Contents

1 Configuring IPv4 Basics

1.1 Introduction

1.1.1 Overview

Internet Protocol (IP) is one of the most core protocols in the Transmission Control Protocol (TCP)/IP protocol suite and works at the network layer. Each IP device in the network needs a logical virtual address, which is used by the IP protocol to realize communication between devices. This address is usually called IP address.

The Internet Protocol version 4 (IPv4) is the fourth revision of the Internet Protocol, and is also the first version that has been widely used. The Internet Protocol version 6 (IPv6), the successor of IPv4, is still in its early stage of deployment in 2011 when IPv4 addresses were about to be used up. IPv4 uses the 32-bit address format, so there are only 4,294,967,296 addresses in the address space, some of which are reserved for special purposes.

Note

The following description is for IPv4 only, and IP addresses mentioned in this document refer to IPv4 addresses.

1.1.2 Basic Concepts

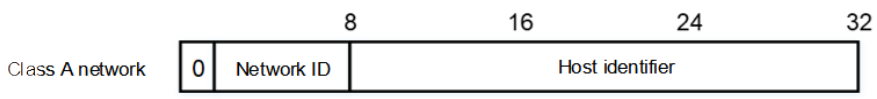
1. Classification of IP Addresses

IP addresses are used for interconnection at the IP layer. An IP address consists of 32 bits in binary. To facilitate writing and description, an IP address is generally expressed in decimal notation. When expressed in decimal notation, an IP address is divided into four groups, with eight bits in each group. The value range of each group is from 0 to 255, and groups are separated by dots (.), which are called dotted decimal notation. For example, "192.168.1.1" is an IP address expressed in decimal notation.

A 32-bit IP address consists of two parts: network ID and local address. A network ID indicates a network identifier, and a local address identifies a host. Based on the values of the first several bits in the network part, IP addresses in use can be classified into four classes.

- For a class A address, the most significant bit is "0", the following 7 bits indicate a network ID, and the last 24 bits indicate a local address (host identifier). There are 2^7 = 128 class A networks in total.

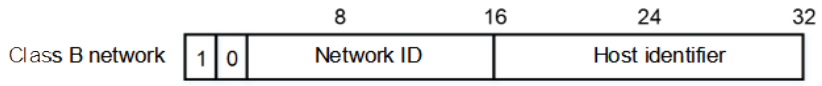
Figure 1-1Class A Network



- For a class B address, the two most significant bits are "10", the following 14 bits indicate a network ID (network identifier), and the last 16 bits indicate a local address (host identifier). There are 2^{14}=16,384 class

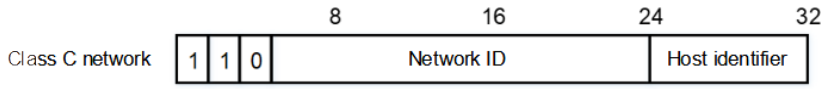
B networks in total.

Figure 1-2Class B Network



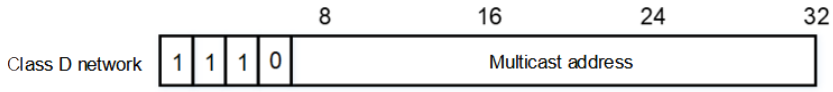
- For a class C address, the three most significant bits are "110", and the following 21 bits indicate a network ID, and the last 8 bits indicate a local address. There are 2^{21}=2,097,152 class C networks in total.

Figure 1-3Class C Network



- For a class D address, the four most significant bits are "1110" and other bits are designated for multicast addresses.

Figure 1-4Class D Network



Note

The addresses with the four most significant bits of "1111" cannot be assigned. These addresses are called class E addresses and are reserved for experimental use.

IP addresses must be assigned according to the nature of the network during IP address planning in the process of network construction. If the network needs to be connected to the Internet, users need to apply to relevant organizations for IP addresses. If the network is built to be an internal private network, users do not need to apply for IP addresses and can be assigned dedicated private network addresses.

Table 1-1Reserved and Available Addresses

Class	Address Range	Status
Class A network	0.0.0.0~0.255.255.255	Reserved
	1.0.0.0~126.255.255.255	Available
	127.0.0.0~127.255.255.255	Reserved
Class B network	128.0.0.0~191.254.255.255	Available
	191.255.0.0~191.255.255.255	Reserved

Class	Address Range	Status
Class C network	192.0.0.0~192.0.0.255	Reserved
	192.0.1.0~223.255.254.255	Available
	223.255.255.0~223.255.255.255	Reserved
Class D network	224.0.0.0~239.255.255.255	Multicast addresses
Class E network	240.0.0.0~255.255.255.254	Reserved
	255.255.255.255	Broadcast addresses

2. Private Network IP Addresses

Private network IP addresses are not used in the Internet. If the devices to which private addresses are assigned need to be connected to the Internet, these IP addresses need to be converted into valid Internet addresses. Table 1-1 lists private network address ranges. Private network addresses are defined in RFC1918 and include three address blocks.

Table 1-1Private Network Addresses

Class	Address Range	Status
Class A network	10.0.0.0–10.255.255.255	One class A network
Class B network	172.16.0.0–172.31.255.255	16 class B networks
Class C network	192.168.0.0–192.168.255.255	256 class C networks

For assignment of IP addresses, TCP/User Datagram Protocol (UDP) ports, and other codes, refer to RFC1166.

3. Special IP Addresses

The IP addresses listed below are used for special purposes and cannot be used as host IP addresses.

- Addresses with the network ID of all zeros: Indicates the host in the network. For example, 0.0.0.16 indicates the host numbered 16 in the network.
- Addresses with the host ID of all zeros: Indicates a network address, used for identifying a network, for example, 192.168.1.0.
- Addresses with the host ID of all ones: Indicates a broadcast address of the network. For example, the packets with the destination address of 192.168.1.255 will be forwarded to all hosts in the 192.168.1.0 network.

4. Network Mask

A network mask is also a 32-bit value and identifies the bits occupied by the network part of an IP address. In a network mask, the IP address bits corresponding to the bits whose values are ones are the network part, and the IP address bits corresponding to the bits whose values are zeros are the host address. For example, for class A networks, the network mask is 255.0.0.0. Network masks can be used to divide a network into several

subnets. Some bits of the host address are used as the network ID to decrease the host capacity and increase the number of networks. In this case, network masks are called subnet masks.

5. MTU

Maximum transmission unit (MTU) is the maximum size, usually in bytes, of the data transmitted by the data link layer to its upper layer, such as the IP and Multiprotocol Label Switching (MPLS). The MTU is protocol-specific, for example:

- The MTU for IEEE802.3/802.2 is 1,492 bytes.
- The MTU range of an Ethernet port is 64 to 1,518 bytes. Ethernet frames beyond this range may be dropped.

The IP protocol decides whether to fragment data based on the Layer 2 MTU value. Routes between the two devices may go through many hops, and the smallest MTU determines the transmission rate.

6. TTL

Time to live (TTL) refers to the number of network segments, through which packets are allowed to pass before the packets are discarded. The TTL value is used to judge whether packets stay on the network for a long time and should be discarded.

An IP packet is transmitted from the source address to the destination address through routers. A TTL value is set at the source end and decreases by 1 each time the IP packet passes through a router. When the TTL value drops to zero, the router deems the destination unreachable and discards the packet. TTL prevents infinite transmission of useless packets and bandwidth waste.

1.1.3 Principles

1. Obtaining IP Addresses

A device must have an IP address before sending and receiving IP datagrams. Only the interface configured with an IP address can run the IP protocol.

An interface can obtain IP addresses in the following four ways. These ways are mutually exclusive. If you configure a new way to obtain an IP address, the old IP address will be overwritten.

(1) Manually configuring IP addresses

(2) Obtaining IP addresses through the Dynamic Host Configuration Protocol (DHCP): For details about the DHCP protocol, see "Configuring DHCP" in the *IP Configuration Guide*.

(3) Obtaining IP addresses through the Point-to-Point Protocol (PPP) negotiation: A point-to-point interface accepts the IP address assigned by the peer through PPP negotiation. During PPP negotiation, the server checks authentication information of the client. If the client passes the authentication, the server assigns an IP address to the client (if the client is configured with an IP address and the IP address meets requirements of the server, the server approves the IP address of the client). The IP address of the peer can be directly specified or assigned from the address pool.

(4) Borrowing IP addresses of other interfaces: An interface can borrow an IP address from another interface on the same device that is assigned an IP address.

Note

- IP addresses of Ethernet interfaces, tunnel interfaces, and loopback interfaces can be borrowed. However, these interfaces cannot borrow IP addresses from other interfaces.

- The IP addresses of the borrowed interfaces cannot be borrowed from other interfaces.
- If a borrowed interface has multiple IP addresses, only the primary IP address can be borrowed.
- The IP address of one interface can be lent to multiple interfaces.
- IP addresses of borrowing interfaces are always consistent with and change with IP addresses of borrowed interfaces.

2. Configuring Multiple IP Addresses for an Interface

An interface on a device can be configured with multiple IP addresses, of which one is the primary IP address and the others are secondary IP addresses. Theoretically, the number of secondary IP addresses is not limited. However, secondary IP addresses must belong to different networks and secondary IP addresses must be in different networks from primary IP addresses. In network construction, secondary IP addresses are often used in the following circumstances:

- A network does not have enough host addresses. For example, when the number of hosts exceeds 254 in a local area network(LAN), one class C network is not enough and another class C network is needed. In this case, two networks need to be connected. Therefore, more IP addresses are needed.
- Many old networks are based on Layer 2 bridged networks without subnetting. You can use secondary IP addresses to upgrade the network to a routing network based on IP layer. For each subnet, one device is configured with one IP address.
- When two subnets of one network are isolated by another network, in consideration that one subnet cannot be configured on two or more interfaces of a device, you can connect the isolated subnets by creating a subnet on the isolated network and configuring a secondary address.

3. Broadcast Packet Processing

Broadcast packets refer to the packets destined for all hosts on a physical network. The device supports two types of broadcast packets. One type is limited broadcast packets, with the 32-bit destination address of all ones, that is, 255.255.255.255. The other type is directed broadcast packets, with the destination address of all hosts in a specified network, that is, host ID bits of all ones, for example, 192.168.1.255/24. Limited broadcast packets are blocked by the router, whereas directed broadcast packets can be forwarded.

If IP network devices forward limited broadcast packets, the network may be overloaded, which severely affects network performance. This circumstance is called a broadcast storm. Devices provide some approaches to confine broadcast storms within the local network and prevent continuous spread of broadcast storms. Layer 2 network devices such as bridges and switches still forward and spread broadcast storms.

The best way to avoid broadcast storms is to assign a broadcast address to each network, which is directed broadcast. This requires the IP protocol to use directed broadcast packets rather than limited broadcast packets to spread data. When receiving IP directed broadcast packets, the devices that is not directly connected to the destination subnet will forward them in the same way as that for unicast packets. After directed broadcast packets reach the device that is directly connected to the destination subnet, the device converts the directed broadcast mode into limited broadcast mode and broadcasts the packets to all hosts on the destination subnet at the link layer.

For details about broadcast, see RFC919 and RFC922.

4. ICMP Packet

Internet Control Message Protocol (ICMP) is a sub protocol of the TCP/IP protocol suite and is used to transfer control messages between IP hosts and network devices to notify certain devices of packet transmission exceptions. The following describes common ICMP packets.

- Echo request and echo reply

  Common ping operations use echo requests and echo replies. A device sends an echo request to another node. If there is no exception on the way, the destination host returns an echo reply, indicating that the host is reachable.

- Protocol unreachable message

  When a device receives a non-broadcast packet destined for itself and the packet uses the IP protocol that cannot be processed by the device, the device sends an ICMP protocol unreachable message to the source host.

- Host unreachable message

  When a device receives a non-broadcast packet destined for itself but the device does not know a route to forward the packet, it sends an ICMP host unreachable message to the source address.

- Redirection message

  Sometimes a network device sends packets from the interface that receives the packets, indicating that a route may be less than optimal. If this condition occurs, the device will send an ICMP redirection message to the data source, informing the source that the gateway reachable to the destination address is another device on the same subnet. In this way, the data source sends subsequent packets according to the optimal path.

- Mask reply message

  Sometimes, a network device sends an ICMP mask request message to obtain the mask of a subnet. The network device that receives the ICMP mask request message sends a mask reply message.

- TTL timeout error message

  When a device forwards an IP packet, if the TTL expires, the device responds to the source end with a TTL timeout error message.

  To prevent attacks from other devices after the device is located through traceroute, you can disable the function of sending TTL timeout errors on the device. After this function is disabled, the device will no longer make a response when receiving a TTL timeout message.

- Timestamp query

  RFC792 requires the system to return its current time after receiving an ICMP timestamp query request.

  To prevent attackers from obtaining the system time through this protocol and attacking some time-based protocols, you can disable the timestamp query function. Then, the device directly discards received ICMP timestamp query requests.

5. Limiting Transmission Rate of ICMP Error Packets

This function limits the transmission rate of ICMP error packets by using the token bucket algorithm to prevent denial of service (DoS) attacks.

If an IP packet needs to be fragmented but the Don’t Fragment (DF) bit in the header is set to 1, the device returns an ICMP destination unreachable message to the source host. This ICMP error message is used to

discover the path MTU. When there are too many other ICMP error messages, the ICMP destination unreachable message may not be sent. As a result, the path MTU discovery function fails. To avoid this problem, you should limit the transmission rate of ICMP destination unreachable messages and other ICMP error messages respectively.

6. IP MTU

The IP protocol at the network layer checks the size of each packet from the upper layer protocol and determines whether it should be "fragmented" based on the MTU size of the local device.

If an IP packet exceeds the IP MTU size, the device fragments the packet. For all devices on the same physical network segment, the IP MTU of interconnected interfaces must be the same. After the link MTU of interfaces is changed, the IP MTU of interfaces will be changed accordingly. The IP MTU of interfaces automatically keeps consistent with the link MTU of interfaces. However, if the IP MTU of interfaces is adjusted, the link MTU of interfaces will not be changed.

7. IP Source Routing

When a device receives an IP packet, it checks the options such as the strict source route, loose source route, and record route in the IP packet header. These options are detailed in RFC791. If the device detects that the packet enables one option, it performs an action accordingly. If the device detects an invalid option, it returns an ICMP parameter error message to the source and then discards the packet.

After the function of processing IP source routing information is enabled on a device, the source route option is added to an IP packet to test the throughput of a specific network or help the packet bypass the failed network. However, this may cause network attacks such as source address spoofing and IP spoofing.

1.1.4 Protocols and Standards

- RFC1918: Address Allocation for Private Internet
- RFC1166: Internet Numbers
- RFC919: Broadcasting Internet Datagrams
- RFC922: Broadcasting Internet Datagrams Subnets
- RFC791: Internet Protocol
- RFC792: Internet Control Message Protocol

1.2 Configuration Task Summary

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring an IP Address for an Interface
- Configuring the Default Gateway for a Management Interface
- Configuring Directed Broadcast Packets
- Configuring ICMP Messages
- Configuring the Transmission Rate of ICMP Error Messages
- Setting the IP MTU Value
- Setting the IP TTL Value
- Configuring IP Routed Port Protection

- Configuring the IP Source Route Option

1.3 Configuring an IP Address for an Interface

1.3.1 Overview

This section describes how to configure an IP address for an interface for communication over the IP network. IP addresses can be manually configured or obtained through DHCP. In general, an interface only needs to be configured with one IP address to achieve communication with other hosts.

1.3.2 Configuration Tasks

(1) Configure an IP address for an interface. The configuration steps below are mutually exclusive. Please configure only one task.

- Configuring a Static IP Address for an Interface
- Configuring an Unnumbered Interface to Borrow an IP Address
- Configuring an IP Address Combination for an Interface

(2) (Optional) Configuring an IP Broadcast Address

1.3.3 Configuring a Static IP Address for an Interface

1. Restrictions and Guidelines

Manual configuration of IP addresses and dynamic acquisition of IP addresses are mutually exclusive. If you configure a new approach to obtain an IP address, the old IP address will be overwritten.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an IP address for an interface.

ip address *ip-address mask* [**secondary**]

No IP address is configured for an interface by default.

1.3.4 Configuring an Unnumbered Interface to Borrow an IP Address

1. Restrictions and Guidelines

- An Ethernet interface cannot be configured as an unnumbered interface. When the Serial Line Internet Protocol (SLIP), High-Level Data Link Control (HDLC), PPP, Link Access Procedure, Balanced (LAPB), or frame relay is configured on a serial interface, the serial interface can be configured as an unnumbered interface. When frame relay is configured, only a point-to-point subinterface can be configured as an unnumbered interface. An X.25 interface cannot be configured as an unnumbered interface.

- The ping operation cannot be used to check whether an unnumbered interface is working properly because an unnumbered interface has no IP address.
- You can monitor the status of an unnumbered interface remotely through the Simple Network Management Protocol (SNMP).
- Network startup cannot be carried out through an unnumbered interface.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an unnumbered interface to borrow an IP address.

ip unnumbered *interface-type interface-number*

An unnumbered interface is not configured to borrow an IP address by default.

1.3.5 Configuring an IP Address Combination for an Interface

1. Restrictions and Guidelines

The IP address combination configuration command can be configured only on switch virtual interfaces (SVIs) and management (MGMT) interfaces.

The IP address combination configuration command and the static IP address configuration command as well as DHCP are mutually exclusive, but the IP address combination configuration command can be used to configure both static IP addresses and DHCP.

- When the IP address combination configuration command is used to configure a static IP address, if an IP address on the same network segment is already configured, the configuration fails.
- When the IP address combination configuration command is used to configure both a static IP address and a dynamic IP address, if the IP address obtained through DHCP does not conflict with the network segment of the static IP address, the IP address obtained through DHCP is the primary IP address and the static IP address is a secondary IP address. If the IP address obtained through DHCP conflicts with the network segment of the static IP address, an IP address will be obtained again, during which the static IP address is a primary IP address.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an IP address combination for the interface.

ip address mix { **dhcp** | *ip-address network-mask* }

No IP address combination is configured for an interface by default.

1.3.6 Configuring an IP Broadcast Address

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an IP broadcast address.

ip broadcast-address *ip-address*

The default IP broadcast address of an interface is 255.255.255.255.

1.4 Configuring the Default Gateway for a Management Interface

1.4.1 Overview

This section describes how to configure the default gateway for a management interface. After configuration, a default route is generated, with the outbound interface of the management interface and the next hop of the configured gateway.

1.4.2 Restrictions and Guidelines

This command can be configured on a management interface only.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface mgmt *interface-number*

(4) Configure the default gateway for the management interface.

gateway *ip-address*

No default gateway is configured for a management interface by default.

1.5 Configuring Directed Broadcast Packets

1.5.1 Overview

You can configure a specified interface to forward directed broadcast packets. Then, the interface can forward directed broadcast packets destined for the directly connected network.

1.5.2 Restrictions and Guidelines

- This configuration applies to the transmission of directed broadcast packets within the destination subnet and will not affect the forwarding of other directed broadcast packets.
- On an interface, you can define an access control list (ACL) to control the forwarding of certain directed broadcast packets. After an ACL is defined, only directed broadcast packets that match the ACL are forwarded.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the interface to allow forwarding directed broadcast packets.

ip directed-broadcast [*acl-number*]

The function of translating the IP directed broadcast mode to the physical broadcast mode is disabled by default.

1.6 Configuring ICMP Messages

1.6.1 Overview

The ICMP protocol is used to transfer control messages between IP hosts and network devices to notify network exceptions. You can enable the functions of sending TTL timeout messages, ICMP destination unreachable messages, ICMP redirection messages, and ICMP mask reply messages, and timestamp query function.

1.6.2 Configuration Tasks

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Enabling the Function of Sending TTL Timeout Messages
- Enabling the Timestamp Query
- Enabling the Function of Sending ICMP Destination Unreachable Messages
- Enabling the Function of Sending ICMP Redirection Messages
- Enabling the Function of Sending ICMP Mask Reply Messages

1.6.3 Enabling the Function of Sending TTL Timeout Messages

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of sending TTL timeout messages.

ip ttl-expires enable

The function of sending TTL timeout messages is enabled by default.

1.6.4 Enabling the Timestamp Query

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the timestamp query function.

ip icmp timestamp

The timestamp query function is enabled by default.

1.6.5 Enabling the Function of Sending ICMP Destination Unreachable Messages

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the function of sending ICMP destination unreachable messages.

ip unreachables

The function of sending ICMP destination unreachable messages is enabled by default.

1.6.6 Enabling the Function of Sending ICMP Redirection Messages

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the function of sending ICMP redirection messages.

ip redirects

The function of sending ICMP redirection messages is enabled by default.

1.6.7 Enabling the Function of Sending ICMP Mask Reply Messages

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the function of sending ICMP mask reply messages.

ip mask-reply

The function of sending ICMP mask reply messages is enabled by default.

1.7 Configuring the Transmission Rate of ICMP Error Messages

1.7.1 Overview

This function limits the transmission rate of ICMP error packets by using the token bucket algorithm to prevent denial of service (DoS) attacks.

If an IP packet needs to be fragmented but the Don't Fragment (DF) bit in the header is set to 1, the device sends an ICMP destination unreachable message to the source host. This ICMP error message is used to discover the path MTU. If there are too many other ICMP error messages, the ICMP destination unreachable packet may not be sent. As a result, the path MTU discovery function fails. To avoid this problem, you should limit the transmission rate of ICMP destination unreachable messages and other ICMP error messages respectively.

1.7.2 Restrictions and Guidelines

Since the precision of the timer is 10 milliseconds, you are advised to set the refresh cycle of a token bucket to an integer multiple of 10 milliseconds. If the refresh cycle is set to a value greater than 0 and smaller than 10 milliseconds, the refresh cycle that actually takes effect is 10 milliseconds. For example, if the transmission rate is set to 1 packet per 5 milliseconds, two ICMP error packets are actually sent per 10 milliseconds. If the refresh cycle is not an integral multiple of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted into an integral multiple of 10 milliseconds. For example, if the transmission rate is set to 3 packets per 15 milliseconds, two ICMP error packets are actually sent per 10 milliseconds.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the transmission rate of ICMP error packets.

ip icmp error-interval [**df**] *interval* [*bucket-size*]

Ten ICMP error packets are transmitted within 100 milliseconds by default.

1.8 Setting the IP MTU Value

1.8.1 Overview

This section describes how to set the MTU of an IP packet. If the size of an IP packet exceeds the IP MTU size, the packet will be fragmented.

1.8.2 Restrictions and Guidelines

For all devices on the same physical network segment, the IP MTU of interconnected interfaces must be the same. The IP MTU of interfaces automatically keeps consistent with the link MTU of interfaces. If the link MTU of interfaces is changed, the IP MTU of interfaces will be changed accordingly. However, if the IP MTU of interfaces is adjusted, the link MTU of interfaces will not be changed.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Set the IP MTU.

ip mtu *mtu*

The default MTU of an IP packet is 1500 bytes.

1.9 Setting the IP TTL Value

1.9.1 Overview

When an IP packet is transmitted from the source address to the destination address through routers, a TTL value is set at the source end and decreases by 1 every time that the IP packet passes through a router. When the TTL value drops to zero, the router discards the packet. TTL prevents infinite transmission of useless packets and waste of bandwidth.

1.9.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Set the IP TTL.

ip ttl

The default TTL value of unicast packets sent by the device is 64.

1.10 Configuring IP Routed Port Protection

1.10.1 Overview

This section describes how to enable routed port protection to prevent packets from being transmitted through the same interface that receives the packets.

1.10.2 Restrictions and Guidelines

This command can only be used for Layer 3 routed ports.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the IP routed port protection.

ip redirect-drop

The IP routed port protection function is disabled by default.

1.11 Configuring the IP Source Route Option

1.11.1 Overview

The IP source route option is used to test the throughput of a specific network and help the packet bypass a failed network.

1.11.2 Restrictions and Guidelines

Enabling the IP source route option may cause network attacks such as source address spoofing and IP spoofing.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the IP source route option.

ip source-route

The IP source route option is enabled by default.

1.12 Monitoring

This section describes the **show** commands used for checking the running status of a configured function to verify the configuration effect.

Table 1-1Monitoring

Command	Purpose
show ip interface [*interface-type interface-number* | **brief**]	Displays the IP address of an interface.
show ip packet statistics [**total** | *interface-type interface-number*]	Displays IP packet statistics.
show ip packet queue	Displays the statistics on sent and received IP packets in the protocol stack.
show ip raw-socket [*protocol-number*]	Displays all IPv4 raw sockets.
show ip sockets	Displays all IPv4 sockets.
show ip udp [**local-port** *port-number* | **peer-port** *port-number*]	Displays all IPv4 UDP sockets.
show ip udp statistics	Displays the statistics on all IPv4 UDP sockets.

1.13 Configuration Examples

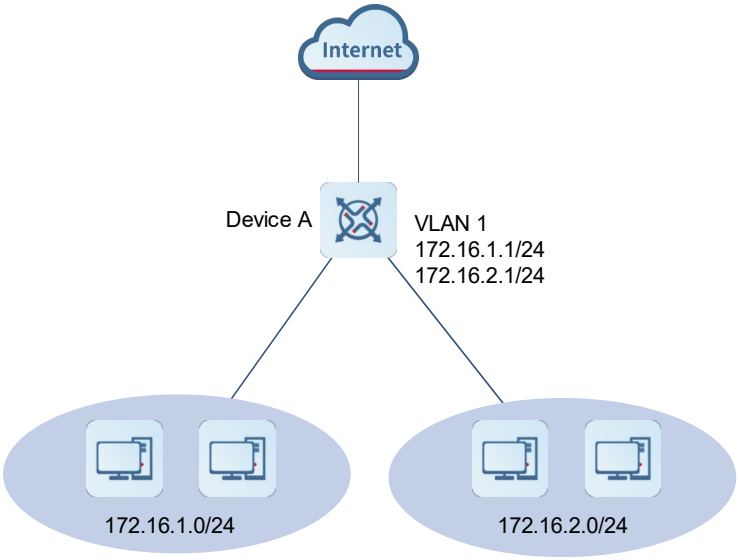
1.13.1 Configuring IPv4 Addresses for Network Communication

1. Requirements

As shown in Figure 1-1, device A is connected to a LAN (belonging to VLAN 1), which involves two network segments: 172.16.1.0/24 and 172.16.2.0/24. Computers on the two network segments are required to access the Internet through device A and hosts on the two network segments can also communicate with each other.

2. Topology

Figure 1-1Topology of Configuring IPv4 Addresses for Network Communication



3. Notes

- Configure two IP addresses on the interface VLAN 1, of which one is a primary IP address and the other is a slave IP address.
- Configure the device as the gateway on the hosts on these two network segments.

4. Procedure

(1) Configure device A.

Configure a primary IP address and a slave IP address for the interface VLAN 1.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface vlan 1
DeviceA(config-if-VLAN 1)# ip address 172.16.1.1 255.255.255.0
DeviceA(config-if-VLAN 1)# ip address 172.16.2.1 255.255.255.0 secondary
```

(2) Configure the hosts on the 172.16.1.0/24 network segment.

Set the gateway to 172.16.1.1/24 for the hosts.

(3) Configure the hosts on the 172.16.2.0/24 network segment.

Set the gateway to 172.16.2.1/24 on the hosts.

5. Verification

Run the **ping** command on device A to check the connectivity with the hosts in the 172.16.1.0/24 network segment.

```
DeviceA# ping 172.16.1.2
Sending 5, 100-byte ICMP Echoes to 172.16.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **ping** command on device A to check the connectivity with the hosts in the 172.16.2.0/24 network segment.

```
DeviceA# ping 172.16.2.1
Sending 5, 100-byte ICMP Echoes to 172.16.2.1, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Run the **ping** command to check the connectivity between the hosts in the 172.16.1.0/24 network segment and the hosts in the 172.16.2.0/24 network segments.

6. Configuration Files

Device A

```
hostname DeviceA
!
interface vlan 1
 ip address 172.16.1.1 255.255.255.0
 ip address 172.16.2.1 255.255.255.0 secondary
!
```