1 eIPv4 Basics Commands

Command	Function
gateway	Configure the default gateway for a management interface.
ip address	Configure an IP address for an interface.
ip address mix	Configure an IP address combination.
ip address negotiate	Configure an interface to obtain the IP address through the Point to Point Protocol (PPP) negotiation.
ip broadcast-address	Configure a broadcast address for an interface.
ip icmp error-interval	Configure the transmission rate of Internet Control Message Protocol (ICMP) error packets.
ip icmp timestamp	Configure the timestamp query function.
ip directed-broadcast	Enable the translation of the IP directed broadcast mode to the physical broadcast mode.
ip mask-reply	Enable the function of sending ICMP mask reply messages.
ip mtu	Configure the maximum transmission unit (MTU) for an IP packet.
ip redirects	Enable the function of sending ICMP redirection messages.
ip redirect-drop	Enable the routed port protection function.
ip source-route	Enable the function of processing IP source routing information.
ip ttl	Configure a time to live (TTL) value for unicast packets sent by the device.
ip ttl-expires enable	Enable the device to send a TTL timeout message.
ip unnumbered	Enable an unnumbered interface to borrow an IP address.
ip unreachables	Enable the function of sending ICMP destination unreachable messages.

show ip interface	Display the IP status of an interface.
show ip packet queue	Display statistics on sent and received IP packets in the protocol stack.
show ip packet statistics	Display the statistics on IP packets.
show ip raw-socket	Display all the IPv4 raw sockets.
show ip sockets	Display all IPv4 sockets.
show ip udp	Display all IPv4 UDP sockets.
show ip udp statistics	Display the number of IPv4 UDP sockets.

1.1 gateway

Function

Run the **gateway** command to configure the default gateway for a management interface.

Run the **no** form of this command to remove this configuration.

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

Syntax

gateway *ip-address*

no gateway

Parameter Description

ip-address: Default gateway of a management interface for Internet Protocol version 4 (IPv4) communication.

Command Modes

MGMT interface mode

Default Level

2

Usage Guidelines

The type of a management interface is MGMT and the interface number is fixed to 0.

Examples

The following example sets the default gateway of a MGMT interface to 1.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface mgmt 0
Hostname(config-if-Mgmt 0)# gateway 1.1.1.1
```

Notifications

When the configured IP address is illegal, the following notification will be displayed:

```
% 0.0.0.0 is not a valid host address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**

1.2 ip address

Function

Run the **ip address** command to configure an IP address for an interface.

Run the **no** form of this command to remove this configuration.

No IP address is configured for an interface by default.

Syntax

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

no ip address [*ip-address mask* [**secondary**]

Parameter Description

ip-address: IP address consisting of 32 bits, with 8 bits for each group. The IP address is expressed in dotted decimal notation.

mask: Network mask consisting of 32 bits. Value **1** indicates the mask bit and **0** indicates the host bit. Every 8 bits form one group. The network mask is expressed in dotted decimal notation.

secondary: Configures an IP address as a secondary IP address.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

A device can receive and send IP packets only after the device is configured with an IP address.

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 bits whose values are ones are for the network part, and the bits whose values are zeros are for host addresses. For example, for class A networks, the network mask is 255.0.0.0. Subnetting allows you to divide a network into several subnets. You can use some bits of the host address as the network ID to decrease the host capacity and increase the number of networks. In this case, network masks are called subnet masks.

The device supports multiple IP addresses on one interface, 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. 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.

Examples

The following example sets the primary IP address to 10.10.10.1, subnet mask to 255.255.255.0, and default gateway to 10.10.10.254, for port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip address 10.10.10.1 255.255.255.0
gateway 10.10.10.254
```

Notifications

Do not set the mask to all ones or zeros (32-bit mask is supported for loopback interfaces). Otherwise, the following notification will be displayed:

```
Invalid IP mask.
```

Do not configure a secondary IP address if a primary IP address is not configured. Otherwise, the following notification will be displayed:

```
Cannot add IP address.
```

Common Errors

- A secondary IP address is configured when no primary IP address is configured.
- Network segments of different IP addresses overlap on the same interface.

Platform Description

N/A

Related Commands

- **show ip interface**
- **gateway**
- **ip default-gateway** (IP routing/static routing)

1.3 ip address mix

Function

Run the **ip address mix** command to configure an IP address combination.

Run the **no** form of this command to remove this configuration.

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

Syntax

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

no ip address mix { **dhcp** | *ip-address network-mask* }

Parameter Description

dhcp: Obtains a dynamic IP address through the Dynamic Host Configuration Protocol (DHCP).

ip-address: IP address consisting of 32 bits, with 8 bits for each group. The IP address is expressed in dotted decimal notation.

network-mask: Network mask, consisting of 32 bits, with 8 bits for each group. Value **1** indicates the mask bit and **0** indicates the host bit. The network mask is expressed in dotted decimal notation.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

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

The IP address combination configuration command, static IP configuration command, and dynamic IP configuration command are mutually exclusive. However, the IP address combination configuration command can be used to configure both static IP addresses and DHCP to obtain dynamic IP addresses.

- When the IP address combination configuration command is used to configure a static IP address, if an IP address in 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 dynamic IP address obtained through DHCP does not conflict with the network segment of the static IP address, the dynamic IP address is the primary IP address and the static IP address is a secondary IP address. If the dynamic 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.

Examples

The following example sets the IP address combination to 192.168.23.110/24 and DHCP on SVI 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# ip address mix dhcp
Hostname(config-if-VLAN 1)# ip address mix 192.168.23.110 255.255.255.0
```

Notifications

N/A

Common Errors

- The IP address combination configuration command is configured after the static or dynamic IP command is configured.
- This command is used on non-SVI interfaces and non-MGMT interfaces.

Platform Description

N/A

Related Commands

- show ip interface

1.4 ip address negotiate

Function

Run the **ip address negotiate** command to configure an interface to obtain the IP address through the Point to Point Protocol (PPP) negotiation.

Run the **no** form of this command to remove this configuration.

No interface is configured to obtain an IP address through the PPP negotiation by default.

Syntax

ip address negotiate

no ip address negotiate

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

When **ip address negotiate** is configured on an interface, **peer default ip address** needs to be configured on the peer.

Examples

The following example configures the interface Dialer 1 to obtain an IP address through the PPP negotiation.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface dialer 1
Hostname(config-if-dialer 1)# ip address negotiate
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**
- **Ошибка: источник перекрёстной ссылки не найден**
- **encapsulation ppp** (interfaces/Ethernet interfaces)

1.5 ip broadcast-address

Function

Run the **ip broadcast-address** command to configure a broadcast address for an interface.

Run the **no** form of this command to remove this configuration.

The default IP broadcast address is 255.255.255.255.

Syntax

ip broadcast-address *ip-address*

no ip broadcast-address

Parameter Description

ip-address: Broadcast address of an IP network.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

Generally, the destination address of IP broadcast packets is all ones, which is expressed as 255.255.255.255. Users can define other IP addresses as broadcast addresses to receive the broadcast packets with the address 255.255.255.255 and user-defined broadcast packets.

Examples

The following example sets the broadcast address of port GigabitEthernet 0/1 to 1.1.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip broadcast-address 1.1.1.1
```

Notifications

Do not configure a broadcast address if no primary IP address is configured for an interface. Otherwise, the following notification will be displayed:

```
Cannot set broadcast address. No primary address exist.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- ip address

1.6 ip icmp error-interval

Function

Run the **ip icmp error-interval** command to configure the transmission rate of Internet Control Message Protocol (ICMP) error packets.

Run the **no** form of this command to restore the default configuration.

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

Syntax

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

no ip icmp error-interval [**df**] *interval* [*bucket-size*]

Parameter Description

df: Configures the transmission rate of ICMP destination unreachable packets triggered by the don't fragment (DF) bit in the IP header.

interval: Refresh cycle of a token bucket, in ms. The value range is from 0 to 2147483647, and the default value is **100**. When the value is **0**, the transmission rate of ICMP error packets is not limited.

bucket-size: Number of tokens contained in a token bucket. The value range is from 1 to 200 and the default value is **10**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

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 DF bit in the header is set to 1, the device sends an ICMP destination unreachable message to the source host. This ICMP error packet is used to discover the path MTU. If there are too many other ICMP error packets, 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 packets and other ICMP error packets respectively.

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 errors 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 errors are actually sent per 10 milliseconds.

Examples

The following example sets the transmission rate of ICMP destination unreachable packets triggered by the DF bit in the IP header to 100 packets per second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip icmp error-interval DF 1000 100
```

The following example sets the transmission rate of other ICMP error packets to 10 packets per second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip icmp error-interval 1000 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ip icmp timestamp

1.7 ip icmp timestamp

Function

Run the **ip icmp timestamp** command to configure the timestamp query function.

Run the **no** form of this command to remove this configuration.

The timestamp query function is enabled by default.

Syntax

ip icmp timestamp

no ip icmp timestamp

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

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

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.

Examples

The following example disables the timestamp query function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip icmp timestamp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip packet queue**
- **show ip packet statistics**

1.8 ip directed-broadcast

Function

Run the **ip directed-broadcast** command to enable the translation of the IP directed broadcast mode to the physical broadcast mode.

Run the **no** form of this command to disable this feature.

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

Syntax

ip directed-broadcast [*acl-number*]

no ip directed-broadcast

Parameter Description

acl-number: No. of an access control list (ACL). The value range is from 1 to 199 and 1300 to 2699. After an ACL is defined, conversion is performed only for directed broadcast packets that match the ACL. No ACL is defined by default and translation is performed for all broadcast packets in subnets.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

IP directed broadcast packets refer to the IP packets destined for a broadcast address in an IP subnet. However, the node that generates the packets is not a member of the destination subnet.

After receiving IP directed broadcast packets, the devices not directly connected to the destination subnet forward the broadcast packets in the same way as that for unicast packets. After directed broadcast packets reach the device directly connected to the destination subnet, the device translates the directed broadcast mode into limited broadcast mode (with a destination IP address being 255.255.255.255) and broadcasts the packets to all hosts on the destination subnet at the link layer.

After the function of translating the directed broadcast mode into the physical broadcast mode is enabled on a specified interface, the interface can forward the directed broadcast packets from the directly connected network. This command affects only the final transmission of directed broadcast packets within destination subnet and will not affect the forwarding of other directed broadcast packets.

On an interface, you can also define an ACL to forward desired directed broadcast packets. After an ACL is defined, only data packets that match the ACL are subject to the translation from the directed broadcast mode to physical broadcast mode.

If the **no ip directed-broadcast** command is run on an interface, the device will discard directed broadcast packets received from the directly connected network.

Examples

The following example enables the translation from directed broadcast mode to physical broadcast mode on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip directed-broadcast
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- ip broadcast-address

1.9 ip mask-reply

Function

Run the **ip mask-reply** command to enable the function of sending ICMP mask reply messages.

Run the **no** form of this command to disable this feature.

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

Syntax

ip mask-reply

no ip mask-reply

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

When 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 returns a mask reply message.

Examples

The following example enables the function of sending ICMP mask reply messages on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip mask-reply
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show ip interface
- show ip packet queue
- show ip packet statistics

1.10 ip mtu

Function

Run the **ip mtu** command to configure the maximum transmission unit (MTU) for an IP packet.

Run the **no** form of this command to restore the default configuration.

The default MTU of an IP packet is 1500 bytes.

Syntax

ip mtu *mtu*

no ip mtu

Parameter Description

mtu: MTU of an IP packet, in bytes. The value range is from 68 to 1500.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

If the size of an IP packet exceeds the IP MTU value, the packet will be fragmented. For all devices on the same physical network segment, the IP MTU configured for the interconnected interfaces must be the same.

If the MTU value of an interface is set by running the **mtu** command, the IP MTU value will be automatically kept the same as that of interfaces. However, if the IP MTU value is adjusted, the MTU value of interfaces will not change accordingly.

Examples

The following example sets the IP MTU of port GigabitEthernet 0/1 to 512 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip mtu 512
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**
- **mtu** (interfaces/Ethernet interfaces)

1.11 ip redirects

Function

Run the **ip redirects** command to enable the function of sending ICMP redirection messages.

Run the **no** form of this command to disable this feature.

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

Syntax

ip redirects

no ip redirects

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

When a route is less than optimal, a device may send packets through an interface that receives the packets. If the function of sending ICMP redirection messages is enabled, when the device sends the packets from the interface that receives the packets, the device sends an ICMP redirection message to the source to inform that the gateway reachable to the destination address is another device on the same subnet. In this way, the source sends subsequent packets along the optimal path.

Examples

The following example disables the function of sending ICMP redirection messages on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no ip redirects
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**
- **show ip packet queue**
- **show ip packet statistics**

1.12 ip redirect-drop

Function

Run the **ip redirect-drop** command to enable the routed port protection function.

Run the **no** command to disable this feature.

The routed port protection function is disabled by default.

Syntax

ip redirect-drop

no ip redirect-drop

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

The routed port protection function is enabled on an interface to prevent packets from being transmitted through the same interface that receives the packets.

Examples

The following example enables the routed port protection function on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip redirect-drop
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**

1.13 ip source-route

Function

Run the **ip source-route** command to enable the function of processing IP source routing information.

Run the **no** form of this command to disable this feature.

The function of processing IP source routing information is enabled by default.

Syntax

ip source-route

no ip source-route

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

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 RFC 791. If the device detects that the packet enables one option, it performs an action accordingly; if the device detects an invalid option, it sends an ICMP parameter error message to the source and then discards the packet.

After the source route option is enabled, you can 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.

Examples

The following example disables the function of processing IP source routing information.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip source-route
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**

1.14 ip ttl

Function

Run the **ip ttl** command to configure a time to live (TTL) value for unicast packets sent by the device.

Run the **no** form of this command to remove this configuration.

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

Syntax

ip ttl *ttl*

no ip ttl

Parameter Description

ttl: TTL value of the unicast packets sent by the device. The value range is from 1 to 255.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

When an IP packet is transmitted from the source address to the destination address through routers, if a TTL value is set, the TTL value decreases by 1 each time 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.

Examples

The following example sets the TTL of unicast packets sent by the device to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip ttl 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show ip interface

1.15 ip ttl-expires enable

Function

Run the **ip ttl-expires enable** command to enable the device to send a TTL timeout message.

Run the **no** form of this command to disable this feature.

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

Syntax

ip ttl-expires enable

no ip ttl-expires enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

When forwarding an IP packet whose TTL expires, a 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 error messages on the device. When this function is disabled, the device will no longer make a response when receiving a TTL timeout message.

Examples

The following example disables the function of sending TTL timeout messages on the device.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip ttl-expires enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**
- **show ip packet queue**
- **show ip packet statistics**

1.16 ip unnumbered

Function

Run the **ip unnumbered** command to enable an unnumbered interface to borrow an IP address.

Run the **no** form of this command to remove this configuration.

No unnumbered interface is configured to borrow an IP address by default.

Syntax

ip unnumbered *interface-type interface-number*

no ip unnumbered

Parameter Description

interface-type interface-number: Interface type and interface number.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

An unnumbered interface is an interface that is enabled with the IP protocol but has no IP address assigned. An unnumbered interface needs to be associated with an interface configured with an IP address for communication. For an IP packet generated by an unnumbered interface, the source IP address of the packet is the IP address of the associated interface. In addition, the routing protocol process decides whether to send a route update packet to the unnumbered interface based on the associated IP address. If you want to use an unnumbered interface, pay attention to the following limitations:

- 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 tool 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.

Examples

The following example configures the unnumbered interface Virtual-ppp 1 to associate with the interface GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface virtual-ppp 1
Hostname(config-if-Virtual-ppp 1)# ip unnumbered gigabitethernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**

1.17 ip unreachables

Function

Run the **ip unreachables** command to enable the function of sending ICMP destination unreachable messages.

Run the **no** form of this command to disable this feature.

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

Syntax

ip unreachables

no ip unreachables

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

If a device receives a unicast packet destined for itself and finds that it cannot process the upper layer protocol of the packet, the device returns an ICMP protocol unreachable message to the data source.

If the device does not know a route to forward packets, it also returns an ICMP host unreachable message to the data source.

This command affects all ICMP destination unreachable messages.

Examples

The following example disables the function of sending ICMP destination unreachable messages on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no ip unreachables
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface**
- **show ip packet queue**
- **show ip packet statistics**

1.18 show ip interface

Function

Run the **show ip interface** command to display the IP status of an interface.

Syntax

show ip interface [*interface-type interface-number* | **brief**]

Parameter Description

interface-type interface-number: Interface type and interface number.

brief: Displays the basic IP configurations of an L3 interface, including primary/secondary IP addresses and interface status.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

If an interface can receive and transmit a data packet, the interface is available, and the device software will create a direct route in the routing table. If the interface becomes unavailable, the software will delete the direct route from the routing table.

If an interface is available, the status of the line protocol will be displayed as "up". If only a physical line is available, the status of the interface will be displayed as "up".

The displayed result may be different depending on the interface type because some options are specific to certain interfaces.

Examples

The following example displays the IP status of all interfaces.

```
Hostname> enable
Hostname# show ip interface brief
Interface            IP-Address(Pri)  IP-Address(Sec) Status Protocol
GigabitEthernet 0/10  2.2.2.2/24     3.3.3.3/24    down    down
GigabitEthernet 0/11  no address     no address    down    down
VLAN 1                   1.1.1.1/24     no address    down    down
```

Table 1-1 Output Fields of the show ip interface brief Command

Field	Description
Interface	Interface name.
IP-Address(Pri)	Primary IP address and mask of an interface.
IP-Address(Sec)	Secondary IP address and mask of an interface.
Status	Link status of an interface. ● **Up**: Indicates that an interface is up. ● **Down**: Indicates that an interface is down. **administratively down**: A user runs the **shutdown** command to forcibly shut down an interface.
Protocol	IPv4 protocol status of an interface.

The following example displays the IP status of interface VLAN 1.

```
Hostname> enable
```

```
Hostname# show ip interface vlan 1
VLAN 1
  IP interface state is: DOWN
  IP interface type is: BROADCAST
  IP interface MTU is: 1500
  IP address is:
    1.1.1.1/24 (primary)
  IP address negotiate is: OFF
  Forward direct-broadcast is: OFF
  ICMP mask reply is: ON
  Send ICMP redirect is: ON
  Send ICMP unreachabled is: ON
  Proxy ARP is: OFF
ARP packet input number:           0
     Request packet:                 0
     Reply packet:                    0
     Unknown packet:                0
TTL invalid packet number:           0
ICMP packet input number:           0
     Echo request:                    0
     Echo reply:                      0
     Unreachable:                    0
     Source quench:                  0
     Routing redirect:                  0
```

Table 1-2Output Fields of the show ip interface Command

Field	Description
IP interface state is	Status of a network interface. ● **Down**: Indicates that an interface is unavailable, with the hardware status or line protocol status being down. **Up**: Indicates that an interface is available, with both the hardware status and line protocol status being up.
IP interface type is	Interface type, such as broadcast and point-to-point.
IP interface MTU is	MTU value set for an interface.
IP address is	IP address and mask of an interface.
IP address negotiate is	Whether the IP address of an interface is obtained by negotiation.
Forward direct-broadcast is	Whether an interface forwards directed broadcast packets.
ICMP mask reply is	Whether an interface sends an ICMP mask reply packet.
Send ICMP redirect is	Whether an interface sends an ICMP redirection packet.

Field	Description
Send ICMP unreachable is	Whether an interface sends an ICMP unreachable packet.
Proxy ARP is	Whether proxy ARP is enabled.
ARP packet input number	Total number of ARP packets received on an interface, including: ● **Request packet**: Indicates ARP request packets. ● **Reply packet**: Indicates ARP reply packets. ● **Unknown packet**: Indicates unknown packets.
TTL invalid packet number	Number of invalid TTL packets received on an interface.
ICMP packet input number	Total number of ICMP packets received on an interface, including: ● **Echo request**: Indicates echo request packets. ● **Echo reply**: Indicates echo reply packets. ● **Unreachable**: Indicates unreachable packets. ● **Source quench**: Indicates source quench packets. ● **Routing redirect**: Indicates routing redirection packets.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.19 show ip packet queue

Function

Run the **show ip packet queue** command to display statistics on sent and received IP packets in the protocol stack.

Syntax

show ip packet queue

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

This command is used to display statistics on sent and received IP packets in the protocol stack.

Examples

The following example displays the statistics on sent and received IP packets in the protocol stack.

```
Hostname> enable
Hostname# show ip packet queue
Receive 31925 packets(fragment=0):
  IP packet receive queue: length 0, max 1542, overflow 0.
  Receive 13 ICMP echo packets, 25 ICMP reply packets .
  Discards:
    Failed to alloc skb: 0.
    Receive queue overflow: 0.
    Unknow protocol drops: 0.
    ICMP rcv drops: 0. for skb check fail.
    ICMP rcv drops: 0. for skb is broadcast.
Sent packets:
  Success: 15644
  Generate 13 and send 8 ICMP reply packets, send 26 ICMP echo packets.
  It records 187 us as max time in ICMP reply process.
Failed to alloc efbuf: 0
  Dropped by EFMP: 0
  NoRoutes: 887
  Get vrf fails: 0
  Cannot assigned address drops: 0
  Failed to encapsulate ethernet head: 0
ICMP error queue: length 0, max 1542, overflow 0.
```

Table 1-1Output Fields of the show ip packet queue Command

Field	Description
IP packet receive queue	IP packet receiving queue in the protocol stack.
Discards	Packets that are dropped during receiving.
Failed to alloc skb	Number of packets dropped due to the receiving thread allocation failure.
Receive queue overflow	Number of packets that are dropped due to queue overflow.
Unknow protocol drops	Number of packets that are dropped because there is no corresponding protocol available for receiving.
ICMP rcv drops: x. for skb check fail.	The number of packets with ICMP checksum error is x.

Field	Description
ICMP rcv drops: x. for skb is broadcast.	The number of broadcast packets dropped by ICMP is x.
Sent packets	Statistics on sent IP packets.
Success	Number of packets successfully sent by the upper layer.
It records x us as max time in ICMP reply process.	The maximum time in the ICMP reply process is x μs.
Failed to alloc efbuf	Failure count of conversion from the socket buffer into expedited forwarding buffer.
Dropped by EFMP	Statistics on transmission failures.
NoRoutes	Number of packets dropped due to a lack of routes.
Get vrf fails	Count of the failures of getting the VRF instance bound to an interface.
Cannot assigned address drops	Number of packets dropped due to address allocation failures.
Failed to encapsulate ethernet head	Number of packets that fail in the Layer 2 header encapsulation.
ICMP error queue	Receiving queue of ICMP error packets.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.20 show ip packet statistics

Function

Run the **show ip packet statistics** command to display the statistics on IP packets.

Syntax

show ip packet statistics [**total** | *interface-type interface-number*]

Parameter Description

total: Displays the sum of statistic values of all interfaces.

interface-type interface-number: Interface type and interface number.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

This command is used to display the statistics of IP packets of all interfaces.

Examples

The following example displays the statistics of IP packets of all interfaces.

```
Hostname> enable
Hostname# show ip packet statistics
Total
  Received 113962 packets, 11948991 bytes
    Unicast:90962,Multicast:5232,Broadcast:17768
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 34917 packets, 1863146 bytes
    Unicast:30678,Multicast:4239,Broadcast:0
GigabitEthernet 0/1
  Received 6715 packets, 416587 bytes
    Unicast:2482,Multicast:4233,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 6720 packets, 417096 bytes
    Unicast:2481,Multicast:4239,Broadcast:0
Loopback 0
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0,Broadcast:0
Tunnel 1
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
```

```
     Others:0
  Sent 21584 packets, 1122848 bytes
Unicast:21584,Multicast:0,Broadcast:0
```

Table 1-1Output Fields of the show ip packet statistics Command

Field	Description
Total	Sum of the statistic values of all interfaces.
GigabitEthernet 0/1	Statistics of a specific interface.
Received x packets, y bytes	x packets are received, with y bytes in total.
Sent x packets, y bytes	x packets are sent, with y bytes in total.
Unicast	Number of unicast packets.
Multicast	Number of multicast packets.
Broadcast	Number of broadcast packets.
Discards	Number of dropped packets.
HdrErrors	Number of error packets.
BadChecksum	Number of packets with checksum error.
TTLExceeded	Number of packets with the size exceeding the TTL value.
Others	Others
NoRoutes	Number of packets without routing.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.21 show ip raw-socket

Function

Run the **show ip raw-socket** command to display all the IPv4 raw sockets.

Syntax

show ip raw-socket [*protocol-number*]

Parameter Description

protocol-number: Protocol number.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

This command is used to display all IPv4 raw sockets, including the protocol number and process name.

Examples

The following example displays all IPv4 raw sockets.

```
Hostname> enable
Hostname# show ip raw-socket
Number Protocol Process name
1      ICMP     dhcp.elf
2      ICMP     vrrp.elf
3      IGMP     igmp.elf
4      VRRP     vrrp.elf
Total: 4
```

Table 1-1Output Fields of the show ip raw-socket Command

Field	Description
Number	No.
Protocol	Protocol number.
Process name	Process name.
Total	Total number.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.22 show ip sockets

Function

Run the **show ip sockets** command to display all IPv4 sockets.

Syntax

show ip sockets

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

This command is used to display all IPv4 sockets and thus obtain the User Datagram Protocol (UDP) port and Transmission Control Protocol (TCP) port that provide services for external devices.

Examples

The following example displays all IPv4 sockets.

```
Hostname> enable
Hostname# show ip sockets
Number Process name     Type     Protocol LocalIP:Port ForeignIP:Port      State
1      dhcp.elf         RAW      ICMP     0.0.0.0:1     0.0.0.0:0
*
2      vrrp.elf         RAW      ICMP     0.0.0.0:1     0.0.0.0:0
*
3      igmp.elf         RAW      IGMP     0.0.0.0:2     0.0.0.0:0
*
4      vrrp.elf         RAW      VRRP     0.0.0.0:112   0.0.0.0:0
*
5      dhcpc.elf        DGRAM    UDP      0.0.0.0:68    0.0.0.0:0
*
6      orion-snmpd         DGRAM    UDP      0.0.0.0:161   0.0.0.0:0
*
7      wbav2            DGRAM    UDP      0.0.0.0:2000  0.0.0.0:0
*
8      vrrp_plus.elf    DGRAM    UDP      0.0.0.0:3333  0.0.0.0:0
*
9     rds_other_th     DGRAM    UDP      0.0.0.0:3799  0.0.0.0:0                *
10     orion-snmpd         DGRAM    UDP      0.0.0.0:14800 0.0.0.0:0
*
```

```
11     orion-sshd          STREAM   TCP      0.0.0.0:22    0.0.0.0:0
LISTEN
12     orion-telnetd       STREAM   TCP      0.0.0.0:23    0.0.0.0:0
LISTEN
13     wbard            STREAM   TCP      0.0.0.0:4389  0.0.0.0:0
LISTEN
14     wbard            STREAM   TCP      0.0.0.0:7165  0.0.0.0:0
LISTEN
Total: 14
```

Table 1-1 Output Fields of the show ip sockets Command

Field	Description
Number	No.
Process name	Process name.
Type	Socket type. ● **RAW** indicates a raw socket. ● **DGRAM** indicates the packet type. ● **STREAM** indicates the stream type.
Protocol	Protocol number.
LocalIP:Port	Local IP address and port.
ForeignIP:Port	IP address and port of the peer.
State	Status (only for TCP sockets).
Total	Total number of sockets.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.23 show ip udp

Function

Run the **show ip udp** command to display all IPv4 UDP sockets.

Syntax

show ip udp [**local-port** *port-number* | **peer-port** *port-number*]

Parameter Description

local-port *port-number*: Specifies a local port number.

peer-port *port-number*: Specifies a peer port number.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

This command is used to display all IPv4 UDP sockets. You can know the UDP port that provides services for external devices.

Examples

The following example displays all IPv4 UDP sockets.

```
Hostname> enable
Hostname# show ip udp
Number Local Address          Peer Address          Process name
1      0.0.0.0:68             0.0.0.0:0             dhcpc.elf
2      0.0.0.0:161            0.0.0.0:0             snmp_mib_cmd_pr
3      0.0.0.0:3784           0.0.0.0:0             bfd.elf
4      0.0.0.0:3785           0.0.0.0:0             bfd.elf
5      0.0.0.0:7784           0.0.0.0:0             bfd.elf
6      0.0.0.0:42011          0.0.0.0:0             snmpd
```

Table 1-1Output Fields of the show ip udp Command

Field	Description
Number	No.
Local Address	Local IP address and port.
Peer Address	Peer IP address and port.
Process name	Process name.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.24 show ip udp statistics

Function

Run the **show ip udp statistics** command to display the number of IPv4 UDP sockets.

Syntax

show ip udp statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the number of IPv4 UDP sockets.

```
Hostname> enable
Hostname# show ip udp statistics
Number of IPv4 UDP sockets is 4.
```

Table 1-1 Output Fields of the show ip udp Command

Field	Description
Number of IPv4 UDP sockets is x	Total number of IPv4 UDP sockets is x.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A