ip redirects	Permit sending the ICMP 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 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 ad 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 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 r edtuces o t hem engths t t f d he tessage t t m ent M o he estina of the route.

If a link in the route is disconnected, the message is to take other routes. Its minimum MTU may b d e fifferetnt o rrom T he sriginalt n oute. s heh o otuting witch 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 ro 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 sw 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 media must have the same MTU protoc created.
To set IP MTU on special interface, run the following command in interface config 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 d befRed 7 s ys FCr r 91: s trict r ource a toutes, I elax ource OLT detects that an option is incorrectly selected, it will send message about the ICMP para 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 p ermits s the t source t r ost t Io n pecify t m he Toutes f r hei P etwork called as the source route. You can specify it by selecting the source route in the IP header option. The routing s h witch f t as I mo orward t t he Po d essagem a ccordingt o he 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.

1.7.2 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 wa connection. T d vhe o t efsault i 7 aslue T f p he cystem h s n 5 econds. 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 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 com configuration mode to change the default window size:

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

1.7.3 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 database need be cleared.

Run the following command to clear incorrect data:

Command	Purpose
clear tcp statistics	To c letar s he d tatistics T r t atfa bout CP, u 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 s ystem d t anc isplay c he a ontent T n s he d ache, ist nd 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 d iisplay a nformation bout CP 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 disp 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/t Internet IP message.
debug ip packet	To display the information about IP interaction, ru debug ip raw.
debug ip tcp	Display the interaction information about TCP.
debug ip udp	Display the interaction information about UDP.

1.8 Configuring Access List

1.8.1 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 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.

1.8.2 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 p conditions in stand configuration mode. The previous se 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 a named extensible IP list.
{**deny** | **permit**} *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range*] [**location** *location*] [**donotfragment-set** | **notfragment**] [**totallen eq|gt|lt** *length*] [**ttl eq|gt|lt** *ttl*] [**offset-not-zero**] [**offset-zero**] {**deny** | **permit**} *protocol* **any any** [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range*] [**location** *location*] [**donotfragment-set** | **notfragment**] [**totallen eq|gt|lt** *length*] [**ttl eq|gt|lt** *ttl*] [**offset-not-zero**] [**offset-zero**]	Designate one or multiple permit conditions in extensible 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 acc 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 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”.

1.8.3 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 switc 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 lis
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 accordi
access l F tst. e or a he l xtensible s access t ist, lhe o t outing wit
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.

1.8.4 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 o
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 e txample t e o apply l i hge Sxtensible a n c ccess t ist s i
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 t c he ponnection s t p eriod, a he Tamem p wo f tort umbers
Internet has a destination port, that is, port 25. The outgoing packet has a cont
number. In fact, the security system behind the routing switch always receives mails fr
port 25. That is the exact reason why the incoming service and the outgoing service can be
uniquely c oTntrolled. l c bhe ccess t o ist s an o te i onfigured s
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 TC
protocol, m a eaning i c oInTection h t As oreRated t b s tCP ata
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
```

1.9 Configuring IP Access List Based on Physical Port

1.9.1 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 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

1.9.2 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 p conditions in stand configuration mode. The previous se 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 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**] [**not-fragment** | **first-fragment** | **non-first-fragment**] [**totallen** **eq|gt|lt** length] [**ttl** **eq|gt|lt** ttl] [**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**] [**not-fragment** | **first-fragment** | **non-first-fragment**] [**totallen** **eq|gt|lt** length] [**ttl** **eq|gt|lt** ttl] [**offset-not-zero**] [**offset-zero**]	Designate one or multiple p conditions in extensi configuration mode. The previous se decides whether the packet is approved or disapproved. precedence means the priority of the IP packet; TOS means type of If protocol is TCP/UDP, designate a single or 14 port number in a certain range. For more details, refer to Access List Configuratio 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 acc 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 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".

1.9.3 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 access control list of the ingress interface. For the expa 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 cont 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.

1.9.4 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) I y f u out m se o de ethod p r f t esignating a l he ort a at the source side and the destination side, some configuration ma because o m fr assive esource c y onsumption.t n 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 res 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
```