

# Network Protocol Configuration Commands

Официальный дистрибьютор в России и СНГ ООО «ТМС»  
Адрес: Россия, 117519, г. Москва, Варшавское ш., дом 133, помещение 370

Тел: +7 (495) 723-81-21  
Факс: +7 (495) 723-81-22  
Техподдержка 24/7: +7 (495) 723-33-33  
E-mail: [sales@tmc.ru](mailto:sales@tmc.ru)  
Сайт: [www.dgsys.ru](http://www.dgsys.ru)

# Table of Contents

Chapter 1 IP Address Configuration Commands .....	1
1.1 IP Address Configuration Commands.....	1
1.1.1 arp .....	1
1.1.2 arp pending-time .....	2
1.1.3 arp max-incomplete.....	3
1.1.4 arp max-gw-retries .....	4
1.1.5 arp retry-allarp.....	4
1.1.6 arp timeout .....	5
1.1.7 arp dynamic.....	6
1.1.8 arp send-gratuitous .....	7
1.1.9 arp fast-refresh.....	7
1.1.10 arp timeout-adjust .....	8
1.1.11 arp synchronize .....	8
1.1.12 clear arp-cache .....	9
1.1.13 clear arp statistics .....	10
1.1.14 ip address.....	10
1.1.15 ip host.....	11
1.1.16 show arp.....	12
1.1.17 show arp statistics.....	13
1.1.18 show hosts .....	14
1.1.19 show ip interface .....	14
Chapter 2 DHCP Client Configuration Commands .....	17
2.1 DHCP Client Configuration Commands.....	17
2.1.1 ip address dhcp.....	17
2.1.2 ip dhcp client .....	18
2.1.3 ip dhcp-server .....	19
2.1.4 show dhcp lease .....	20
2.1.5 show dhcp server .....	21
2.1.6 debug dhcp.....	22
Chapter 3 IP Service Configuration Commands .....	24
3.1 IP Service Configuration Commands.....	24
3.1.1 clear tcp.....	24
3.1.2 clear tcp statistics .....	26
3.1.3 debug arp .....	26
3.1.4 debug ip icmp.....	27
3.1.5 debug ip packet.....	30
3.1.6 debug ip raw.....	35
3.1.7 debug ip tcp packet.....	36
3.1.8 debug ip tcp transactions .....	37
3.1.9 debug ip udp.....	40
3.1.10 ip mask-reply.....	41
3.1.11 ip mtu.....	41
3.1.12 ip source-route .....	42

3.1.13 ip tcp synwait-time.....	43
3.1.14 ip tcp window-size .....	44
3.1.15 ip unreachable.....	44
3.1.16 show ip sockets .....	45
3.1.17 show ip traffic .....	46
3.1.18 show tcp .....	47
3.1.19 show tcp brief .....	51
3.1.20 show tcp statistics .....	52
3.1.21 show tcp tcb .....	54
3.2 IP Access List Configuration Commands.....	55
3.2.1 deny.....	56
3.2.2 ip access-group .....	58
3.2.3 ip access-list.....	59
3.2.4 permit .....	60
3.2.5 show ip access-lists .....	62
3.3 IP Access List Configuration Commands.....	63
3.3.1 deny.....	63
3.3.2 ip access-group .....	65
3.3.3 ip access-list.....	66
3.3.4 permit .....	67
3.3.5 show ip access-lists .....	69

## Chapter 1 IP Address Configuration Commands

### 1.1 IP Address Configuration Commands

IP address configuration commands include:

- arp arp
- arp pending-time
- arp max-incomplete
- arp max-gw-retries
- arp retry-allarp
- arp timeout
- arp dynamic
- arp send-gratuitous
- arp fast-refresh
- arp timeout-adjust
- arp synchronize
- clear arp-cache
- clear arp statistics
- ip address
- ip host
- show arp
- show arp statistics
- show hosts
- show ip interface

#### 1.1.1 arp

##### Syntax

To add a static and permanent entry in the Address Resolution Protocol (ARP) cache, use the **arp** command in global configuration mode. To remove an entry from the ARP cache, use the no form of this command.

**arp** *ip-address hardware-address vlan [alias]*

**no arp** *ip-address [vlan]*

##### Parameter

Parameter	Description
<i>ip-address</i>	IP address corresponding to the local data-link address.
<i>hardware-address</i>	Physical address of local data-link address
<i>vlan</i>	vlan belongs to the static arp
<i>alias</i>	(Optional) router responds to ARP requests as if it were the interface of the specified address.

## Default

No entries are permanently installed in the ARP cache.

## Command Mode

Global configuration mode

## Usage Guidelines

The common host all supports dynamic ARP analysis, so user doesn't need to configure static ARP entries for host.

## Example

The following is an example of a static ARP entry for a typical Ethernet host:

```
arp 1.1.1.1 00:12:34:56:78:90 vlan1
```

## Related Commands

**clear arp-cache**

### 1.1.2 arp pending-time

#### Syntax

To configure the pending time for ARP cache resolution, use the **arp pending-time** command. To resume the default setting, use the no form of this command.

**arp pending-time** *seconds*

**no arp pending-time**

#### Parameter

Parameter	Description
seconds	The pending time (seconds) for ARP cache resolution.

## Default

15s

## Command Mode

Global configuration mode

## Usage Guidelines

The first resolution of arp will generate an incomplete entry. This command sets the survival time of the incomplete entry.

## Example

The following example shows how to set the arp pending time to 10 seconds.

```
arp pending-time 10
```

## Related Commands

**show arp**

### 1.1.3 arp max-incomplete

#### Syntax

To configure the maximum number of incomplete ARP entries, use the **arp max-incomplete** command. To resume the default setting, use the no form of this command.

**arp max-incomplete** *number*

**no arp max-incomplete**

#### Parameter

Parameter	Description
number	The maximum number of incomplete ARP entries

#### Default

0 (means no upper limit)

#### Command Mode

Global configuration mode

#### Usage Guidelines

This command sets the upper limit number of incomplete entries during ARP resolution, that is, the number of entries that can be simultaneously resolved.

## Example

The following example shows how to configure an upper limit of incomplete ARP cache entries to 10.

```
arp max-incomplete 10
```

## Related Commands

**show arp**

### 1.1.4 arp max-gw-retries

#### Syntax

To set the maximum retransmissions of the Re-Detect packets, run the first one of the following commands. To return to the default setting, use the no form of this command.

**arp max-gw-retries** *number*

**no arp max-gw-retries**

#### Parameter

Parameter	Description
<i>number</i>	Sets the maximum retransmissions of the Re-Detect packets.

#### Default

3

#### Command Mode

Global configuration mode

#### Usage Guidelines

The ARP entries, which the routing entry gateway depends on, require being redetected at their aging so that the promptness and correctness of the hardware subnet routing can be guaranteed. This command is here used for setting the maximum ARP retransmissions in the redetection process. The bigger its value is, the greater chance the detection has.

#### Example

The following example shows how to set the maximum retransmissions of the Re-Detect packets to 5:

```
arp max-gw-retries 5
```

#### Related Commands

**show arp**

### 1.1.5 arp retry-allarp

#### Syntax

To set whether to carry on redetection at the aging of ARP entries (not just meaning the gateway-related ARP entries), run the following command:

**arp retry-allarp**

**no arp retry-allarp**

## Parameter

None

## Command Mode

Global configuration

## Usage Guidelines

By default, redetection is conducted only to the aging ARPs, which the routing entry gateway depends on. However, if this command is enabled, redetection will be conducted towards all types of aging ARP entries.

## Example

The following example shows how to enable redetection to be carried out to all aging ARP entries.

```
arp retry-allarp
```

## Related Commands

**show arp**

### 1.1.6 arp timeout

#### Syntax

To configure the exist time that a dynamic ARP entry remains in the Address Resolution Protocol (ARP) cache, use the **arp timeout**. To restore the default value, use the no form of this command or **default arp timeout** command.

**arp timeout** *seconds*

**no arp timeout**

**default arp timeout**

#### Parameter

Parameter	Description
<i>seconds</i>	Time in seconds that an entry remains in the ARP cache. A value of zero means that entries are never cleared from the cache.

#### Default

14400 seconds (4 hours)

#### Mode

Interface configuration



## Usage Guidelines

This command is ignored when it is not configured on interfaces using ARP. The show interface command displays the ARP timeout value, as seen in the following example from the show interfaces command:

ARP type: ARPA, ARP timeout 04:00:00

## Example

The following example sets the ARP timeout to 900 seconds on Ethernet interface 10 to allow entries to time out more quickly than the default

```
interface vlan 10
```

```
arp timeout 900
```

## Related Commands

**show interface**

### 1.1.7 arp dynamic

#### Syntax

To configure dynamic learning of ARP, use the **arp dynamic** command. To restore the default setting, use the no form of this command.

**arp dynamic**

**no arp dynamic**

#### Parameter

None

#### Command Mode

Interface configuration mode

#### Example

The following example shows how to allow dynamic ARP learning on interface VLAN 10:

```
interface vlan 10
```

```
arp dynamic
```

## Related Commands

**show interface**

### 1.1.8 arp send-gratuitous

#### Syntax

To configure gratuitous ARP sending function, run the first one of the following commands. To return to the default setting, use the no form of this command.

**arp send-gratuitous [ interval value ]**

**no arp send-gratuitous**

#### Parameter

Parameter	Description
<b>interval</b>	Sets the interval of sending gratuitous ARP.
<i>value</i>	Sets time interval. The default is 120s. Value range: 15-600s.

#### Command Mode

Interface configuration

#### Example

The following example shows how to enable gratuitous ARP sending on Interface Vlan1 and set the time interval to 180s.

```
switch_config_v1#arp send-gratuitous interval 180
```

#### Related Commands

**arp**

### 1.1.9 arp fast-refresh

#### Syntax

To configure ARP fast refresh, run the first one of the following commands. To return to the default setting, use the no form of this command.

**arp fast-refresh**

**no arp fast-refresh**

#### Parameter

None

#### Command Mode

Global configuration mode

#### Example

The following example shows how to enable ARP fast refresh.

```
switch_config#arp fast-refresh
```

## Related Commands

**arp**

### 1.1.10 arp timeout-adjust

#### Syntax

To configure ARP timeout adjustment, run the first one of the following commands. To return to the default setting, use the no form of this command.

**arp timeout-adjust [time]**

**no arp timeout-adjust**

#### Parameter

Parameter	Description
<i>time</i>	Time of time-out adjustio. Default value is 15s. The range is from 0 to 1000s.

#### Command Mode

Global configuration mode

#### Example

The following example shows how to configure ARP timeout to 1s.

```
switch_config#arp timeout-adjust 1
```

## Related Commands

**arp**

### 1.1.11 arp synchronize

#### Syntax

To configure ARP synchronization parameter, run the first one of the following commands. To return to the default setting, use the no form of this command.

**arp synchronize [type]**

**no arp synchronize [type]**

#### Parameter

Parameter	Description
-----------	-------------

type	Synchronization parameter types, including delete-period, update-period, ctrlcard-only-timeout, response-immediately, request-immediately, deletion, distributed-handle-arpreply
------	--

## Command Mode

Global configuration mode

## Example

The following example shows how to synchronize the deletion of arp.

```
switch_config#arp synchronize deletion
```

## Related Commands

**arp**

### 1.1.12 clear arp-cache

## Syntax

To clear all dynamic entries from the ARP cache, use the clear arp-cache command.

**clear arp-cache** [ *ip-address* [ *mask* | *vlan vlanid* ] ]

## Parameter

Parameter	Description
<i>ip-address</i>	IP or subnets
<i>mask</i>	Subnets mask
<i>vlanid</i>	Vlan number

## Command Mode

EXEC

## Example

The following example removes all dynamic entries from the ARP cache:

```
clear arp-cache
```

## Related Command

**arp**

### 1.1.13 clear arp statistics

#### Syntax

To configure ARP statistics, run the following command.

**clear arp statistics** [vlan *vlan* ]

#### Parameter

The parameter vlan means to only show statistics within a vlan.

#### Command Mode

EXEC

#### Example

The following command clears all arp statistics (the current number will not be cleared).

clear arp statistic

#### Related Commands

**show arp statistic**

### 1.1.14 ip address

#### Syntax

To set an IP address and mask for an interface, use the **ip address** command. Currently, there is no strict regulation to distinguish A.B.C IP address. But multicast address and broadcast address can not be used (all host section is '1'). Other than the Ethernet, multiple interfaces of other types can be connected to the same network. Other than the unnumbered interface, the configured network range to the Ethernet interface can not be the same as the arbitrary interfaces of other types. You should configure the primary address before configuring the secondary address. Also you should delete all secondary addresses before deleting the primary address. IP packets generated by the system, if the upper application does not specify the source address, the router will use the IP address configured on the sending interface that on the same network range with the gateway as the source address of the packet. If the IP address is uncertain (like interface route), the router will use the primary address of the sending interface. If the ip address is not configured on an interface, also it is not the unnumbered interface, and then this interface will not deal with any IP packet. To remove an IP address or disable IP processing, use the no form of this command.

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

**no ip address** *ip-address mask*

**no ip address**

#### Parameter

Parameter	Description
-----------	-------------

<i>ip-address</i>	IP address
<i>mask</i>	IP mask
<i>secondary</i>	(optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

## Default

No IP address is defined for the interface.

## Command Mode

interface configuration mode

## Usage Guidelines

If any router on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops. When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses

## Example

In the following example, 202.0.0.1 is the primary address, 255.255.255.0 is the mask and 203.0.0.1 and 204.0.0.1 are secondary addresses for Ethernet interface 1/0:

```
interface vlan 10
ip address 202.0.0.1 255.255.255.0
ip address 203.0.0.1 255.255.255.0 secondary
ip address 204.0.0.1 255.255.255.0 secondary
```

## 1.1.15 ip host

### Syntax

To define a static host name-to-address mapping in the host cache, use the **ip host** command in global configuration mode. To remove the host name-to-address mapping, use the no form of this command.

**ip host** *name address*

**no ip host** *name*

### Parameter

Parameter	Description
<i>name</i>	Host name
<i>Address</i>	IP address

## Default

Disabled

## Command Mode

Global configuration

## Example

The following example shows how to configure host name dns-server to IP host address 202.96.1.3:

```
ip host dns-server 202.96.1.3
```

## 1.1.16 show arp

### Syntax

To display the entries in the Address Resolution Protocol (ARP) table, including the ARP mapping of interface IP address, the static ARP mapping that user configures and the dynamic ARP mapping, use the **show arp** command.

```
show arp
```

### Parameter

This command has no parameters or keywords.

### Mode

EXEC

### Usage Guidelines

The display includes:

Parameter	Description
Protocol	Displays the type of the network address that maps with the physical address. IP, for example.
Address	Displays the network address that maps with the physical address. IP address, for example.
Age	Displays the age in seconds. The router will refresh the time to 0 when using this ARP entry.
Hardware Address	Displays the physical address that corresponds to the network address. It is empty for the unanalyzed entries.
Type	Specifies request encapsulation types that the interface use, including ARPA, SNAP and so on.
Interface	Interface, interface connected with the network address

## Example

The following command displays ARP cache.

```
switch#show arp
Protocol  IP Address      Age(min)  Hardware Address  Type  Interface
IP        192.168.20.77    11        00:30:80:d5:37:e0  ARPA  vlan 10
IP        192.168.20.33    0          Incomplete
IP        192.168.20.22    -         08:00:3e:33:33:8a  ARPA  vlan 10
IP        192.168.20.124  0         00:a0:24:9e:53:36  ARPA  vlan 10
IP        192.168.0.22   -         08:00:3e:33:33:8b  ARPA  vlan 11
```

## 1.1.17 show arp statistics

### Syntax

To show ARP related statistical table items, use the following command.

**show arp statistic [vlan *vlan*]**

### Parameter

The parameter *vlan* means to only show statistics within a *vlan*.

### Command Mode

EXEC

### Usage Guidelines

Display description:

Total statistics	Including total number of arp, incomplete arp, complete arp.
Add and delete statistics	Accumulated times of adding and deleting arp.
Physical egress migration statistics	The number of physical address migrations due to the change in mac address egress.
Delete reason statistics	Including aging, caused by various configurations, mac address migration, command line deletion, etc.

## Example

The following command displays ARP statistics:

```
switch_config#show arp statistics
Total ARP entries 1, Complete ARP entries 1, Incomplete ARP entries 0
Total added: 20, Total deleted: 19
Physical port changed: 18
Deleted by reason
-----
Aged out                : 17
Overwritten by static    : 0
IP address configured    : 0
IP address deleted       : 0
Interface deleted       : 0
```



```

Protocol up-down          : 0
MAC address aged         : 2
Deleted on other cards    : 0
Static arp deleted        : 0
Clear arp                 : 0
HSRP or OIR insertion     : 0
HSRP or sync static deletion: 0

```

### 1.1.18 show hosts

#### Syntax

To display all entries of the host name—address cache, use the **show hosts** command.

**show hosts**

#### Parameter

This command has no parameters or keywords.

#### Command Mode

EXEC

#### Example

The following command shows how to display all host names/address mappings.

```
show hosts
```

#### Related Command

None

### 1.1.19 show ip interface

#### Syntax

To display the IP configuration on interface, use the **show ip interface** command

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

#### Parameter

Parameter	Description
<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.
<i>brief</i>	(Optional) Displays the brief of ip protocols of all vlan ports

## Command Mode

EXEC

## Usage Guidelines

If the interface link layer is usable, the line protocol is marked "Protocol up." If you configure IP address on this interface, the router will add a direct route to the routing table. If the link layer protocol is marked "Protocol down", the direct route will be deleted. This command displays the specified interface information if specified interface type and number, or IP configuration information of all interfaces will be displayed.

## Example

The following example shows how to display IP configuration on interface VLAN 10.

```
switch#show ip interface vlan 10
  vlan 10 is up, line protocol is up
IP address : 192.168.20.167/24
  Broadcast address : 192.168.20.255
  Helper address : not set
  MTU : 1500(byte)
  Forward Directed broadcast : OFF
  Multicast reserved groups joined:
    224.0.0.9 224.0.0.6 224.0.0.5 224.0.0.2
    224.0.0.1
  Outgoing ACL : not set
  Incoming ACL : not set
  IP fast switching : ON
  IP fast switching on the same interface : OFF
  ICMP unreachable : ON
  ICMP mask replies : OFF
  ICMP redirects : ON
```

Display description:

Domain	Description
vlan 10 is up	If the interface hardware is usable, the interface is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.
line protocol is up	If the interface can provide two-way communication, the line protocol is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.
IP address	IP address and mask for interface
Broadcast address	Displays broadcast address
MTU	Displays the MTU value set on the interface.
Helper address	Displays helper address.
Directed broadcast forwarding	Whether the interface forwards the directed broadcast packet.
Multicast reserved groups joined	The multicast group the interface joined.

Outgoing ACL	Outgoing ACL.
Incoming ACL	Incoming ACL.
IP fast switching	Whether enable fast switching on the interface.
Proxy ARP	Whether the interface supports proxy ARP.
ICMP redirects	Whether the interface forwards ICMP redirection packet.
ICMP unreachable	Whether forwards ICMP unreachable packets.
ICMP mask replies	Whether forwards ICMP mask reply packets.

## Chapter 2 DHCP Client Configuration Commands

### 2.1 DHCP Client Configuration Commands

DHCP Client configuration commands include:

- `ip address dhcp`
- `ip dhcp client`
- `ip dhcp-server`
- `show dhcp lease`
- `show dhcp server`
- `debug dhcp`

The section describes DHCP configuration commands, which configure and monitor DHCP protocols on the switch.

#### 2.1.1 `ip address dhcp`

##### Syntax

To obtain an IP address for the interface through Dynamic Host Configuration Protocol (DHCP), run **`ip address dhcp`**. To delete all IP addresses, use the `no` form of this command.

**`ip address dhcp`**

**`no ip address dhcp`**

##### Parameter

None

##### Default

None

##### Command Mode

Interface configuration mode

##### Usage Guidelines

The command enables the interface to obtain an IP address through DHCP protocol, which is conducive for connecting the ISP through the Ethernet interface.

When the command is configured, the switch will forward DHCPDISCOVER information to the DHCP server on the internet.

When the command is canceled, the switch will forward DHCPRELEASE information.

## Example

The following example shows how VLAN11 interface obtains an IP address through DHCP protocol.

```
!
interface vlan11
 ip address dhcp
```

## Related Commands

**ip dhcp client**  
**ip dhcp-server**  
**show dhcp lease**  
**show dhcp server**

## 2.1.2 ip dhcp client

### Syntax

To configure parameters of local switch DHCP client, run the following command.

```
ip dhcp client { bootfileaddmac | minlease seconds | retransmit count | select seconds | class_identifier WORD | client_identifier hrd_ether | retry_interval <1-1440> | tftpdownload | timeout_shut }
```

```
no ip dhcp client { bootfileaddmac | minlease | retransmit | select | class_identifier | client_identifier | retry_interval | tftpdownload | timeout_shut }
```

### Parameter

Parameter	Description
<b>bootfileaddmac</b>	(optional) Enables to add client MAC to the bootfile file name.
<b>minlease <i>seconds</i></b>	(optional) Stands for the acceptable minimum lease time, which ranges from 60 to 86400 seconds.
<b>retransmit <i>count</i></b>	(optional) Stands for the retransmission times of the protocol packets, which ranges from 1 to 10.
<b>select <i>seconds</i></b>	(optional) Stands for the interval of SELECT, which ranges from 5 to 30.
<b>class_identifier <i>WORD</i></b>	(optional) Stands for class ID belongs to the client.
<b>client_identifier <i>hrd_ether</i></b>	(optional) Configures the type of the client ID as Ethernet.
<b>retry_interval &lt;1-1440&gt;</b>	(optional) Configures the retransmission interval.
<b>tftpdownload</b>	(optional) Enable tftp download function.
<b>timeout_shut</b>	(optional) When the time is out, enable the interface up/down.

## Default

The default of minlease is 60s.

The default of retransmit is 4 times.

The default of select is 5s.

The default of class\_identifier is no parameter.

The default of client\_identifier is the character string.

The default of retry\_interval is 1 mins.

The default of timeout\_shut is no parameter.

## Command Mode

Global configuration mode

## Usage Guidelines

Modify these parameters, according to the network structure and the DHCP server.

To return to the default setting, use the no form of these commands.

## Example

The following example shows how to set the minilease time on the DHCP client to 100s.

```
ip dhcp client minlease 100
```

The following example shows how to set the retransmit times on the DHCP client to 3.

```
ip dhcp client retransmit 3
```

The following example shows how to set the time interval of SELECT on the DHCP client to 10s.

```
ip dhcp client select 10
```

## Related Commands

**ip address dhcp**

**ip dhcp-server**

**show dhcp lease**

**show dhcp server**

### 2.1.3 ip dhcp-server

#### Syntax

To specify a familiar DHCP server, you can use ip dhcp-server to designate the IP address of the DHCP server.

**ip dhcp-server** *ip-address*

**no ip dhcp-server** *ip-address*

## Parameter

Parameter	Description
<i>ip-address</i>	IP address of DHCP server

## Default

No any default IP address on the DHCP server.

## Command Mode

Global configuration

## Usage Guidelines

You can designate an IP address for a DHCP server by using this command, which will not replace the previously designated IP address of the DHCP server.

The delete all previous configured IP addresses on the DHCP server, use the no form of this command.

## Example

The following example shows how to designate IP address 192.168.20.1 on the DHCP server:

```
ip dhcp-server 192.168.20.1
```

## Related Commands

**ip address dhcp**

**ip dhcp client**

**show dhcp lease**

**show dhcp server**

### 2.1.4 show dhcp lease

#### Syntax

To check DHCP server distribution information on the switch, run the following command:

**Show dhcp lease**

#### Parameter

None

#### Default

None

## Command Mode

EXEC

## Usage Guidelines

The command is used to check DHCP server distribution information on the switch.

## Example

The following example shows DHCP distribution information on the switch:

```
switch#show dhcp lease
Temp IP addr: 192.168.20.3   for peer on Interface: vlan11
Temp  sub net mask: 255.255.255.0
      DHCP Lease server: 192.168.1.3, state: 4 Rebinding
      DHCP transaction id: 2049
      Lease: 86400 secs,  Renewal: 43200 secs,  Rebind: 75600 secs
Temp default-gateway addr: 192.168.1.2
      Next timer fires after: 02:34:26
      Retry count: 1   Client-ID: router-0030.80bb.e4c0-v11
```

## Related Commands

**ip address dhcp**

**ip dhcp client**

**ip dhcp-server**

**show dhcp server**

**debug dhcp**

## 2.1.5 show dhcp server

### Syntax

To show DHCP server information, run the following command:

**show dhcp server**

### Parameter

None

### Default

None

## Command Mode

EXEC

## Usage Guidelines

The command is used to show DHCP server information.



## Example

The following example shows DHCP server information:

```
switch#show dhcp sever
DHCP server: 255.255.255.255
Leases: 0
Discovers: 62 Requests: 0 Declines: 0 Releases: 0
Offers: 0 Acks: 0 Naks: 0 Bad: 0
Subnet: 0.0.0.0, Domain name:
```

## Related Commands

**ip address dhcp**

**ip dhcp client**

**ip dhcp-server**

**show dhcp lease**

## 2.1.6 debug dhcp

### Syntax

To check the operating state of the dhcp protocol, run the first one of the following two commands:

**debug dhcp [detail]**

**no debug dhcp [detail]**

### Parameter

Parameter	Description
<b>detail</b>	Displays the packet content of DHCP protocol.

### Default

No information is shown by default.

### Command Mode

EXEC

### Usage Guidelines

The following example shows important information about dealing with DHCP:

```
switch#debug dhcp
switch#2000-4-22 10:50:40 DHCP: Move to INIT state, xid: 0x7
2000-4-22 10:50:40 DHCP: SDISCOVER attempt # 1, sending 277 byte DHCP packet
2000-4-22 10:50:40 DHCP: B'cast on vlan11 interface from 0.0.0.0
2000-4-22 10:50:40 DHCP: Move to SELECTING state, xid: 0x7
2000-4-22 10:50:46 DHCP: SDISCOVER attempt # 2, sending 277 byte DHCPpacket
```

2000-4-22 10:50:46 DHCP: B'cast on vlan11 interface from 0.0.0.0  
2000-4-22 10:50:54 DHCP: SDISCOVER attempt # 3, sending 277 byte DHCPpacket

#### Related Commands

**show dhcp lease**

## Chapter 3 IP Service Configuration Commands

### 3.1 IP Service Configuration Commands

The following are IP service configuration commands:

- clear tcp
- clear tcp statistics
- debug arp
- debug ip icmp
- debug ip packet
- debug ip raw
- debug ip tcp packet
- debug ip tcp transactions
- debug ip udp
- ip mask-reply
- ip mtu
- ip source-route
- ip tcp synwait-time
- ip tcp window-size
- ip unreachable
- show ip sockets
- show ip traffic
- show tcp
- show tcp brief
- show tcp statistics
- show tcp tcb

#### 3.1.1 clear tcp

##### Syntax

It is used to delete a TCP connection.

**clear tcp** {**local** *host-name port* **remote** *host-name port* | **tcb** *address*}

##### Parameter

Parameter	Description
<b>local</b> <i>host-name port</i>	IP address and TCP port of the local host
<b>remote</b> <i>host-name port</i>	IP address and TCP port of the remote host
<b>tcb</b> <i>address</i>	TCB address of the to-be-deleted TCP connection

	TCB is an identifier of TCP connection in the inner system, which can be obtained by the command <b>show tcp brief</b> .
--	--

## Command Mode

Management mode

## Usage Guidelines

The **clear tcp** command is mainly used to delete the terminated TCP connection. In some cases, such as faulty in communication lines, restarting TCP connection or the peer host, the TCP connections are terminated in fact. However, the system cannot obtain information about the terminated TCP connection because there is no communication on the TCP connections. In this case, you can run the **clear tcp** command to terminate these invalid TCP connections. The command **clear tcp local host-name port remote host-name port** is used to terminate the connections between the specified host's IP address/port and the remote host's IP address/port. The command **clear tcp tcb address** is used to terminate the TCP connections identified by the TCB address.

## Example

The following example shows that the TCP connection between 192.168.20.22:23 and 192.168.20.120:4420 is deleted. The **show tcp brief** command is used to show the information about the local host and the remote host in TCP connection.

```
switch#show tcp brief
TCB          Local Address      Foreign Address      State
0xE85AC8     192.168.20.22:23    192.168.20.120:4420 ESTABLISHED
0xEA38C8     192.168.20.22:23    192.168.20.125:1583 ESTABLISHED
switch#clear tcp local 192.168.20.22 23 remote 192.168.20.120 4420
```

```
switch#show tcp brief
TCB          Local Address      Foreign Address      State
0xEA38C8     192.168.20.22:23    192.168.20.125:1583 ESTABLISHED
```

In the following example, the TCP connection whose TCB address is **0xea38c8** is deleted. The command **show tcp brief** displays the TCB address of the TCP connection.

```
switch#show tcp brief
TCB          Local Address      Foreign Address      State
0xEA38C8     192.168.20.22:23    192.168.20.125:1583 ESTABLISHED
switch#clear tcp tcb 0xea38c8
switch#show tcp brief
TCB          Local Address      Foreign Address      State
```

## Related Commands

**show tcp**

**show tcp brief**

**show tcp tcb**

### 3.1.2 clear tcp statistics

#### Syntax

It is used to clear the TCP statistics data.

**clear tcp statistics**

#### Parameter

The command has no parameter or keyword.

#### Command Mode

Management mode

#### Example

The following command is used to delete the TCP statistics data:

```
switch#clear tcp statistics
```

#### Related Command

**show tcp statistics**

### 3.1.3 debug arp

#### Syntax

It is used to display the ARP interaction information, such as sending ARP requests, receiving ARP requests, sending ARP response and receiving ARP response. When the switch cannot communicate with the host, the command is used to analyze the ARP interaction. You can run the **no debug arp** command to stop displaying the relative information.

**debug arp [ packet / delete ]**

**no debug arp**

#### Parameter

The command has no parameter or keyword.

#### Command Mode

Management mode

#### Example

```
switch#debug arp
switch#IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, vlan 10
IP ARP: req filtered src 192.168.20.139 00:90:27:d5:a9:1f, dst 192.168.20.82 00:
00:00:00:00:00, wrong cable, vlan 11
IP ARP: created an incomplete entry for IP address 192.168.20.77, vlan 10
IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, vlan 10
```

IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, vlan 10

The first information indicates: the switch receives an ARP request on interface vlan 10; the IP address of the host that sends the ARP request is 192.168.20.116 and the MAC address of the host is 00:90:27:a7:a9:c2; the MAC address of the host 192.168.20.111 is **IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, vlan 10.**

The second information indicates that the switch receives an ARP request from 192.168.20.139 host on interface vlan 10. However, the interface is not in the network the host declares according to the interface configuration on the switch. The host may not be correctly configured. If the switch creates the ARP cache according to the information, it may not communicate with the host that is configured the same address and connected to the normal interface

IP ARP: req filtered src 192.168.20.139 00:90:27:d5:a9:1f, dst 192.168.20.82 00:00:00:00:00, wrong cable, vlan 11

In the third information, to resolve the MAC address of host 192.168.20.77, the switch first creates an incomplete ARP item in the ARP cache. After receiving an ARP response, the MAC address is then added to the ARP cache. According to the location of the switch, the host connects the interface vlan 10.

IP ARP: created an incomplete entry for IP address 192.168.20.77, vlan 10

In the fourth information, the switch sends out the ARP request from the interface vlan 10. The IP address of the switch is 192.168.20.22. The MAC address of the interface is 08:00:3e:33:33:8a. The IP address of the requested host is 192.168.20.77. The fourth information is relative with the third information.

IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, vlan 10

In the fifth information, the switch receives the ARP response on interface vlan 10 from host 192.168.20.77 to host 192.168.20.22. The switch is then informed that the MAC address of the host that returns the ARP response is 00:30:80:d5:37:e0. The information is relative to the third and fourth information.

IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, vlan 10

### 3.1.4 debug ip icmp

#### Syntax

It is used to display the ICMP interaction information. You can run the command **no debug ip icmp** to close the debugging output.

**debug ip icmp**

**no debug ip icmp**

#### Parameter

The command has no parameter or keyword.

#### Command Mode

Management mode

## Usage Guidelines

The command is used to display the received or transmitted ICMP message, which helps to solve end-to-end connection problems. To know the detailed meaning of the command `debug ip icmp`, refer to RFC 792, "Internet Control Message Protocol".

## Example

```
switch#debug ip icmp
switch#ICMP: sent pointer indicating to 192.168.20.124 (dst was 192.168.20.22), len 48
ICMP: rcvd echo from 192.168.20.125, len 40
ICMP: sent echo reply, src 192.168.20.22, dst 192.168.20.125, len 40
ICMP: sent dst (202.96.209.133) host unreachable to 192.168.20.124, len 36
ICMP: sent dst (192.168.20.22) protocol unreachable to 192.168.20.124, len 36
ICMP: rcvd host redirect from 192.168.20.77, for dst 22.0.0.3 use gw 192.168.20.26, len 36
ICMP: rcvd dst (22.0.0.3) host unreachable from 192.168.20.26, len 36
ICMP: sent host redirect to 192.168.20.124, for dst 22.0.0.5 use gw 192.168.20.77, len 36
ICMP: rcvd dst (2.2.2.2) host unreachable from 192.168.20.26, len 36
```

Details about the first information are shown in the following table:

ICMP: sent pointer indicating to 192.168.20.124 (dst was 192.168.20.22), len 48

Field	Description
ICMP	Information about the ICMP message
Sent	Sending the ICMP message
pointer indicating	ICMP message which means that the original parameters of the IP message are incorrect and incorrect domain is pointed out  The following are other types of ICMP message:  echo reply  dst unreachable: ---net unreachable ---host unreachable ---protocol unreachable ---port unreachable ---fragmentation needed and DF set ---source route failed ---net unknown ---destination host unknown ---source host isolated ---net prohibited ---host prohibited ---net tos unreachable ---host tos unreachable  source quench  redirect messages:

	---net redirect ---host redirect ---net tos redirect ---host tos redirect echo router advertisement router solicitation time exceeded : ---ttl exceeded ---reassembly timeout parameter problem : ---pointer indicating ---option missed ---bad length timestamp timestamp reply information request information reply mask request mask reply  If the ICMP type is unknown, the system is to display the values of the ICMP type and code.
to 192.168.20.124	Destination address of the ICMP message, which is also the source address of the original message that generates the ICMP message
(dst was 192.168.20.22)	Destination address of the original message that generates the ICMP message
len 48	Length of the ICMP message, excluding the length of the IP header

Details about the second information are shown in the following table:

ICMP: rcvd echo from 192.168.20.125, len 40

Field	Description
rcvd	Receiving the ICMP message
echo	Echo request message, which is a type of the ICMP message
from 192.168.20.125	Source address of the ICMP message

Details about the third information are shown in the following table:

ICMP: sent echo reply, src 192.168.20.22, dst 192.168.20.125, len 40

Field	Description
-------	-------------



src 192.168.20.22	Means that the source address of the ICMP message is 192.168.20.22.
dst 192.168.20.125	Means that the destination address of the ICMP message is 192.168.20.125.

According to the type of the ICMP message, the information that generates the ICMP message adopts different formats to display the message content.

For example, the **redirect** message of ICMP is printed in the following format:

ICMP: rcvd host redirect from 192.168.20.77, for dst 22.0.0.3 use gw 192.168.20.26, len 36

ICMP: sent host redirect to 192.168.20.124, for dst 22.0.0.5 use gw 192.168.20.77, len 36

In the first information, an ICMP redirect message from host 192.168.20.77 is received. Gateway 192.168.20.26 is recommended to reach the destination host 22.0.0.3. The length of the ICMP message is 36 bytes.

In the second information, the ICMP redirect message is sent to from host 192.168.20.124 to host 22.0.0.5 through gateway 192.168.20.77. The length of the ICMP message is 36 bytes.

The **dst unreachable** message of ICMP adopts the following format for printing:

ICMP: sent dst (202.96.209.133) host unreachable to 192.168.20.124, len 36

ICMP: rcvd dst (2.2.2.2) host unreachable from 192.168.20.26, len 36

In the first information, the switch cannot route a certain IP message, so it sends the **destination** (202.96.209.133) **unreachable** message to the source host (192.168.20.124). The length of the ICMP message is 36 bytes.

In the second information, after receiving an ICMP message from host 192.168.20.26, the switch notifies host 192.168.20.26 that the destination address (2.2.2.2) cannot be reached. The length of the ICMP message is 36 bytes.

### 3.1.5 debug ip packet

#### Syntax

It is used to display the IP interaction information. The command **no debug ip packet** is used to stop displaying information.

**debug ip packet** [**detail**] [**access-group** *ip-access-list-name*] [**interface** *type number*]

**no debug ip packet**

#### Parameter

Parameter	Description
<b>detail</b>	The parameter is used to export the protocol information about IP message encapsulation, such as protocol number, UDP, TCP port number and ICMP message type
<i>ip-access-list-name</i>	The parameter is used to filter the names of the IP access control list in the exported information Only the information about the IP message in the specified IP access control list can be exported.

<i>access-group</i>	<p>The parameter is used to filter the names of the IP access control list in the exported information</p> <p>Only the information about the IP message in the specified IP access control list can be exported.</p>
<i>interface</i>	<p>The parameter is used to filter the port name of the exported information</p> <p>Only the information about the IP message satisfied the designated port can be exported.</p>

## Command Mode

Management mode

## Usage Guidelines

The command is used to find the destination of each received or locally generated IP message, which helps to detect the reason of communication problems.

The command is used in the following cases:

- forwarded
- forwarded as the multicast message or the broadcast message
- addressing failure during message forwarding
- Sending the **redirect** message
- Rejected because of having the original routing option
- Rejected because of illegal IP options
- Original route
- Message sent from the local machine should be segmented, but the DF is reset.
- Receiving message
- Receiving IP segment
- Sending message
- Sending broadcast/multicast
- Addressing failure when message is generated locally
- Locally generated message is segmented
- Received message is filtered
- Transmitted message is filtered
- Link layer fails to be encapsulated (only for Ethernet)
- Unknown protocol

This command may export lots of information. You'd better use it when the switch is in the free state. Otherwise, the performance of the system will be badly affected. You are recommended to filter the output information through the IP access control list, enabling the system to export the useful message.

## Command Mode

Management mode

## Example

```
switch#debug ip packet
switch#IP: s=192.168.20.120 (vlan 10), d=19.0.0.9 (vlan 10), g=192.168.20.1, len=60, redirected
IP: s=192.168.20.22 (local), d=192.168.20.120 (vlan 10), g=192.168.20.120, len=56, sending
IP: s=192.168.20.120 (vlan 10), d=19.0.0.9 (vlan 10), g=192.168.20.1, len=60, forward
IP: s=192.168.20.81 (vlan 10), d=192.168.20.22 (vlan 10), len=56, rcvd
```

Field	Description
IP	Means that the information is about the IP message.
s=192.168.20.120 (vlan 10)	Source address of the IP message and the interface name that receives message (for message that is not locally generated)
d=19.0.0.9 (vlan 10)	Destination address of the IP message and the interface name that sends message (if routing is successful)
g=192.168.20.1	Next-hop destination address of the IP message, which may be the gateway's address or the destination address
len	Length of the IP message
redirected	Means that the routing switch is to send the ICMP redirect message to the source host. Other cases are shown in the following:  <b>forward</b> --- the message is forwarded.  <b>forward directed broadcast</b> ---the message is forwarded as the <b>redirect</b> message and the message will become the physical broadcast on the transmitting interface.  unroutable---the message addressing fails and the message will be dropped.  source route---source route  rejected source route---the current system does not support the source route, therefore, the message with the IP source route is declined.  bad options---the IP option is incorrect and the message will be dropped.  need frag but DF set---the local message need be fragmented,while the DF is set.  rcvd---the message is locally received.  rcvd fragment---the message fragment is received.  sending---the locally generated message is sent.  sending broad/multicast---the locally generated broadcast/muticast message is sent.  sending fragment--- the IP message locally fragmented is sent.  denied by in acl---It is declined by the access control list on the reception interface.  denied by out acl---It is declined by the transmitter access control on the transmitter interface.  unknown protocol--- unknown protocol

	encapsulation failed---The protocol fails to be encapsulated. It is only for the Ethernet. When the message on the Ethernet is dropped because of the ARP resolution failure, the information is displayed.
--	---

In the first information, the switch receives an IP message; the source address of the received message is 192.168.20.120; the message is from the network segment the vlan 10 interface connects; its destination address is 19.0.0.9. According to the routing table, the transmitter interface is vlan 10, the address of the gateway is 192.168.20.1 and the message length is 60 bytes. The gateway and the source host are directly connected in the same network, that is, the network that vlan 10 connects. In this case, the switch sends out the ICMP redirect message.

IP: s=192.168.20.120 (vlan 10), d=19.0.0.9 (vlan 10), g=192.168.20.1, len=60, redirected

In the second information, the transmission of the ICMP redirect message is described. The source address is the local address 192.168.20.22. The destination address is 192.168.20.120. The message is directly sent from the vlan 10 interface to the destination address. Therefore, the gateway's address is the destination address 192.168.20.120. The length of the ICMP redirect message is 56 bytes.

IP: s=192.168.20.22 (local), d=192.168.20.120 (vlan 10), g=192.168.20.120, len=56, sending

The third information shows that the IP layer receives an IP message. The source address and destination address of the IP message are 192.168.20.120 and 19.0.0.9 respectively. The reception interface is vlan 10. By checking the routing table, the system finds that the IP message needs to be forwarded to the vlan10 interface. The length of the IP message is 60 bytes. The third information shows that the message shown in the first information will be forwarded after the system sends the ICMP redirect message.

IP: s=192.168.20.120 (vlan 10), d=19.0.0.9 (vlan 10), g=192.168.20.77, len=60, forward

The fourth information shows that the IP layer receives an IP message. The source address and destination address of the IP message are 192.168.20.81 and 192.168.20.22 respectively. The reception interface is vlan 10. The length of the IP message is 56 bytes. The IP message is locally received.

IP: s=192.168.20.81 (vlan 10), d=192.168.20.22 (vlan 10), len=56, rcvd

The following is an example about the output information after running the **debug ip packet detail** command. Only the newly added parts are described.

switch#debug ip packet detail

switch#IP: s=192.168.12.8 (vlan 10), d=255.255.255.255 (vlan 10), len=328, rcvd, UDP: src=68, dst=67

IP: s=192.168.20.26 (vlan 10), d=224.0.0.5 (vlan 10), len=68, rcvd, proto=89

IP: s=192.168.20.125 (vlan 10), d=192.168.20.22 (vlan 10), len=84, rcvd, ICMP: type=0, code = 0

IP: s=192.168.20.22 (local), d=192.168.20.124 (vlan 10), g=192.168.20.124, len=40, sending, TCP: src=1024, dst=23, seq=75098622, ack=161000466, win=17520, ACK

Field	Description
UDP	Name of the protocol, such as UDP, ICMP and TCP Other protocols are represented by their protocol number.
type, code	Type and code of the ICMP message
src, dst	Source address and destination address of the UDP message and the TCP message

seq	Sequence number of the TCP message
ack	Acknowledge number of the TCP message
win	Window value of the TCP message
ACK	If ACK is set in the control bit of the TCP message, the acknowledge number is valid. Other control bits include SYN, URG, FIN, PSH and RST.

The first information indicates that the UDP message is received. The source port is port 68 and the destination port is port 67.

IP: s=192.168.12.8 (vlan 10), d=255.255.255.255 (vlan 10), len=328, rcvd, UDP: src=68, dst=67

The second information indicates that the protocol number of the received message is 89.

IP: s=192.168.20.26 (vlan 10), d=224.0.0.5 (vlan 10), len=68, rcvd, proto=89

The third information indicates that the ICMP message is received. Both the type and the code of the message are represented by the number 0.

IP: s=192.168.20.125 (vlan 10), d=192.168.20.22 (vlan 10), len=84, rcvd, ICMP: type=0, code = 0

The fourth information indicates that the TCP message is sent. The source port and destination port are port 1024 and port 23 respectively. The sequence number and the acknowledge number are 75098622 and 161000466 respectively. The size of the reception window is 17520. The ACK logo is set. For details, refer to RFC 793—Transmission Control Protocol.

IP: s=192.168.20.22 (local), d=192.168.20.124 (vlan 10), g=192.168.20.124, len=40, sending, TCP: src=1024, dst=23, seq=75098622, ack=161000466, win=17520, ACK

The access control list is described in the following. For example, if the messages with the source address 192.168.20.125 require to be displayed, you need to define the standard access control list to permit only the IP message whose source address is 192.168.20.125. You then run the command **debug ip packet** to use the access control list.

```
switch#config
switch_config#ip access-list standard abc
switch_config_std_nacl#permit 192.168.20.125
switch_config_std_nacl#exit
switch_config#exit
switch#debug ip packet abc
switch#IP: s=192.168.20.125 (vlan 101), d=192.168.20.22 (vlan 101), len=48, rcvd
```

In the previous commands, the standard access control list is used. You can also use the extensible access control list.

## Related Command

### **debug ip tcp packet**

### 3.1.6 debug ip raw

#### Syntax

It is used to display the IP interaction information. Run the command **no debug ip raw** to stop displaying the information.

**debug ip raw** [**detail**] [**access-group access-list-group**] [**interface type number**]  
**no debug ip raw**

#### Parameter

Parameter	Description
<b>detail</b>	(optional) The parameter is used to export the protocol information about IP message encapsulation, such as protocol number, UDP, TCP port number and ICMP message type
<i>access-list-group</i>	(optional) The parameter is used to filter the names of the IP access control list in the exported information Only the information about the IP message in the specified IP access control list can be exported.
<i>interface</i>	(optional) The parameter is used to filter the port name of the exported information Only the information about the IP message satisfied the designated port can be exported.

#### Command Mode

Management mode

#### Usage Guidelines

The command is used to find the destination of each received or locally generated IP message, which helps to detect the reason of communication problems.

The command is used in the following cases:

- Forwarded
- Forwarded as the multicast message or the broadcast message
- Addressing failure during message forwarding
- Sending the **redirect** message
- Rejected because of having the original routing option
- Rejected because of illegal IP options
- Original route
- Message sent from the local machine should be segmented, but the DF is reset.
- Receiving message
- Receiving IP segment
- Sending message

- Sending broadcast/multicast
- Addressing failure when message is generated locally
- Locally generated message is segmented
- Received message is filtered
- Transmitted message is filtered
- Link layer fails to be encapsulated (only for Ethernet)
- Unknown protocol

This command may export lots of information. You'd better use it when the switch is in the free state. Otherwise, the performance of the system will be badly affected. You are recommended to filter the output information through the IP access control list, enabling the system to export the useful message.

### Example

Similar to the **debug ip packet** command

### Related Command

**debug ip tcp packet**

## 3.1.7 debug ip tcp packet

### Syntax

It is used to display the TCP message. To stop displaying the TCP message, run the command **no debug ip tcp packet**.

**debug ip tcp packet**

**no debug ip tcp packet**

### Parameter

The command has no parameter or keyword.

### Command Mode

Management mode

### Example

```
switch#debug ip tcp packet
switch#tcp: O ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 50659460
        DATA 1 ACK 3130379810 PSH WIN 4380
tcp: I ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 3130379810
        DATA 2 ACK 50659460 PSH WIN 16372
tcp: O ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 50659461
        DATA 50 ACK 3130379812 PSH WIN 4380
tcp: O FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 50659511
        ACK 3130379812 FIN WIN 4380
tcp: I FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
        ACK 50659511 WIN 16321
```

```

tcp: I FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
      ACK 50659512 WIN 16321
tcp: I FIN_WAIT_2 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
      ACK 50659512 FIN WIN 16321
tcp: O TIME_WAIT 192.168.20.22:23 192.168.20.125:3828 seq 50659512
      ACK 3130379813 WIN 4380
tcp: I LISTEN 0.0.0.0:23 0.0.0.0:0 seq 3813109318
      DATA 2 ACK 8057944 PSH WIN 17440
tcp: O LISTEN 0.0.0.0:23 0.0.0.0:0 seq 8057944
      RST

```

Field	Description
tcp:	Information about the TCP message
O	Sending the TCP message
ESTABLISHED	Current state of the TCP connection For the description of the TCP connection state, refer to the description of the command <b>debug ip tcp transactions</b> .
192.168.20.22:23	Means that the source address of the message is 192.168.20.22 and the source port is port 23.
192.168.20.125:3828	Means that the destination address of the message is 192.168.20.125 and the destination port is port 3828.
seq 50659460	Means that the sequence number of the message is 50659460.
DATA 1	Means that the number of valid data bytes contained in the message is 1.
ACK 3130379810	Means that the acknowledge number of the message is 3130379810.
PSH	Means that PSH in the control bits of the message is set. Other control bits include ACK, FIN, SYN, URG and RST.
WIN 4380	It is used to notify the peer reception end of the cache size. The current cache size is 4380 sizes.
I	Receiving the TCP message

If the previous fields are not displayed, the field in the TCP message does not have the valid value.

## Related Command

**debug ip tcp transactions**

### 3.1.8 debug ip tcp transactions

#### Syntax

It is used to display the TCP interaction information, such as the change of the TCP connection state. Run the command **no debug ip tcp transactions** to stop displaying the information.



## debug ip tcp transactions

## no debug ip tcp transactions

### Parameter

The command has no parameter or keyword.

### Command Mode

Management mode

### Example

```
switch#debug ip tcp transactions
switch#TCP: rcvd connection attempt to port 23
TCP: TCB 0xE88AC8 created
TCP: state was LISTEN -> SYN_RCVD [23 -> 192.168.20.125:3828]
TCP: sending SYN, seq 50658312, ack 3130379657 [23 -> 192.168.20.125:3828]
TCP: state was SYN_RCVD -> ESTABLISHED [23 -> 192.168.20.125:3828]
TCP: connection closed by user, state was LISTEN [23 -> 0.0.0.0]
TCP: state was TIME_WAIT -> CLOSED [23 -> 192.168.20.125:3827]
TCP: TCB 0xE923C8 deleted
TCP: TCB 0xE7DBC8 created
TCP: connection to 192.168.20.124:513 from 192.168.20.22:1022, state was CLOSED to SYN_SENT
TCP: sending SYN, seq 52188680, ack 0 [1022 -> 192.168.20.124:513]
TCP: state was SYN_SENT -> ESTABLISHED [1022 -> 192.168.20.124:513]
TCP: rcvd FIN, state was ESTABLISHED -> CLOSE_WAIT [1022 -> 192.168.20.124:513]
TCP: connection closed by user, state was CLOSE_WAIT [1022 -> 192.168.20.124:513]
TCP: sending FIN [1022 -> 192.168.20.124:513]
TCP: connection closed by user, state was LAST_ACK [1022 -> 192.168.20.124:513]
TCP: state was LAST_ACK -> CLOSED [1022 -> 192.168.20.124:513]
TCP: TCB 0xE7DBC8 deleted
```

Field	Description
TCP:	Means that the TCP interaction information is displayed.
rcvd connection attempt to port 23	Means that the connection request from peer port 23 (telnet port) is received.
TCB 0xE88AC8 created	Means a new TCP connection control block is generated and its logo is 0xE88AC8.
state was LISTEN -> SYN_RCVD	Means that the state of the TCP state machine changes from the LISTEN state to the SYN_RCVD state.  The TCP state may be one of the following:  LISTEN---waiting for the TCP connection request from any remote host  SYN_SENT---the connection request for creating TCP connection negotiation has been sent and the reply is being waited.  SYN_RCVD---the connection request from the peer has been

		<p>received and the acknowledgement information and its own connection request have also been sent out; the acknowledge information about the peer's connection is being waited.</p> <p>ESTABLISHED---the connection is successful; the data is being transmitted; the data of the upper application can be received and sent.</p> <p>FIN_WAIT_1---the connection termination request has been sent to the peer; the acknowledgement information and the connection termination request from the peer are being waited.</p> <p>FIN_WAIT_2---the connection termination request has been sent to the peer and the acknowledgement information from the peer has been received; the connection termination request from the peer is being waited.</p> <p>CLOSE_WAIT--- the connection termination request from the peer has been received and the acknowledgement information has been sent out; the local user is being waited to close the connection. Once the user demands to close the connection, the system sends out the connection termination request.</p> <p>CLOSING--- the connection termination request has been sent to the peer and the connection termination request from the peer has been received and the acknowledgement information has been sent out; the system is waiting for the local connection termination request acknowledge from the peer.</p> <p>LAST_ACK---The system has received the connection termination request from the peer and acknowledged it; the system has already sent out connection termination request; the acknowledge is being waited for.</p> <p>TIME_WAIT---the period when the system waits for the peer to receive the acknowledgement of the connection termination request</p> <p>CLOSED---the connection is closed.</p> <p>For details, refer to RFC 793, Transmission Control Protocol.</p>
[23 192.168.20.125:3828]	->	<p>The first field (23) in the bracket means the local TCP port.</p> <p>The second field (192.168.20.125) in the bracket means the remote IP address.</p> <p>The third field (3828) in the bracket means the remote TCP port.</p>
sending SYN		Means a connection request message is sent out (SYN in the control bits of the TCP header is set). Other TCP control bits include SYN, ACK, FIN, PSH, RST and URG.
seq 50658312		Means that the sequence number for sending the message is 50658312.
ack 3130379657		Means that the acknowledgement number for sending the message is 3130379657.
rcvd FIN		Means that the connection termination request is received (FIN in the control bits of the TCP header is set).
connection closed by		Means that the upper application requires closing the TCP

user	connection.
connection timed out	Means that connection timeout is closed.

## Related Command

### debug ip tcp packet

## 3.1.9 debug ip udp

### Syntax

It is used to display the UDP interaction information. Run the command **no debug ip udp** to stop displaying the information.

### debug ip udp

### no debug ip udp

### Parameter

The command has no parameter or keyword.

### Command Mode

Management mode

### Example

```
switch#debug ip udp
switch#UDP: rcvd src 192.168.20.99(520), dst 192.168.20.255(520), len = 32
UDP: sent src 192.168.20.22(20001), dst 192.168.20.43(1001), len = 1008
```

Field	Description
UDP	Means that the information is about the UDP message.
rcvd	Means that the message is received.
sent	Means that the message is sent.
src	Means the source IP address of the UDP message and the UDP port.
dst	Means the destination IP address of the UDP message and the UDP port.
len	Means the length of the UDP message.

The first line in the previous information shows that a UDP message is received. The UDP message is sent from host 192.168.20.99. Both the source port and the destination port are port 520. The destination address is 192.168.20.255. The length of the message is 32 bytes.

The second line in the previous information shows that a UDP message is sent. The local address and the destination address are 192.168.20.22 and 192.168.20.43 respectively. The source port and the destination port are port 20001 and port 1001 respectively. The length of the message is 1008 bytes.

### 3.1.10 ip mask-reply

#### Syntax

It is used to enable the switch to reply the mask request of the IP address on the designated interface. Run the command **no ip mask-reply** to disable the function.

**ip mask-reply**

**no ip mask-reply**

**default ip mask-reply**

#### Parameter

The command has no parameter or keyword.

#### Default

The mask request of the IP address is not replied.

#### Command Mode

Interface configuration mode

#### Example

```
interface vlan 11
ip mask-reply
```

### 3.1.11 ip mtu

#### Syntax

It is used to set the MTU of the IP message. To reuse **MTUDefault**, run the command **no ip mtu**.

**ip mtu bytes**

**no ip mtu**

#### Parameter

Parameter	Description
<i>bytes</i>	Maximum transmission unit of the IP message, which is calculated by byte

#### Default

It varies with different physical media of the interface. It is the same as MTU. The minimum value is 68 bytes.

## Command Mode

Interface configuration mode

## Usage Guidelines

If the length of the IP message exceeds IP MTU configured on the interface, the switch fragments the message. All devices connecting on the same physical media need be configured the same MTU. The MTU affects the IP MTU. If the value of IP MTU is the same as that of the MTU, the value of IP MTU automatically changes to the new value of the MTU when the MTU value changes. The change of the IP MTU does not affect the MTU.

The minimum value of IP MTU is 68 bytes and the maximum value of IP MTU cannot exceed the MTU value configured on the interface.

## Example

The following example shows that IP MTU on interface vlan 10 is set to 200:

```
interface vlan 10
ip mtu 200
```

## Related Command

**mtu**

### 3.1.12 ip source-route

#### Syntax

It is used to enable the routing switch to process the IP message with the source IP route. To enable the routing switch to drop the IP message with the source IP route, run the command **no ip source-route**.

**ip source-route**

**no ip source-route**

#### Parameter

None

#### Default

The IP message with the source IP route is processed.

## Command Mode

Global configuration mode

## Example

The following command enables the routing switch to process the IP message with the source IP route.

```
ip source-route
```

## Related Command

**ping**

### 3.1.13 ip tcp synwait-time

#### Syntax

It is used to set the timeout time, which is used in the case when the switch waits for the successful TCP connection. To resume to the default time, run the command **no ip tcp synwait-time**.

**ip tcp synwait-time** *seconds*

**no ip tcp synwait-time**

#### Parameter

Parameter	Description
<i>seconds</i>	Time for waiting for the TCP connection, which ranges from 5 to 300 seconds Its default value is 75 seconds.

#### Default

75 seconds

#### Command Mode

Global configuration mode

#### Usage Guidelines

When the switch originates the TCP connection, if the TCP connection is unsuccessful after the waiting time, the switch considers that the connection fails and sends the result to the upper application. You can set the waiting time for the successful TCP connection. The default value is 75 seconds. The option has nothing with the TCP connection message forwarded by the switch. However, it is relevant with the local TCP connection of the switch.

To know the current value of the waiting time, run the command **ip tcp synwait-time ?**. The value in the square bracket is the current value.

#### Example

The following example shows that the waiting time of the TCP connection is set to 30 seconds:

```
switch_config#ip tcp synwait-time 30
```

### 3.1.14 ip tcp window-size

#### Syntax

It is used to set the size of the TCP window. To resume to the default value, run the command **no ip tcp window-size**.

**ip tcp window-size** *bytes*

**no ip tcp window-size**

#### Parameter

Parameter	Description
<i>bytes</i>	Size of the window whose unit is second The maximum size is 65535 bytes. The default size is 2000 bytes.

#### Default

2000 bytes

#### Command Mode

Global configuration mode

#### Usage Guidelines

Do not hastily modify the default value of the window size unless you have a definite purpose.

#### Example

The following example shows that the size of the TCP window is set to 6000 bytes:

```
switch_config#ip tcp window-size 6000
```

### 3.1.15 ip unreachable

#### Syntax

It is used to enable the switch to send the ICMP unreachable message. To stop sending the message, run the command **no ip unreachable**.

**ip unreachable**

**no ip unreachable**

#### Parameter

The command has no parameter or keyword.

#### Default

The ICMP unreachable message is sent.

## Command Mode

Interface configuration mode

## Usage Guidelines

When the switch forwards the IP message, the message is dropped if the relevant route is not in the routing table. In this case, the switch sends the ICMP unreachable message to the source host. According to the information in the ICMP unreachable message, the source host promptly detects the fault and removes it.

## Example

The following example shows that the interface vlan 10 is set to send the ICMP unreachable message:

```
interface vlan 10
ip unreachable
```

### 3.1.16 show ip sockets

## Syntax

It is used to display the socket information.

show ip sockets [ **socketid** ]

## Parameter

Parameter	Description
<i>socketid</i>	Show details of a socket

## Command Mode

Management mode

## Example

```
switch#show ip sockets
```

Proto	Local	Port	Remote	Port	In	Out
17	0.0.0.0	0	0.0.0.0	0	161	0
6	0.0.0.0	0	0.0.0.0	0	513	0
17	0.0.0.0	0	0.0.0.0	0	1698	0
17	0.0.0.0	0	0.0.0.0	0	69	0
6	0.0.0.0	0	0.0.0.0	0	23	0
17	0.0.0.0	0	0.0.0.0	0	137	122590



Field	Description
Proto	IP number The protocol number of UDP is 17 and the number of TCP is 6.
Remote	Remote address
Port	Remote port
Local	Local address
Port	Local port
In	Total number of the received bytes
Out	Total number of the transmitted bytes

### 3.1.17 show ip traffic

#### Syntax

It is used to display the statistics information about the IP traffic.

#### **show ip traffic**

#### Parameter

The command has no parameter or keyword.

#### Command Mode

Management mode

#### Example

```
switch#show ip traffic
IP statistics:
Rcvd: 0 total, 0 local destination, 0 delivered
      0 format errors, 0 checksum errors, 0 bad ttl count
      0 bad destination address, 0 unknown protocol, 0 discarded
      0 filtered , 0 bad options, 0 with options
Opts: 0 loose source route, 0 record route, 0 strict source route
      0 timestamp, 0 router alert, 0 others
Frgs: 0 fragments, 0 reassembled, 0 dropped
      0 fragmented, 0 fragments, 0 couldn't fragment
Bcast: 0 received, 0 sent
Mcast: 0 received, 0 sent
Sent: 230 generated, 0 forwarded
      0 filtered, 0 no route, 0 discarded
ICMP statistics:
Rcvd: 0 total, 0 format errors, 0 checksum errors
      0 redirect, 0 unreachable, 0 source quench
      0 echos, 0 echo replies, 0 mask requests, 0 mask replies
      0 parameter problem, 0 timestamps, 0 timestamp replies
      0 time exceeded, 0 router solicitations, 0 router advertisements
```

Sent: 0 total, 0 errors  
 0 redirects, 0 unreachable, 0 source quench  
 0 echos, 0 echo replies, 0 mask requests, 0 mask replies  
 0 parameter problem, 0 timestamps, 0 timestamp replies  
 0 time exceeded, 0 router solicitations, 0 router advertisements

#### UDP statistics:

Rcvd: 28 total, 0 checksum errors, 22 no port, 0 full sock  
 Sent: 0 total

#### TCP statistics:

Rcvd: 0 total, 0 checksum errors, 0 no port  
 Sent: 3 total

#### IGMP statistics:

Rcvd: 0 total, 0 format errors, 0 checksum errors  
 0 host queries, 0 host reports  
 Sent: 0 host reports

#### ARP statistics:

Rcvd: 8 total, 7 requests, 1 replies, 0 reverse, 0 other  
 Sent: 5 total, 5 requests, 0 replies (0 proxy), 0 reverse

Field	Description
format errors	Means that the format of the message is incorrect, such as the incorrect length of the IP header.
bad hop count	Means that the TTL value decreases to 0 when the routing switch forwards the message. In this case, the message will be dropped.
no route	Means that the routing switch does not have relevant route message.

### 3.1.18 show tcp

#### Syntax

It is used to display the state of all TCP connections.

#### **show tcp**

#### Parameter

The command has no parameter or keyword.

#### Command Mode

Management mode

#### Example

```
switch#show tcp
TCB 0xE9ADC8
```

Connection state is ESTABLISHED, unread input bytes: 934

Local host: 192.168.20.22, Local port: 1023

Foreign host: 192.168.20.124, Foreign port: 513

Enqueued bytes for transmit: 0, input: 934 mis-ordered: 0 (0 packets)

Timer	Starts	Wakeups	Next(ms)
Retrans	33	1	0
TimeWait	0	0	0
SendWnd	0	0	0
KeepAlive	102	0	7199500

iss: 29139463 snduna: 29139525 sndnxt: 29139525 sndwnd: 17520

irs: 709124039 rcvnxt: 709205436 rcvwnd: 4380

SRTT: 15 ms, RXT: 2500 ms, RTV: 687 ms

minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Datagrams (max data segment is 1460 bytes):

Rcvd: 102 (out of order: 0), with data: 92, total data bytes: 81396

Sent: 104 (retransmit: 0), with data: 31, total data bytes: 61

Field	Description
TCB 0xE77FC8	Internal identifier of the TCP connection control block
Connection state is ESTABLISHED	<p>Current state of the TCP connection</p> <p>The TCP connection may be in one of the following state:</p> <p>LISTEN---waiting for the TCP connection request from any remote host</p> <p>SYN_SENT---the connection request has been sent and the reply is being waited.</p> <p>SYN_RCVD---the connection request from the peer has been received and the acknowledgement information and its own connection request have also been sent out; the acknowledge information about the peer's connection is being waited.</p> <p>ESTABLISHED---the connection is successful; the data is being transmitted; the data of the upper application can be received and sent.</p> <p>FIN_WAIT_1---the connection termination request has been sent to the peer; the acknowledgement information and the connection termination request from the peer are being waited.</p> <p>FIN_WAIT_2---the connection termination request has been sent to the peer and the acknowledgement information from the peer has been received; the connection termination request from the peer is being waited.</p> <p>CLOSE_WAIT--- the connection termination request from the peer has been received and the acknowledgement information has been sent out; the local user is being waited to close the connection. Once the user demands to close the connection, the system sends out the connection termination request.</p>

	<p>CLOSING--- the connection termination request has been sent to the peer and the connection termination request from the peer has been received and the acknowledgement information has been sent out; the system is waiting for the local connection termination request acknowledge from the peer.</p> <p>LAST_ACK---The system has received the connection termination request from the peer and acknowledged it; the system has already sent out connection termination request; the acknowledgement is being waited for.</p> <p>TIME_WAIT---the period when the system waits for the peer to receive the acknowledgement of the connection termination request</p> <p>CLOSED---the connection is closed.</p> <p>For details, refer to RFC 793, Transmission Control Protocol.</p>
unread input bytes:	Data that is processed by the lower-layer TCP and the upper application has not received
Local host:	Local IP address
Local port:	Local TCP port
Foreign host:	Remote IP address
Foreign port:	Remote TCP port
Enqueued bytes for transmit:	Bytes in the transmitter queue, including the data that is sent but not yet acknowledged and the data that is not sent
input:	<p>Bytes in the reception queue</p> <p>After sorting, these data waits for the upper application to accept.</p>
mis-ordered:	<p>Number of bytes and messages in the misordered queue</p> <p>After other data is received, these data can enter the reception queue in turn and then can be received by the upper application. For example, after messages 1, 2, 4, 5 and 6 are received, messages 1 and 2 can enter the reception queue, but messages 4, 5 and 6 have to enter the misordered queue and wait for message 3.</p>

After that, the information about the timer of the current connection is displayed, including its startup times, timeout times and the next-time timeout time. The value 0 means that the timer does not run currently. Each connection has its own unique timer. The timeout times is less than the startup times because the timer may be reset in its process. For example, when the retransmission timer works, the system will receive the acknowledgements for all data from the peer. In this case, the retransmission timer stops running.

Timer	Starts	Wakeup	Next(ms)
Retrans	33	1	0
TimeWait	0	0	0
SendWnd	0	0	0
KeepAlive	102	0	7199500

Field	Description
-------	-------------

Timer	Name of the timer
Starts	Startup times of the timer
Wakeups	Timeout times of the timer
Next(ms)	Next-time timeout time (unit: ms) The value 0 means the timer does not run.
Retrans	Retransmission timer, which is used to trigger resending data The timer is started up after the data is sent. If the data is not acknowledged by the peer within the timeout time, the data will be resent.
TimeWait	Time Waiting timer, which is used to know that the peer has already received the acknowledgement of the connection termination request.
SendWnd	Timer of the transmission window, which is used to assure that the transmission window resume to the normal size after the TCP acknowledgement information is dropped
KeepAlive	Keep-alive timer, which is used to assure that the communication link is in normal state and the peer is still in the connection state It triggers the testing message to be sent for testing the state of the communication link and the peer.

After the timer is displayed, the sequence number of the TCP connection is displayed. TCP uses the sequence number to guarantee reliable and orderly data transmission. The local or remote host can control the traffic and send the acknowledgement information according to the sequence number.

iss: 29139463 snduna: 29139525 sndnxt: 29139525 sndwnd: 17520  
irs: 709124039 rcvnxt: 709205436 rcvwnd: 4380

Field	Description
iss:	Sequence number of original transmission
snduna:	Sequence number of the first byte in the data that is already sent but whose acknowledgement information has not been received
sndnxt:	Transmission sequence number of the first data in the data that is sent later
sndwnd:	TCP window size of the remote host
irs:	Original reception sequence number, that is, original transmission sequence number of the remote host
rcvnxt:	Reception sequence number that is acknowledged recently
rcvwnd:	TCP window size of the local host

The transmission time recorded by the local host is displayed afterwards. The system can adapt itself to different networks according to the transmission time.

SRTT: 15 ms, RXT: 2500 ms, RTV: 687 ms  
minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Field	Description
SRTT:	Round-trip time after smooth processing
RXT:	Retransmission timeout time
RTV:	Change value of the round-trip time
MinRXT:	Permissible minimum retransmission timeout time
MaxRXT:	Permissible maximum retransmission timeout time
ACK hold:	Maximum delay time when the acknowledgement is delayed for being sent together with the data

Datagrams (max data segment is 1460 bytes):

Rcvd: 102 (out of order: 0), with data: 92, total data bytes: 81396

Sent: 104 (retransmit: 0), with data: 31, total data bytes: 61

Field	Description
max data segment is	Maximum length of the data segment which is permitted by the connection
Rcvd:	Number of messages that the local host receives during the connection procedure, including the number of the misordered messages
with data:	Number of messages that contain valid data
total data bytes:	Number of data bytes contained by the message
Sent:	Number of messages that are sent or resent by the local host during the connection procedure
with data:	Number of messages that contain valid data
total data bytes:	Number of data bytes contained by the message

## Related Command

**show tcp brief**

**show tcp tcb**

### 3.1.19 show tcp brief

#### Syntax

It is used to display the brief information about the TCP connection.

**show tcp brief [all]**

#### Parameter

Parameter	Description
<b>all</b>	An optional parameter, which means that all ports are displayed

	If the parameter is not entered, the system does not display the ports in the LISTEN state.
--	---

## Command Mode

Management mode

## Example

```
switch#show tcp brief
TCB          Local Address      Foreign Address      State
0xE9ADC8     192.168.20.22:1023    192.168.20.124:513  ESTABLISHED
0xEA34C8     192.168.20.22:23     192.168.20.125:1472 ESTABLISHED
```

Field	Description
TCB	Internal identifier of the TCP connection
Local Address	Local IP address and the TCP port
Foreign Address	Remote IP address and the TCP port
State	State of the connection For details, refer to the description of the <b>show tcp</b> command.

## Related Command

**show tcp**

**show tcp tcb**

### 3.1.20 show tcp statistics

## Syntax

It is used to display the TCP statistics data.

**show tcp statistics**

## Parameter

The command has no parameter or keyword.

## Command Mode

Management mode

## Example

```
switch#show tcp statistics
Rcvd: 148 Total, 0 no port
0 checksum error, 0 bad offset, 0 too short
131 packets (6974 bytes) in sequence
0 dup packets (0 bytes)
0 partially dup packets (0 bytes)
```

0 out-of-order packets (0 bytes)  
 0 packets (0 bytes) with data after window  
 0 packets after close  
 0 window probe packets, 0 window update packets  
 0 dup ack packets, 0 ack packets with unsend data  
 127 ack packets (247 bytes)  
 Sent: 239 Total, 0 urgent packets  
 6 control packets  
 123 data packets (245 bytes)  
 0 data packets (0 bytes) retransmitted  
 110 ack only packets (101 delayed)  
 0 window probe packets, 0 window update packets  
 4 Connections initiated, 0 connections accepted, 2 connections established  
 3 Connections closed (including 0 dropped, 1 embryonic dropped)  
 5 Total rxmt timeout, 0 connections dropped in rxmt timeout  
 1 Keepalive timeout, 0 keepalive probe, 1 Connections dropped in keepalive

Field	Description
Rcvd:	Statistics data about the messages received by the routing switch
Total	Total number of the received messages
no port	Number of messages showing the destination port does not exist
checksum error	Number of messages showing that sum check is incorrect
bad offset	Number of messages showing that the data offset is incorrect
too short	Number of messages showing that the message length is less than the minimum effective length
packets in sequence	Number of messages that are received in turn
dup packets	Number of received duplicate messages
partially dup packets	Number of received messages that are partly duplicated
out-of-order packets	Number of misordered messages
packets with data after window	Number of messages whose data exceeds the reception window
packets after close	Number of messages that are received after the connection is closed
window probe packets	Number of received messages about window probe
window update packets	Number of received messages about window update
dup ack packets	Number of received messages that are duplicately acknowledged
ack packets with unsend data	Number of received messages that are acknowledged but has not been sent
ack packets	Number of received messages that are acknowledged
Sent	Statistics data about messages that are sent by the routing switch



Total	Total number of the transmitted messages
urgent packets	Number of the transmitted urgent messages
control packets	Number of the transmitted control messages (SYN, FIN or RST)
data packets	Number of the transmitted data messages
data packets retransmitted	Number of the retransmitted data messages
ack only packets	Number of the purely acknowledged messages
window probe packets	Number of the transmitted window probe messages
window update packets	Number of the transmitted window update messages
Connections initiated	Number of the locally initiated connections
connections accepted	Number of the locally received connections
connections established	Number of the locally established connections
Connections closed	Number of the locally closed connections
Total rxmt timeout	Total number of retransmission timeouts
Connections dropped in rxmit timeout	Number of the connections dropped because of retransmission timeout
Keepalive timeout	Number of Keepalive timeouts
keepalive probe	Number of the transmitted messages for keepalive probe
Connections dropped in keepalive	Number of the connections dropped because of Keepalive

## Related Command

### clear tcp statistics

## 3.1.21 show tcp tcb

### Syntax

It is used to display the state of a certain TCP connection.

### show tcp tcb address

### Parameter

Parameter	Description
<i>address</i>	TCB address of the TCP connection  TCB is an identifier of the TCP connection in the system, which can be obtained by the command <b>show tcp brief</b> .

## Command Mode

Management mode

## Example

For detailed explanation, refer to the command **show tcp**.

```
switch_config#show tcp tcb 0xea38c8
```

TCB 0xEA38C8

Connection state is ESTABLISHED, unread input bytes: 0

Local host: 192.168.20.22, Local port: 23

Foreign host: 192.168.20.125, Foreign port: 1583

Enqueued bytes for transmit: 0, input: 0 mis-ordered: 0 (0 packets)

Timer	Starts	Wakeups	Next(ms)
Retrans	4	0	0
TimeWait	0	0	0
SendWnd	0	0	0
KeepAlive	+5	0	6633000

```
iss: 10431492 snduna: 10431573 sndnxt: 10431573 sndwnd: 17440
irs: 915717885 rcvnxt: 915717889 rcvwnd: 4380
```

SRTT: 2812 ms, RXT: 18500 ms, RTV: 4000 ms

minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Datagrams (max data segment is 1460 bytes):

Rcvd: 5 (out of order: 0), with data: 1, total data bytes: 3

Sent: 4 (retransmit: 0), with data: 3, total data bytes: 80

## Related Command

**show tcp**

**show tcp brief**

## 3.2 IP Access List Configuration Commands

- deny
- ip access-group
- ip access-list
- permit
- show ip access-list

### 3.2.1 deny

#### Syntax

To set conditions in a named IP access list that will deny packets, use the deny command in access list configuration mode. To remove a deny condition from an access list, use the no form of this command.

**deny** *source* [*source-mask*] [**log**] [**location**]

**no deny** *source* [*source-mask*] [**log**]

**deny** protocol source source-mask destination destination-mask [[**precedence** precedence] [**tos** tos ] [**log**] [**offset-zero**] [**totalen**] [**time-range**] [**location**] [**tll**] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**offset-not-zero**] [**log** ]]

**no deny** protocol source source-mask destination destination-mask [[**precedence** precedence] [**tos** tos ] [**log**] [**offset-zero**] [**totalen**] [**time-range**] [**location**] [**tll**] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**offset-not-zero**] [**log** ]]

Internet Control Message Protocol (ICMP)

**deny icmp** source source-mask destination destination-mask [icmp-type] [**precedence** precedence] [**tos** tos] [**log**]

Internet Group Management Protocol (IGMP)

**deny igmp** source source-mask destination destination-mask [igmp-type] [**precedence** precedence] [**tos** tos] [**log**]

Transmission Control Protocol (TCP)

**deny tcp** source source-mask [operator port] destination destination-mask [operator port ] [**established**] [**precedence** precedence] [**tos** tos] [**log**]

User Datagram Protocol (UDP)

**deny udp** source source-mask [operator port] destination destination-mask [operator port] [**precedence** precedence] [**tos** tos] [**log**]

#### Parameter

Parameter	Description
<i>protocol</i>	Stands for the protocol name or IP protocol number. It can be one of these keywords icmp, igmp, igrp, ip, ospf, tcp or udp, or be an integer (protocol number) from 0 to 255. To match up with any Internet protocols (include ICMP, TCP and UDP), use the keyword ip. Some protocols allow further limitations as described later.
<i>source</i>	Stands for a source network or host number. There are two methods to designate the source: 32-bit binary number or a decimal number separated by four points. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
<i>source-mask</i>	Stands for the source address of the network mask. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.

<i>destination</i>	Number of the network or host to which the packet is being sent. There are two alternative ways to specify the destination:  Use a 32-bit quantity in four-part dotted-decimal format.  Use the any keyword as an abbreviation for the destination and destination-wildcard of 0.0.0.0 0.0.0.0.
destination-mask	Destination address network mask. Use the any keyword as an abbreviation for the destination address and destination address mask of 0.0.0.0 0.0.0.
<b>precedence</b> <i>precedence</i>	(Optional) Packets can be filtered by priority, as specified by a number from 0 to 7.
<b>tos</b> <i>tos</i>	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15.
operator	(Optional) Compares source or destination ports. The operations include the eq operation. If the operator follows the source parameter and the source-mask parameter, it must match up with the source port. If the operator follows the destination parameter and the destination-mask parameter, it must match up with the destination port.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535.
established	(Optional) One established connection only for TCP protocol. If the TCP data packet has ACK or RST, the match is established; otherwise, the TCP data packet will be initialized.
log	(Optional) log record.
location	Insert rule on the designated num location.

## Command Mode

### IP Access List Configuration Mode

## Usage Guidelines

Use this command following the ip access-list command to specify conditions under which a packet cannot pass the named access list. The time-range keyword allows you to identify a time range by name. The time-range, absolute, and periodic commands specify when this deny statement is in effect.

### Note:

After initially establishing an access list, any subsequent adding content (which can be input by terminal) is put in the bottom of the list.

## Example

The following example denies the network range 192.168.5.0:

```
ip access-list standard filter
deny 192.168.5.0 255.255.255.0
```

### Note:

IP access table is concluded in a cryptic deny rule.

## Related Commands

**ip access-group**  
**ip access-list**  
**permit**  
**show ip access-list**

## 3.2.2 ip access-group

### Syntax

To apply an access control list to control packet access, use the `ip access-group` command in the appropriate configuration mode. To remove the specified access group, use the `no` form of this command.

```
ip access-group {access-list-name}{in | out}
no ip access-group {access-list-name}{in | out}
```

### Parameter

Parameter	Description
<i>access-list-name</i>	Name of an IP access list as specified by an <code>ip access-list</code> command.
<b>in</b>	Use the access list in the ingress.
<b>out</b>	Use the access list in the egress.

## Command Mode

Interface configuration mode

## Usage Guidelines

Access lists can be applied on either outbound or inbound interfaces. For standard inbound access lists, after receiving a packet, the Cisco IOS software checks the source address of the packet against the access list. For extended access lists, the router also checks the destination access list. If the access list permits the address, the software continues to process the packet. If the access list rejects the address, the software discards the packet and returns an ICMP host unreachable message. If the specified access list does not exist, all packets are passed.

## Example

The following example applies list on packets outbound from Ethernet interface vlan1:

```
interface vlan 1
ip access-group filter out
```

## Related Commands

**ip access-list**  
**show ip access-list**

### 3.2.3 ip access-list

To define an IP access list by name or number, use the ip access-list command in global configuration mode. To remove the IP access list, use the no form of this command.

**ip access-list {standard | extended} name**  
**no ip access-list {standard | extended} name**

## Parameter

Parameter	Description
<b>standard</b>	Specifies a standard IP access list.
<b>extended</b>	Specifies an extended IP access list.
<i>name</i>	Name of the access list. It is a character string with no more than 20 characters.

## Default

No IP access list is defined.

## Command Mode

Global configuration

## Usage Guidelines

Use this command to configure a named or numbered IP access list. This command will place the router in access-list configuration mode, where you must define the denied or permitted access conditions with the deny or permit commands.

## Example

The following example defines a standard access list:

```
ip access-list standard filter
deny 192.168.1.0 255.255.255.0
```

permit any

## Related Commands

**deny**

**ip access-group**

**permit**

**show ip access-list**

## 3.2.4 permit

### Syntax

To set conditions to allow a packet to pass a named IP access list, use the permit command in access list configuration mode. To remove a permit condition from an access list, use the no form of this command.

**permit source** [*source-mask*] [**log**] [*location*]

**no permit source** [*source-mask*] [**log**]

**permit protocol source** *source-mask* **destination** *destination-mask* [[**precedence** *precedence*] [**tos** *tos*] [**log**] [**offset-zero**] [**totalen**] [**time-range**] [*location*] [**ttl**] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**offset-not-zero**] [**log** ]]

**no permit protocol source** *source-mask* **destination** *destination-mask* [[**precedence** *precedence*] [**tos** *tos*] [**log**] [**offset-zero**] [**totalen**] [**time-range**] [*location*] [**ttl**] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**offset-not-zero**] [**log** ]]

Internet Control Message Protocol (ICMP)

**permit icmp source** *source-mask* **destination** *destination-mask* [*icmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

Internet Group Management Protocol (IGMP)

**permit igmp source** *source-mask* **destination** *destination-mask* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

Transmission Control Protocol (TCP)

**permit tcp source** *source-mask* [**operator** *port*] **destination** *destination-mask* [**operator** *port*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**log**]

User Datagram Protocol (UDP)

**permit udp source** *source-mask* [**operator** *port*] **destination** *destination-mask* [**operator** *port*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

### Parameter

Parameter	Description
<i>protocol</i>	Stands for the protocol name or IP protocol number. It can be one of these keywords icmp, igmp, igmp, ip, ospf, tcp or udp, or be an integer (protocol number) from 0 to 255. To match up with any Internet protocols (include ICMP, TCP and UDP), use the

	keyword ip. Some protocols allow further limitations as described later.
source	Stands for a source network or host number. There are two methods to designate the source: 32-bit binary number or a decimal number separated by four points. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
source-mask	Stands for the source address of the network mask. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
destination	Number of the network or host to which the packet is being sent. There are two alternative ways to specify the destination:  Use a 32-bit quantity in four-part dotted-decimal format.  Use the any keyword as an abbreviation for the destination and destination-wildcard of 0.0.0.0 0.0.0.0.
destination-mask	Destination address network mask. Use the any keyword as an abbreviation for the destination address and destination address mask of 0.0.0.0 0.0.0.0.
tos tos	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15.
operator	(Optional) Compares source or destination ports. The operations include the eq operation. If the operator follows the source parameter and the source-mask parameter, it must match up with the source port. If the operator follows the destination parameter and the destination-mask parameter, it must match up with the destination port.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535.
established	(Optional) One established connection only for TCP protocol. If the TCP data packet has ACK or RST, the match is established; otherwise, the TCP data packet will be initialized.
log	(Optional) log record.

## Command Mode

### IP access list configuration

## Usage Guidelines

Use this command following the ip access-list command to define the conditions under which a packet passes the named access list.



The time-range keyword allows you to identify a time range by name. The time-range, absolute, and periodic commands specify when this permit statement is in effect.

**Note:**

After initially establishing an access list, any subsequent adding content (which can be input by terminal) is put in the bottom of the list.

### Example

The following example permits network range 192.168.5.0:

```
ip access-list standard filter
permit 192.168.5.0 255.255.255.0
```

**Note:**

IP access table is concluded in a cryptic deny rule.

### Related Commands

**deny**

**ip access-group**

**ip access-list**

**show ip access-list**

## 3.2.5 show ip access-lists

### Syntax

To display the contents of all current IP access lists, use the show ip access-list command in user EXEC or privileged EXEC mode.

**show ip access-list** [*access-list-name*]

### parameter

Parameter	Description
<i>access-list-name</i>	Name of the IP access list. It is a character string of 20 characters.

### Default

All standard and extended IP access lists are displayed.

### Command Mode

EXEC

### Usage Guidelines

The show ip access-list command provides output identical to the show access-lists command, except that it is IP-specific and allows you to specify a particular access list.

## Example

The following is sample output from the **show ip access-list** command when the name of a specific access list is not requested:

```
Switch# show ip access-list
ip access-list standard aaa
permit 192.2.2.1
permit 192.3.3.0 255.255.255.0
ip access-list extended bbb
permit tcp any any eq www
permit ip any any
```

The following is sample output from the **show ip access-list** command when the name of a specific access list is requested:

```
ip access-list extended bbb
permit tcp any any eq www
permit ip any any
```

## 3.3 IP Access List Configuration Commands

### IP Access List Configuration Commands Based on Physical Interface

- deny
- ip access-group
- ip access-list
- permit
- show ip access-list

### 3.3.1 deny

#### Syntax

To set conditions in a named IP access list that will deny packets, use the **deny** command in access list configuration mode. To remove a deny condition from an access list, use the **no** form of this command.

**deny source** [*source-mask*] [**log**] [**location**]

**no deny source** [*source-mask*] [**log**]

**deny** protocol source source-mask destination destination-mask [[**precedence** precedence] [**tos** tos ] [**log**] [**offset-zero**] [**totalen**] [**time-range**] [**location**] [**ttl**] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**offset-not-zero**] [**log** ]]

**no deny** protocol source source-mask destination destination-mask [[**precedence** precedence] [**tos** tos ] [**log**] [**offset-zero**] [**totalen**] [**time-range**] [**location**] [**ttl**] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**offset-not-zero**] [**log** ]]

Internet Control Message Protocol (ICMP)

**deny icmp** source source-mask destination destination-mask [**icmp-type**] [**tos** tos]

Internet Group Management Protocol (IGMP)

**deny igmp** source source-mask destination destination-mask [**igmp-type**] [**tos** tos]

### Transmission Control Protocol (TCP)

**deny tcp** source source-mask [operator port] destination destination-mask [operator port] [**tos** tos]

### User Datagram Protocol (UDP)

**deny udp** source source-mask [operator port] destination destination-mask [operator port] [**tos** tos]

### Parameter

Parameter	Description
<i>protocol</i>	Stands for the protocol name or IP protocol number. It can be one of these keywords icmp, igmp, igmp, ip, ospf, tcp or udp, or be an integer (protocol number) from 0 to 255. To match up with any Internet protocols (include ICMP, TCP and UDP), use the keyword ip. Some protocols allow further limitations as described later.
source	Stands for a source network or host number. There are two methods to designate the source: 32-bit binary number or a decimal number separated by four points. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
source-mask	Stands for the source address of the network mask. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
destination	Number of the network or host to which the packet is being sent. There are two alternative ways to specify the destination:  Use a 32-bit quantity in four-part dotted-decimal format.  Use the any keyword as an abbreviation for the destination and destination-wildcard of 0.0.0.0 0.0.0.0.
destination-mask	Destination address network mask. Use the any keyword as an abbreviation for the destination address and destination address mask of 0.0.0.0 0.0.0.0.
<b>tos</b> tos	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15.
operator	(Optional) Compares source or destination ports. The operations include the eq operation. If the operator follows the source parameter and the source-mask parameter, it must match up with the source port. If the operator follows the destination parameter and the destination-mask parameter, it must match up with the destination port.
port	(Optional) The decimal number or name of a TCP or UDP port. A

	port number is a number from 0 to 65535.
--	--

## Command Mode

IP Access List Configuration Mode

## Usage Guidelines

Use this command following the `ip access-list` command to specify conditions under which a packet cannot pass the named access list. The time-range keyword allows you to identify a time range by name. The time-range, absolute, and periodic commands specify when this deny statement is in effect.

### Note:

After initially establishing an access list, any subsequent adding content (which can be input by terminal) is put in the bottom of the list.

## Example

The following example denies the network range 192.168.5.0:

```
ip access-list standard filter
deny 192.168.5.0 255.255.255.0
```

### Note:

IP access table is concluded in a cryptic deny rule.

## Related Commands

**ip access-group**  
**ip access-list**  
**permit**  
**show ip access-lists**

### 3.3.2 ip access-group

## Syntax

To apply an access control list to control packet access, use the `ip access-group` command in the appropriate configuration mode. To remove the specified access group, use the `no` form of this command.

**[no] ip access-group** *[access-list-name]*

## Parameter

Parameter	Description
<i>access-list-name</i>	Name of an IP access list as specified by an <code>ip access-list</code> command.

## Command Mode

Interface configuration mode

## Usage Guidelines

Access lists can be applied on either outbound or inbound interfaces. For standard inbound access lists, after receiving a packet, the Cisco IOS software checks the source address of the packet against the access list. For extended access lists, the router also checks the destination access list. If the access list permits the address, the software continues to process the packet. If the access list rejects the address, the software discards the packet and returns an ICMP host unreachable message. If the specified access list does not exist, all packets are passed.

## Example

The following example applies list on packets outbound from Ethernet interface g0/10:

```
interface g0/10
ip access-group filter
```

## Related Commands

**ip access-list**  
**show ip access-lists**

### 3.3.3 ip access-list

## Syntax

To define an IP access list by name or number, use the `ip access-list` command in global configuration mode. To remove the IP access list, use the `no` form of this command.

**ip access-list {standard | extended} name**  
**no ip access-list {standard | extended} name**

## Parameter

Parameter	Description
<b>standard</b>	Specifies a standard IP access list.
<b>extended</b>	Specifies an extended IP access list.
<i>name</i>	Name of the access list. It is a character string with no more than 20 characters.

## Default

No IP access list is defined.

## Command Mode

Global configuration

## Usage Guidelines

Use this command to configure a named or numbered IP access list. This command will place the router in access-list configuration mode, where you must define the denied or permitted access conditions with the deny or permit commands.

## Example

The following example defines a standard access list:

```
ip access-list standard filter
deny 192.168.1.0 255.255.255.0
permit any
```

## Related Commands

**deny**  
**ip access-group**  
**permit**  
**show ip access-lists**

### 3.3.4 permit

#### Syntax

To set conditions to allow a packet to pass a named IP access list, use the permit command in access list configuration mode. To remove a permit condition from an access list, use the no form of this command.

**permit source** [*source-mask*] [**log**] [**location**]

**no permit source** [*source-mask*] [**log**]

**permit protocol source** *source-mask destination destination-mask* [[**precedence** precedence] [**tos** tos ] [**log**] [**offset-zero**] [**totalen**] [**time-range**] [**location**] [**ttl**] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**offset-not-zero**] [**log** ]]

**no permit protocol source** *source-mask destination destination-mask* [[**precedence** precedence] [**tos** tos ] [**log**] [**offset-zero**] [**totalen**] [**time-range**] [**location**] [**ttl**] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**offset-not-zero**] [**log** ]]

Internet Control Message Protocol (ICMP)

**permit icmp source** *source-mask destination destination-mask* [*icmp-type*] [**tos** tos]

Internet Group Management Protocol (IGMP)

**permit igmp source** *source-mask destination destination-mask* [*igmp-type*] [**tos** tos]

Transmission Control Protocol (TCP)

**permit tcp source** *source-mask* [**operator** *port*] **destination** *destination-mask* [**operator** *port*] [**tos** *tos*]

User Datagram Protocol (UDP)

**permit udp source** *source-mask* [**operator** *port* [*port*]] **destination** *destination-mask* [**tos** *tos*]

## Parameter

Parameter	Description
<i>protocol</i>	Stands for the protocol name or IP protocol number. It can be one of these keywords icmp, igmp, igmp, ip, ospf, tcp or udp, or be an integer (protocol number) from 0 to 255. To match up with any Internet protocols (include ICMP, TCP and UDP), use the keyword ip. Some protocols allow further limitations as described later.
<i>source</i>	Stands for a source network or host number. There are two methods to designate the source: 32-bit binary number or a decimal number separated by four points. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
<i>source-mask</i>	Stands for the source address of the network mask. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
<i>destination</i>	Number of the network or host to which the packet is being sent. There are two alternative ways to specify the destination:  Use a 32-bit quantity in four-part dotted-decimal format.  Use the any keyword as an abbreviation for the destination and destination-wildcard of 0.0.0.0 0.0.0.0.
<i>destination-mask</i>	Destination address network mask. Use the any keyword as an abbreviation for the destination address and destination address mask of 0.0.0.0 0.0.0.0.
<b>tos</b> <i>tos</i>	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15.
<i>icmp-type</i>	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
<i>igmp-type</i>	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15.
<i>operator</i>	(Optional) Compares source or destination ports. The operations include the eq operation. If the operator follows the source parameter and the source-mask parameter, it must match up with the source port. If the operator follows the destination parameter and the destination-mask parameter, it must match up with the destination port.
<i>port</i>	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535.

## Command Mode

IP access list configuration

## Usage Guidelines

Use this command following the `ip access-list` command to define the conditions under which a packet passes the named access list.

The `time-range` keyword allows you to identify a time range by name. The `time-range`, `absolute`, and `periodic` commands specify when this permit statement is in effect.

### Note:

After initially establishing an access list, any subsequent adding content (which can be input by terminal) is put in the bottom of the list.

## Example

The following example permits network range 192.168.5.0:

```
ip access-list standard filter
permit 192.168.5.0 255.255.255.0
```

### Note:

IP access table is concluded in a cryptic deny rule.

## Related Commands

**deny**

**ip access-group**

**ip access-list**

**show ip access-list**

## 3.3.5 show ip access-lists

### Syntax

To display the contents of all current IP access lists, use the `show ip access-list` command in user EXEC or privileged EXEC mode.

**show ip access-list** [*access-list-name*] [**config-list** | **merge-list** | **both-list**]

### Parameter

Parameter	Description
<i>access-list-name</i>	Name of the IP access list. It is a character string of 20 characters.
<b>config-list</b>	Displays the original config list.
<b>merge-list</b>	Displays the merge list.
<b>both-list</b>	Displays the config list and the merge list.



## Default

All standard and extended IP access lists are displayed.

## Command Mode

EXEC

## Usage Guidelines

The `show ip access-list` command provides output identical to the `show access-lists` command, except that it is IP-specific and allows you to specify a particular access list.

## Example

The following is sample output from the **show ip access-list** command when the name of a specific access list is not requested:

```
Switch# show ip access-list
ip access-list standard aaa
permit 192.2.2.1
permit 192.3.3.0 255.255.255.0
ip access-list extended bbb
permit tcp any any eq 25
permit ip any any
```

The following is sample output from the `show ip access-list` command when the name of a specific access list is requested:

```
ip access-list extended bbb
permit tcp any any eq 25
permit ip any any
```