Security

absolute time-range

To configure an absolute time range that specifies when an access control list (ACL) is in effect, use the **absolute** command in the time-range configuration mode. To remove the absolute time-range, use the **no** form of the command.

[no]absolute [start *time-range*] [end*time-range*]

Syntax Description

time-range	Specifies the time in the format of HH:MM:SS YYYY/MM/DD

Command Modes Global Configuration (config)

Command Default None

Example

```
Device#configure terminal
Device(config)#time-range weekends
Device(config-timerange-weekends)#absolute start 04:50:30 2020/04/01 end 09:50:40 2020/04/30
```

access-limit

To enable or disable the number limit of authentication users in the domain and set the number limit of allowed users, use the **access-limit** commmand in AAA configuration mode.

access-limit {**enable** *allowed-user-number-limit* | **disable**}

Syntax Description

enable	Enables the number limit of authentication users in the domain
allowed-user-number-limit	Sets the number limit of allowed users in the domain. The range is from 1 to 640.
disable	Disables the number limit of authentication users in the domain.

Command Modes

AAA configuration (config-aaa)

Example

This example shows how to enable the number limit of authentication users in the domain and set the number limit of allowed users:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# domain eee
Device(config-aaa-domain-eee)# exit
Device(config-aaa)# default domain-name enable eee
Device(config-aaa)# domain eee
Device(config-aaa-domain-eee)# access-limit enable 3
 Succeed to set MaxLinks of domain.
```

Example

This example shows how to disable the number limit of authentication users in the domain and set the number limit of allowed users:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# default domain-name enable eee
 Succeed in setting default domain.
Device(config-aaa)# domain eee
Device(config-aaa-domain-eee)# access-limit disable
 Succeed to disable access limit of domain.
```

access-list match-order

To configure the access control list (ACL) matching order, use the **access-list match-order** command in the global configuration mode. The matching order decides which rule is executed.

access-list *acl-num*match-order {auto |config}

Syntax Description

auto	Matches the ACL rules according to the depth-first rule, wherein the longest subitem in a rule takes priority. The longest subset of a rule is matched first before the rule.
config	Matches the ACL rules according to the configuration order.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

An ACL consists of multiple permit or deny rules. The rules may overlap or conflict. In such cases, the matching order decides which rule is executed.

Example

```
Device#configure terminal
Device(config)#access-list 2 match-order config
```

access-group

To activate an access control list that is already defined, use the **access-group** command in the global configuration mode.

access-group [**ip-group** [*name* | *number*]] [**link-group** [*name* | *number*]] [**subitem** *number*]

Syntax Description

ip-group [*name* | *number*]	Specifies a predefined Standard ACL or Extended ACL.
link-group [*name* | *number*]	Specifies a predefined Layer 2 ACL.
subitem *number*	Specifies the sub item number in the ACL

Command Modes

Global Configuration (config)

Command Default

None

Usage Guidelines

After defining an Access Control List (ACL), it has to be activated to take effect. Use the **access-group ip-group** command to activate a Standard ACL or an Extended ACL. Use the **access-group link-group** command to activate a Layer 2 ACL.

Example

The following example creates a standard access control list (ACL), 10, and activates the subitem number 1 of the ACL.

```
Device#configure terminal
Device(config)#access-list 10 deny any

Device(config)#access-list 10 permit 10.1.1.5 0
Device(config)#access-group ip-group 10
```

access-list numbered standard

To define a numbered Standard Access Control List (ACL), use the **access-list** *number* command in the global configuration mode.

```
access-list num{permit |deny} { source-ipv4 | ipv6-source-prefix | any | ipv6any}
[ time-range timerange-name]
```

Syntax Description

permit	Specifies that the rule defined by the ACL is permitted.
deny	Specifies that the rule defined by the ACL is not permitted.
source-ipv4	Specifies the IPv4 address of the source host.
ipv6-source-prefix	Specifies the IPv6 prefix of the source host.
ipv6any	Specifies any IPv6 host
any	Specifies any IPv4 host
time-range*timerange-name*	Defines the specific time range to implement the ACL.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

The ACL is identified by the number assigned to it. You can create an ACL and assign a number to it. If you don't specify a number, the system assigns a number to the created ACL. For a Standard ACL, the numbers range from 1 through 99. You can create upto 99 Standard ACLs.

Example

```
Device#configure terminal
Device(config)#access-list 10 permit any
```

access-list standard

To create a named Standard Access Control List, use the **access-list standard** command in the global configuration mode.

```
access-list standard {num|name }[ match-order { auto | config }]
```

Syntax Description

num	Specifies a standard ACL. Values can range from 1 through 99.
name	Specifies a name for the ACL. The name is a string of alphanumeric characters, upto 32 characters in length.
match-order	Defines a matching order for the entries in the ACL.
config	Matches the ACL rules according to the configuration order in the list.
auto	Matches the ACL rules according to the depth-first rule, wherein the longest subitem in a rule takes priority. The longest subset of a rule is matched first before the rule.

Command Default

None

Command Modes

Global configuration (config)

Example

```
Device#configure terminal
Device(config)#access-list standard stdacl
```

accounting-on

To configure accounting-on fucntion, use the **accounting-on** command in AAA configuration mode.

accounting-on {**enable** *packet-number* | **disable**}

Syntax Description

enable	Enables accounting-on function.
packet-number	The number of accounting-on packets sent. The range is 1 to 255.
disable	Disables accounting-on function.

Command Modes

AAA configuration (config-aaa)

Example

This example shows how to enable the accounting-on function:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# accounting-on enable 10
 configure success
```

acct-secret-key

To configure the shared key of the secondary RADIUS server, use the **acct-secret-key** command in AAA configuration mode. To delete the configured shared key of the secondary RADIUS server, use the **no** form of the command.

acct-secret-key*key*

no acct-secret-key

Syntax Description

key	The shared secret key.

Command Modes

AAA Configuration (config-aaa)

Example

This example shows how to configure the shared key of a secondary RADIUS server using the **acct-secret-key** command:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# acct-secret-key 1
 Modify secret key of RADIUS configuration successfully
```

anti-dos ip fragment

To configure a new threshold value for IP fragmentations, use the **anti-dos ip fragment** command in global configuration mode. To restore the default threshold value, use the **no** form of the command.

anti-dos ip fragment *threshold-value*

no anti-dos ip fragment

Syntax Description

threshold-value	The maximum number of allowed IP fragmentations. The range is 0 to 800. The default value is 800.

Command Modes

Global Configuration (config)

Example

This example shows how to configure a new threshold value for IP fragmentations using the **anti-dos ip fragment** command:

```
Device> enable
Device# configure terminal
Device(config)# anti-dos ip fragment 100
```

anti-dos ip ttl

To enable TTL monitoring and anti-TTL attack, use the **anti-dos ip ttl** command in global configuration mode. To disable TTL monitoring and anti-TTL attack, use the **no** form of the command.

anti-dos ip ttl

no anti-dos ip ttl

Command Default

Messages with TTL with a value of 0 are discarded.

Command Modes

Global Configuration (config)

Example

This example shows how to enable TTL monitoring using the **anti-dos ip ttl** command:

```
Device> enable
Device# configure terminal
Device(config)# anti-dos ip ttl
```

arp anti-spoofing

To enable ARP anti-spoofing, use the **arp anti-spoofing** command in global configuration mode. To disable ARP anti-spoofing, use the **no** form of the command.

arp anti-spoofing

no arp anti-spoofing

Command Modes

Global Configuration (config)

Example

This example shows how to enable ARP anti-spoofing using the **arp anti-spoofing** command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-spoofing
Device(config)#
```

arp anti-spoofing deny-disguiser

To enable ARP gateway anti-spoofing, use the **arp anti-spoofing deny-disguiser** command in global configuration mode. To disable ARP gateway anti-spoofing, use the **no** form of the command.

arp anti-spoofing deny-disguiser

no arp anti-spoofing deny-disguiser

Command Modes

Global Configuration (config)

Example

This example shows how to enable ARP gateway anti-spoofing using the **arp anti-spoofing deny-disguiser** command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-spoofing deny-disguiser
Device(config)#
```

arp anti-spoofing unknown

To enable ARP anti-spoofing and configure the device to flood or disable unknown packets, use the **arp anti-spoofing unknown** command in global configuration mode.

arp anti-spoofing unknown {**flood** | **disable**}

Syntax Description

flood	Floods the unknown packets.
disable	Disables the unknown packets.

Command Modes

Global Configuration (config)

Example

This example shows how to flood the unknown packets using the **arp anti-spoofing unknown flood** command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-spoofing unknown flood
Device(config)#
```

Example

This example shows how to disable the unknown packets using the **arp anti-spoofing unknown disable** command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-spoofing unknown disable
Device(config)#
```

arp anti-spoofing valid-check

To enable ARP anti-spoofing and configure source MAC address consistency inspection, use the **arp anti-spoofing valid-check** command in global configuration mode. To disable source MAC address consistency inspection, use the **no** form of the command.

arp anti-spoofing valid-check

no arp anti-spoofing valid-check

Command Modes

Global Configuration (config)

Example

This example shows how to enable source MAC address consistency inspection using the **arp anti-spoofing valid-check** command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-spoofing valid-check
Device(config)#
```

arp anti-flood

To enable ARP anti-flooding attack and configure its parameters on all ports, use the **arp anti-flood** command in global configuration mode.

To enable ARP anti-flooding attack and configure its parameters on a specific port, use the **arp anti-flood** command in interface configuration mode.

To disable ARP anti-flooding attack, use the **no** form of the command.

arp anti-flood [[**action** {**deny-all** | **deny-arp**}] [**threshold** *threshold-value*] | **recover** {*mac-address* | **all**} | **recover-time** *time*]

no arp anti-flood [**recover-time** | **threshold**]

Syntax Description

action deny-all	Adds the host to a blackhole address list and discards all packets.
action deny-arp	Adds the host to a blackhole address list and discards only ARP packets.
threshold *threshold-value*	Configures the ARP anti-flood threshold value. The default value is 16 packets per second.
recover *mac-address*	Manually restores the host with the specified MAC address to transmit again.
recover all	Manually restores all the hosts to transmit again.
recover-time *time*	Defines the recovery time interval after which a host is allowed to transmit again. The recovery interval is 0 to 1440 minutes. The default value is 10 minutes.

Command Modes

Global configuration (config)
Interface configuration (config-if)

Example

This example shows how to configure ARP anti-flooding attack using the **arp anti-flood** command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-flood
Device(config)#
```

Example

This example shows how to add the host to a blackhole address list and discard all packets using the **arp anti-flood action deny-all** command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-flood action deny-all
Device(config)#
```

Example

This example shows how to configure ARP anti-flooding threshold value using the **arp anti-flood threshold** *threshold-value* command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-flood threshold 30
Device(config)#
```

Example

This example shows how to manually restore the host to transmit again using the **arp anti-flood recover** command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-flood recover 00:00:00:00:32:33
Device(config)#
```

Example

This example shows how to define the recovery time interval after which a host is allowed to transmit again using the **arp anti-flood recover-time** *time* command:

```
Device> enable
Device# configure terminal
Device(config)# arp anti-flood recover-time 100
Device(config)#
```

channel-group spanning-tree cost

To configure the path cost of an STP aggregation group, use the **channel-group** *group-id* **spanning-tree cost** command in global configuration mode. To restore the default path cost of an STP aggregation group, use the **no** form of the command.

channel-group *group-id* **spanning-tree cost** *path-cost*

no channel-group *group-id* **spanning-tree cost**

Syntax Description

group-id	The channel group ID. The range is 0 to 5.
path-cost	The path cost of the aggregation group. The range is 1 to 200000000.

Command Modes

Global configuration (config)

Example

This example shows how to configure the path cost of an aggregation group using the **channel-group** *group-id* **spanning-tree cost** command:

```
Device> enable
Device# configure terminal
Device(config)# channel-group 1 spanning-tree cost 2000
Device(config)#
```

clear cpu-classification

To clear the CPU packet classification statistics, run the **clear cpu-classification** command in global configuration mode.

clear cpu-classification interface {**ethernet** | **gpon**}*slot-number/port-number*

Syntax Description

slot-number/port-number	The port ID. - *slot-number*: - GPON: The value is 0. - GE Ethernet: The value is 1. - 10GE Ethernet: The value is 2. - *port-number*: - GPON: The range is from 1 to 8. - GE Ethernet: The range is from 1 to 4. - 10GE Ethernet: The range is from 1 to 2.

Command Default

None

Command Modes

Global configuration (config)

Example

This example shows how to clear the CPU packet classification statistics:

```
Device> enable
Device# configure terminal
Device(config)# clear cpu-classification interface ethernet 1/3
Clear packets sent to cpu classification statistics successfully
```

clear cpu-statistics

To clear the port statistics, use the **clear cpu-statistics** command in privileged EXEC and global configuration modes.

clear cpu-statistics

Command Default

None

Command Modes

Privileged EXEC (#)
Global configuration (config)

Examples

This example shows how to clear the port statistics.

```
Device> enable
Device# configure terminal
Device(config)# clear cpu-statistics
Clear packet sent to cpu statistic information successfully
```

cpu-car

To configure the CPU-car rate limit for packets, use the **cpu-car** command in global configuration mode. To restore the default CPU-car rate limit, use the **no** form of the command.

cpu-car *rate-limit*

no cpu-car

Syntax Description

rate-limit	Configures the CPU-car rate limit. The range is 1 to 10000 packets per second. The default value is 4000 packets per second.

Command Modes

Global configuration (config)

Example

This example shows how to configure real time accounting using the **realtime-account** command:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# realtime-account interval 25
 Modify realtime_acct configuration of radius server successfully.
```

dhcp anti-attack

To enable DHCP packet monitoring and configure the monitoring parameters on all ports, use the **dhcp anti-attack** command in global configuration mode.

To enable DHCP packet monitoring and configure the monitoring parameters on a specific port, use the **dhcp anti-attack** command in interface configuration mode.

To disable DHCP packet monitoring and restore the parameters to their default values, use the **no** form of the command.

dhcp anti-attack [[**action** {**deny-all** | **deny-dhcp**}] [**threshold** *threshold-value*] | [**bind blackhole** | **recover**] {*mac-address* | **all**} | **recover-time** *time*]

no dhcp anti-attack [**recover-time** | **threshold**]

Syntax Description

action deny-all	Adds the host to a blackhole address list and discards all packets.
action deny-dhcp	Adds the host to a blackhole address list and discards only DHCP packets.
threshold *threshold-value*	Configures the rate threshold for DHCP packets globally. The default value is 16 packets per second.
bind blackhole *mac-address*	Binds the dynamic MAC address generated by DHCP with the static MAC address for the specified MAC address in the blackhole address list.
bind blackhole all	Binds the dynamic MAC address generated by DHCP with the static MAC address for all the MAC addresses in the blackhole address list.
recover *mac-address*	Manually restores the table items for the host with the specified MAC address.
recover all	Manually restores the table items for all the hosts .
recover-time *time*	Defines the recovery time interval. The recovery interval is 0 to 1440 minutes. The default value is 10 minutes.

Command Modes

Global configuration (config)
Interface configuration (config-if)

Example

This example shows how to configure DHCP packet monitoring using the **dhcp anti-attack** command:

```
Device> enable
Device# configure terminal
Device(config)# dhcp anti-attack
Device(config)#
```

Example

This example shows how to configure DHCP packet monitoring and discard all packets using the **dhcp anti-attack action deny-all** command:

```
Device> enable
Device# configure terminal
Device(config)# dhcp anti-attack action deny-all
Device(config)#
```

Example

This example shows how to configure the threshold value for DHCP packet globally using the **dhcp anti-attack threshold** command:

```
Device> enable
Device# configure terminal
Device(config)# dhcp anti-attack threshold 10
Device(config)#
```

Example

This example shows how to manually restore the table items for the host using the **dhcp anti-attack recover** command:

```
Device> enable
Device# configure terminal
Device(config)# dhcp anti-attack recover all
Device(config)#
```

Example

This example shows how to configure recovery time interval using the **dhcp anti-attack recover-time** command:

```
Device> enable
Device# configure terminal
Device(config)# dhcp anti-attack recover-time 100
Device(config)#
```

discard-bpdu

To enable the local discard of external BPDU messages, use the **discard-bpdu** command in global configuration mode. To disable the local discard of external BPDU messages, use the **no** form of the command.

discard-bpdu

no discard-bpdu

Command Modes

Global configuration (config)

Example

This example shows how to enable the local discard of external BPDU messages using the **discard-bpdu** command:

```
Device> enable
Device# configure terminal
Device(config)# discard-bpdu
Enable discard bpdu successfully.
```

access-list extended name

To create a named Extended Access Control List, use the **access-list extended** command in the global configuration mode.

access-list extended {*num*|*name* }[match-order { auto | config }]

Syntax Description

num	Specifies an extended ACL. Values can range from 100 through 199.
name	Specifies a name for the ACL. The name is a string of alphanumeric characters, upto 32 characters in length.
match-order	Defines a matching order for the entries in the ACL.
config	Matches the ACL rules according to the configuration order in the list.
auto	Matches the ACL rules according to the depth-first rule, wherein the longest subitem in a rule takes priority. The longest subset of a rule is matched first before the rule.

Command Default

None

Command Modes

Global configuration (config)

Example

```
Device#configure terminal
Device(config)#access-list extended extacl match-order auto
```

access-list numbered extended

To define a numbered Extended Access Control List (ACL), use the **access-list** *number* command in the global configuration mode.

```
access-list number {permit |deny} [protocol ] [established] { source-ipv4 |
ipv6-source-prefix | any | ipv6any}[source-port-wildcard]{ dest-ipv4 | ipv6-dest-prefix | any
| ipv6any}[dest-port-wildcard][ icmp type icmp-code][igmp-type] [ traffic-class traffic-class
][ precedence precedence ][ tos tos ][ dscp dscp][ fragments ][ time-range
time-range ]
```

Syntax Description

permit	Specifies that the rule defined by the ACL is permitted.
deny	Specifies that the rule defined by the ACL is not permitted.
protocol	Specifies the type of Layer 2 protocol. It is in the range of 1 through 255 by number. Select from GRE, ICMP, IGMP, IPinIP, OSPF, TCP, UDP, and ICMPv6 to specify the protocol by name.
established	Defines the SYN flag in TCP. A value 1 indicates that the flag is active. This is applicable only if the *protocol* is tcp.
source-ipv4	Specifies the IPv4 address of the source host.
ipv6-source-prefix	Specifies the IPv6 prefix of the source host.
ipv6any	Specifies any IPv6 host
dest-ipv4	Specifies the IPv4 address of the destination host.
ipv6-dest-prefix	Specifies the IPv6 prefix of the destination host.
any	Specifies any host.
icmp type icmp-code	Specifies the type of ICMP protocol packet. It is valid only when protocol is configured as **icmp** or **icmpv6**.
igmp-type	Specifies the type of IGMP protocol packet. It is valid only when protocol is configured as **igmp**.
traffic-class	Specifies the traffic class for IPv6.
precedence	Specifies the precedence priority. IP precedence ranges from 0 through 7.
tos	Specifies the Type of Service (ToS) priority. The values range from 0 through 15.
dscp	Specifies the Differentiated Services Code Point (DSCP) priority value.
fragments	Specifies that the ACL rule is valid for non-first fragmented packets. This helps prevent fragment packet attacks.

time-range*timerange-name*	Defines the specific time range to implement the ACL.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

The ACL is identified by the number assigned to it. You can create an ACL and assign a number to it. If you don't specify a number, the system assigns a number to the created ACL. For an Extended ACL, the numbers range from 100 through 199. You can create upto 100 Extended ACLs.

Example

```
Device#configure terminal
Device(config)#access-list 101 permit tcp 10.0.0.1 0 ftp any
```

host-guard bind ip

To configure host protection on a port, use the **host-guard bind ip** command in global configuration mode. To disable host protection on a port, use the **no** form of the command.

host-guard bind ip *ip-address* **interface ethernet** *slot_number/port_number* [**[to ethernet** *slot_number/port_number*]

no host-guard bind ip *ip-address* **interface ethernet** *slot_number/port_number* [**[to ethernet** *slot_number/port_number*]

Syntax Description

to	Displays the information for a range of ports. If you use the **to** keyword, specify the same port type before and after the keyword.
slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to 8. • GE Ethernet: The range is from 1 to 4. • 10GE Ethernet: The range is from 1 to 2.

Command Modes

Global configuration (config)

Example

This example shows how to configure host protection on a port using the **host-guard bind ip** command:

```
Device> enable
Device# configure terminal
Device(config)# host-guard bind ip 10.10.10.1 interface ethernet 1/3
 Add host guard entry successfully.
```

ip route

To add a static IP route to the routing table, use the **ip route** command in the global configuration mode. To remove a static IP route from the routing table, use the **no** form of the command.

ip route *dest-ip mask* [*gate-ip*]

no ip route *dest-ip mask* [*gate-ip*]

Syntax Description

dest-ip	The destination address of the static route that needs to be added.
mask	The mask of the destination address.
gate-ip	The next-hop address of the static route.

Command Modes

Global configuration (config)

Example

This example shows how to add a static IP route to the routing table using the **ip route** command:

```
Device> enable
Device# configure terminal
Device(config)# ip route 10.10.10.10 255.255.0.0 10.0.11.254
```

access-list link name

To create a named Layer 2 Access Control List (ACL), use the **access-list link** command in the global configuration mode.

```
access-list link {num|name }[ match-order { auto | config }]
```

Syntax Description

num	Specifies an extended ACL. Values can range from 200 through 299.
name	Specifies a name for the ACL. The name is a string of alphanumeric characters, upto 32 characters in length.
match-order	Defines a matching order for the entries in the ACL.
config	Matches the ACL rules according to the configuration order in the list.
auto	Matches the ACL rules according to the depth-first rule, wherein the longest subitem in a rule takes priority. The longest subset of a rule is matched first before the rule.

Command Default

None

Command Modes

Global configuration (config)

Example

```
Device#configure terminal
Device(config)#access-list link laye2acl match-order auto
```

access-list link number

To define a numbered Layer 2 Access Control List (ACL), use the **access-list** *number* command in the global configuration mode.

```
access-list number {permit |deny} [protocol ] [cos vlan-priority] ingress { {
[inner-vidvid ][start-vlan-id end-vlan-id ] [source-mac-addr source-mac-wildcard][interface
interface-number ]} |any } egress { { [dest-mac-addr dest-mac-wildcard ][interface
interface-num | cpu]} | any}[ time-range time-range ]
```

Syntax Description

permit	Specifies that the rule defined by the ACL is permitted.
deny	Specifies that the rule defined by the ACL is not permitted.
protocol	Specifies the type of protocol packet carried by the Ethernet frame. In hexadecimal notation, the range is 0 through FFFF. It is optional in case of ARP, IP, RARP.
cos	Defines the SYN flag in TCP. A value 1 indicates that the flag is active. This is applicable only if the *protocol* is tcp.
ingress	Specifies the rule for the incoming packets at the ingress port.
inner-vid	Specifies the inner VLAN ID of a double-tagged packet.
start-vlan-id end-vlan-id	Specifies the range of VLANs. For a double-tagged packet, it is the VLAN ID of the outer tag.
source-mac-addr source-mac-wildcard	Specifies the source MAC address options. *source-mac-wildcard* indicates the source MAC range.
interface *interface-num*	Specifies the physical port number. It can be either the ingress port or the egress port.
CPU	Indicates that the data will be forwarded to the CPU.
any	Specifies any address which can be at ingress or egress directions.
time-range *name*	Specifies the time range in which the ACL rule takes effect.
time-range*timerange-name*	Defines the specific time range to implement the ACL.

Command Default

None

Command Modes

Global configuration (config)

Usage Guidelines

The ACL is identified by the number assigned to it. You can create an ACL and assign a number to it. If you don't specify a number, the system assigns a number to the created ACL. For an Extended ACL, the numbers range from 200 through 299. You can create upto 100 Layer 2 ACLs.

Example

```
Device# configure terminal
Device(config)# access-list 201 permit arp ingress 00:00:00:00:01:01 0 egress any
```

local-user

To configure a local user, use the **local-user** command in the AAA configuration mode. To delete all local users, use the **no** form of the command.

local-user username *username* **password** *password* [**vlan** *vlan-id*]

no local-user {**all** | **user** *username*}

Syntax Description

username	Username of the local user.
password	Password of the local user.
vlan-id	The VLAN ID. The range is 1 to 4094.

Command Modes

AAA configuration (config-aaa)

Example

This example shows how to configure a local user using the **local-user** command:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# local-user username name1 password pass1 vlan 220
Device(config-aaa)#
```

nas-ipaddress

To configure the NAS client IP address for a RADIUS server, use the **nas-ipaddress** command in AAA configuration mode. To delete the configured NAS client IP address for a RADIUS server, use the **no** form of the command.

nas-ipaddress *ip-address*

no nas-ipaddress

Syntax Description

ip-address	IP address of RADIUS client.

Command Modes

AAA configuration (config-aaa)

Example

This example shows how to configure the NAS client IP address for a RADIUS server:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# nas 10.1.1.10
```

no ip route static all

To delete all static IP routes from the routing table, use the **no ip route static all** command in global configuration mode.

no ip route static all

Command Modes

Global configuration (config)

Example

This example shows how to delete all static IP routes from the routing table using the **no ip route static all** command:

```
Device> enable
Device# configure terminal
Device(config)# no ip route static all
```

periodic time-range

To configure a time period that specifies when an access control list (ACL) is in effect, use the **periodic** command in the time-range configuration mode. To remove the absolute time-range, use the **no** form of the command.

`[no]periodic [`*days-of-week*`]` *HH:MM:SS* `to [`*days-of-week* `]` *HH:MM:SS*

Syntax Description

days-of-week	Specifies the period, which are the days of the week: **mon**, **tue**, **wed**, **thu**, **fri**, **sat**, **sun**, **weekdays**, daily **weekdays** are Monday to Friday.
HH:MM:SS	Specifies the time in *hours*:*minutes*:*seconds* format.

Command Modes

Global Configuration (config)

Command Default

None

Example

```
Device#configure terminal
Device(config)#time-range days
Device(config-timerange-days)#periodic daily 04:50:30 to 09:50:40
```

preemption-time

To configure the recovery time to switch to the primary server, use the **preemption-time** command in AAA configuration mode.

preemption-time *time*

Syntax Description

time	The preemption time The unit in minutes. The range is from 0 to 1440. The default value isc0

Command Modes

AAA configuration (config-aaa)

Usage Guidelines

Use this command in the AAA configuration mode.

Examples

This example shows how to configure the recovery time to switch to the primary server.

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# preemption-time 200
```

Related Commands

Command	Description
aaa	Enters AAA configuration mode

{primary-acct-ip | second-acct-ip}

To configure the primary and secondary accounting servers, use the {**primary-acct-ip** |**second-acct-ip**} *ip_address port* command in AAA configuration mode. To disable the configured primary and secondary accounting servers, use the **no** form of the command.

{**primary-acct-ip** | **second-acct-ip**}*ip_address port*

no {**primary-acct-ip** | **second-acct-ip**}

Syntax Description

primary-acct-ip	The primary accounting server.
second-acct-ip	The secondary accounting server.
ip_address	The IP address of the server.
port	The accounting port The range is from 1 to 65535.

Command Modes

AAA configuration (config-aaa)

Examples

This example shows how to configure the primary and secondary accounting server.

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# primary-acct-ip 10.1.1.10 333
Device(config-aaa-radius-radius1)# second-acct-ip 10.1.1.11 350
```

{primary-auth-ip | second-auth-ip}

To configure the primary and secondary RADIUS servers, use the {**primary-auth-ip** |**second-auth-ip**} *ip_address port* command in AAA configuration mode. To disable the configured primary and secondary RADIUS servers, use the **no** form of the command.

{**primary-auth-ip** | **second-auth-ip**} *ip_address port*

no {**primary-auth-ip** | **second-auth-ip**}

Syntax Description

primary-auth-ip	The primary RADIUS server.
second-auth-ip	The secondary RADIUS server.
ip_address	The IP address of the server.
port	The server port The range is from 1 to 65535.

Command Default

None

Command Modes

AAA configuration (config-aaa)

Examples

This example shows how to configure the primary and secondary accounting server

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# primary-auth-ip 10.2.1.10 80
Device(config-aaa-radius-radius1)# second-auth-ip 10.2.1.11 90
```

radius

To configure the RADIUS server parameters, use the **radius** command in AAA configuration mode. To restore the default RADIUS server settings, use the **no** version of the command.

radius {**8021p enable** | **accounting** | **attribute client-version** | **bandwidth-limit enable** | **config-attribute** {**access-bandwidth** {**downlink** *vendor-type* | **unit** {**bps** | **kbps**} | **uplink***vendor-type*} | **dscp** *vendor-type* | **mac-address-number** *vendor-type*} | **host** *host-name* | **mac-address-number enable** | **server-disconnect drop1x** | **vlan enable**}

no radius {**8021p** | **accounting** | **attribute client-version** | **bandwidth-limit enable** | **host** *host-name* | **mac-address-number** | **server-disconnect drop1x** | **vlan**}

Syntax Description

8021p enable	Configures RADIUS to distribute port priority.
accounting	Enables accounting function.
attribute client-version	Send the H3C client's version to radius server.
bandwidth limit-enable	Configures RADIUS to distribute bandwidth control.
config-attribute	Configures the RADIUS attribute types with the vendor's attributes.
access-bandwidth	Configures the RADIUS access bandwidth attribute.
downlink	Configures the RADIUS downlink attribute.
uplink	Configures the RADIUS uplink attribute.
unit bps	Configures the RADIUS ACL bandwidth in units of bits per second.
unit kbps	Configures the RADIUS ACL bandwidth in units of kilobits per second.
dscp	Configures the RADIUS DSCP attribute.
config-attribute mac-address-number	Configures the maximum MAC address on the port that is learned for the RADIUS server.
vendor-type	The vendor type. The range is from 1 to 500.
mac-address-number enable	Configures RADIUS to distribute number limit of MAC address.
host *host-name*	Creates a RADIUS scheme and enters RADIUS scheme mode for the specified host name.
server-disconnect drop1x	Configures the device to shut the user down if the accounting packet does not respond.

vlan enable	Configures RADIUS to distribute port PVID.

Command Modes

AAA configuration (config-aaa)

Example

This example shows how to configure RADIUS to distribute port priority:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius 8021p enable
 Configure successfully.
```

Example

This example shows how to enable accounting function:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius accounting
 Modify accounting configuration of radius server successfully.
```

Example

This example shows how to send the H3C client's version to radius server:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius attribute client-version
Device(config-aaa)#
```

Example

This example shows how to configure RADIUS to distribute bandwidth control:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius bandwidth limit-enable
 Configure successfully.
```

Example

This example shows how to configure the RADIUS access bandwidth and downlink attribute:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius config-attribute access-bandwidth downlink 400
 Configure successfully.
```

Example

This example shows how to configure the RADIUS DSCP attribute:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius config-attribute dscp 1
 Configure successfully.
```

Example

This example shows how to create a RADIUS scheme and enters RADIUS scheme mode:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host hostname1
Device(config-aaa-radius-hostname1)#
```

Example

This example shows how to configure RADIUS to distribute number limit of MAC address:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius mac-address-number enable
 Configure successfully.
```

Example

This example shows how to shut the user down if the accounting packet does not respond:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius server-disconnect drop 1x
 Configure successfully.
```

Example

This example shows how to configure RADIUS to distribute port PVID:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius vlan enable
 Configure successfully.
```

realtime-account

To configure realtime accounting and its time interval, use the **realtime-account** command in AAA configuration mode. To disable realtime accounting, use the **no** form of the command.

realtime-accountinterval*time*

no realtime-account

Syntax Description

interval *time*	Configures the realtime accounting time interval. The range is 1 to 255 minutes.

Command Modes

AAA configuration (config-aaa)

Example

This example shows how to configure real time accounting using the **realtime-account** command:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# realtime-account interval 25
 Modify realtime_acct configuration of radius server successfully.
```

no access-list

To remove an entry or all entries from the Access Control List (ACL), use the **no access-list** command in the global configuration mode.

```
no access-list {number| name |all}
```

Syntax Description

number	Specifies that numbered ACL to delete
name	Specifies the name of the ACL to delete.

Command Default

None

Command Modes

Global configuration (config)

Example

```
Device#configure terminal
Device(config)#no access-list 10
```

scheme

To configure the server authentication scheme, use the **scheme** command in AAA configuration mode.

scheme {**local** | **radius** [**local**]}

Syntax Description

local	Configures to use local user authentication.
radius	Configures to use RADIUS server authentication.
radius local	Configures to use local user authentication if RADIUS server authentication fails.

Command Modes

AAA configuration (config-aaa)

Example

This example shows how to configure a server authentication scheme using the **scheme** command:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# domain eee
Device(config-aaa-domain-eee)# scheme radius
Device(config-aaa-domain-eee)#
```

show access-list config

To display the Access Controlled List (ACL) configurations, use the **show access-list config** command in the EXEC mode

show access-list config {*number* | **all** | **name** | **statistic** }

Syntax Description

number	Specifies the numbered ACL. Numbers 1 to 99 represent standard ACL. Numbers 100 to 199 represent extended ACL. Numbers 200 to 299 represent Layer 2 ACL.
all	Specifies all ACLs.
name	Specifies an ACL by name.
statistic	Specifies ACL statistics.

Command Modes

EXEC

Command Default

None

Usage Guidelines

Use the **show access-list config statistic** command to see the statistics of the ACL rules usage.

Use the **show access-list config name** command to see the ACL specified by name.

Use the **show access-list config all** command to all see the ACLs.

Examples

```
Device> enable
Device# show access-list config 1
Standard IP Access List 1, match-order is config, 2 rule:
  0  deny    any
permit  1.1.1.1  0.0.0.0
```

show access-list runtime

To display the Access Controlled List (ACL) at run time, use the **show access-list runtime** command in the EXEC mode

show access-list runtime {*number* | **all** | **name** | **statistic** }

Syntax Description

number	Specifies the numbered ACL. Numbers 1 to 99 represent standard ACL. Numbers 100 to 199 represent extended ACL. Numbers 200 to 299 represent Layer 2 ACL.
all	Specifies all ACLs.
name	Specifies an ACL by name.
statistic	Specifies ACL statistics.

Command Modes

EXEC

Command Default

None

Usage Guidelines

Use the **show access-list runtime statistic** command to see the statistics of the ACL rules usage.

Use the **show access-list runtime name** command to see the ACL specified by name.

Use the **show access-list runtime all** command to all see the ACLs.

Examples

```
Device> enable
Device# show access-list runtime 1
Standard IP Access List 1, match-order is config, 1 rule:
  0  deny    any
```

show anti-dos

To display the anti-DDOS configuration information, use the **show anti-dos** command in privileged EXEC or global configuration modes.

show anti-dos

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show anti-dos** command:

```
Device> enable
Device# configure terminal
Device(config)# show anti-dos
Informations of AntiDos:
Ip fragment max number:800
Ip fragment number now:0
TTL=0 packet traffic to CPU is disable.
```

show arp anti-flood

To display the ARP anti-flood configuration and attackers list, use the **show arp anti-flood** command in privileged EXEC or global configuration modes.

show arp anti-floodport-threshold [{ **ethernet** | **gpon** } *slot-number/port-number* [**to** { **ethernet** | **gpon** } *slot-number/port-number*]]

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to 8. • GE Ethernet: The range is from 1 to 4. • 10GE Ethernet: The range is from 1 to 2.
to	Displays the information for a range of ports. If you use the **to** keyword, specify the same port type before and after the keyword.

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show arp anti-flood** command:

```
Device> enable
Device# configure terminal
Device(config)# show arp anti-flood
Arp anti-flood: disabled
Arp rate limit:25pps
User recovery time:234 minutes
Reject type:DenyAll
DeniedSrcMAC       SourceIP         Port     Vlan  DenyType  RemainAgingTime(m)

Total entry:0.
```

Example

This example shows a sample output for the **show arp anti-flood port-threshold** command:

```
Device> enable
Device# configure terminal
Device(config)# show arp anti-flood port-threshold
Arp anti-flood: disabled
Arp rate limit:25pps
User recovery time:234 minutes
Reject type:DenyAll
Port        Port-threshold
g0/1        16
g0/2        16
g0/3        16
g0/4        16
g0/5        16
g0/6        16
g0/7        16
g0/8        16
e1/1        16
e1/2        16
e1/3        16
e1/4        16
e2/1        16
e2/2        16
```

show arp anti interface

To display the state of the interface, use the **show arp anti interface** command in privileged EXEC or global configuration modes.

show arp anti interface [{**ethernet** | **gpon**} *slot-number/port-number*]

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to 8. • GE Ethernet: The range is from 1 to 4. • 10GE Ethernet: The range is from 1 to 2.

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show arp anti interface** command:

```
Device> enable
Device# configure terminal
Device(config)# show arp anti interface
Port          mode          threshold(anti-flood)
g0/1          untrust       -
g0/2          untrust       -
g0/3          untrust       -
g0/4          untrust       -
g0/5          untrust       -
g0/6          untrust       -
g0/7          untrust       -
g0/8          untrust       -
e1/1          untrust       -
e1/2          untrust       -
e1/3          untrust       -
e1/4          untrust       -
e2/1          untrust       -
e2/2          untrust       -
```

show cpu-car

To display the CPU-car performance, use the **show cpu-car** command in privileged EXEC or global configuration modes.

show cpu-car

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show cpu-car** command:

```
Device> enable
Device# configure terminal
Device(config)# show cpu-car
Send packet to cpu rate = 4000 pps.
```

show cpu-classification

To display CPU receiving packet classification statistics, run the **show cpu-classification** command in privileged EXEC or global configuration modes.

show cpu-classification [**interface** {**ethernet** | **gpon**}*slot-number/port-number*]

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to 8. • GE Ethernet: The range is from 1 to 4. • 10GE Ethernet: The range is from 1 to 2.

Command Default

None

Command Modes

Privileged EXEC(#)
Global Configuration(config)

Examples

This example shows how to view CPU receiving packet classification statistics.

```
Device> enable
Device# configure terminal
Device(config)# show cpu-classification
Type        Count       Percent(%)
Total       460699064   100

BPDU        8237424     1

ARP         378164060   82

IGMP        607189      0
ICMP        699125      0
OSPF        0           0
RIP         139         0
DHCP        12658100    2

SNMP        4079818     0

Telnet      122166      0
SSH         10788       0
Other       56120236    12
```

show cpu-statistics

To display CPU receiving packet port statistics, use the **show cpu-statistics** command in privileged EXEC and global configuration modes.

show cpu-statistics [**channel-group** *channel-group-number* | {**gpon** | **ethernet**}*slot-number/port-number*] [**to**{**channel-group** *channel-group-number* | {**gpon** | **ethernet** }*slot-number/port-number*}]

Syntax Description

channel-group*channel-group-number*	The LACP channel group.
slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to 8. • GE Ethernet: The range is from 1 to 4. • 10GE Ethernet: The range is from 1 to 2.
to	Displays the information for a range of ports. If you use the **to** keyword, specify the same port type before and after the keyword.

Command Default

None

Command Modes

Privileged EXEC (#)
Global configuration (config)

Examples

This example shows how to view CPU receiving packet port statistics.

```
Device> enable
Device# configure terminal
Device(config)# show cpu-statistics ethernet 1/1
Show packets sent to cpu  statistic information
port  64Byte  128Byte  256Byte  512Byte  1024Byte  2048Byte
e1/1  0       0        0        0        0         0
```

show cpu-utilization

To display CPU utilization, use the **show cpu-utilization** command in global configuration mode.

show cpu-utilization

Command Default

None

Command Modes

Global configuration (config)

Examples

This example shows how to view CPU utilization.

```
Device> enable
Device# configure terminal
Device(config)# show cpu-utilization
CPU Information:
CPU Idle : 79 %
```

show dhcp anti-attack

To display the DHCP anti-attack configuration, use the **show dhcp anti-attack** command in privileged EXEC and global configuration modes.

show dhcp anti-attack [**interface**{**ethernet** | **gpon**} *slot-number/port-number*[**to** {**ethernet** | **gpon**} *slot-number/port-number*]]

Syntax Description

to	Displays the information for a range of ports. If you use the **to** keyword, specify the same port type before and after the keyword.
slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to 8. • GE Ethernet: The range is from 1 to 4. • 10GE Ethernet: The range is from 1 to 2.

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show dhcp anti-attack** command:

```
Device> enable
Device# configure terminal
Device(config)# show dhcp anti-attack
Dhcp anti-attack: enabled
Dhcp rate limit:1pps
User recovery time:3 minutes
Reject type:DenyDHCP
DeniedSrcMAC Port Vlan DenyType RemainAgingTime(m)
00:00:00:01:11:23 e1/1 2 DenyDHCP 3
Total entry: 1.
#After 3 minutes, the attack entry is aged out
```

show discard-bpdu

To display the BPDU status, use the **show discard-bpdu** command in privileged EXEC and global configuration modes.

show discard-bpdu

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show discard-bpdu** command:

```
Device> enable
Device# configure terminal
Device(config)# show discard-bpdu
Discard BPDU global status: disable
Discard BPDU enable port:

Notes: Once global status is on, the switch will discard all BPDUs.
If want to enable on some ports only, need to disable global function and choose another
commands.
```

show dot1x

To display the 802.1x authentication function details, run the **show dot1x** command in privileged EXEC and global configuration modes.

show dot1x [[**daemon** | **detect** | **eapol-relay** | **guest-vlan**] [**interface**{**ethernet** | **gpon**} *slot-number/port-number*] [**to** {**ethernet** | **gpon**} *slot-number/port-number*] | **max-reauth** | **max-req** | **port-auth** | **quiet-period-value** | **session** [**interface**{**ethernet** | **gpon**} *slot-number/port-number* [**to** {**ethernet** | **gpon**} *slot-number/port-number*] | **mac-address** *mac-address-value*]]

Syntax Description

daemon	Displays the configuration of 802.1x authentication interface watch function.
detect	Displays heartbeat detection configuration.
eapol-relay	Displays EAPOL pass through configuration.
guest-vlan	Displays guest VLAN information.
interface	Displays interface configuration, such as the interface control mode, re-authentication state, the maximum number of users for the interface authentication.
slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to 8. • GE Ethernet: The range is from 1 to 4. • 10GE Ethernet: The range is from 1 to 2.
to	Displays the information for a range of ports. If you use the **to** keyword, specify the same port type before and after the keyword.
max-reauth	Displays information about maximum count of the EAP requests and identity packets sent by the server.
max-req	Displays information about the maximum count of the EAP requests sent by the server.

port-auth	Displays whether the interface authentication is enabled or disabled.
quiet-period-value	Displays the quiet period.
session	Displays 802.1x session.
mac-address *mac-address-value*	Displays 802.1x session information for the specified MAC address.

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows the sample output for the **show dot1x daemon**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x daemon
port  daemonstatus  daemontime(s)
g0/1  close         60
g0/2  close         60
g0/3  close         60
g0/4  close         60
g0/5  close         60
g0/6  close         60
g0/7  close         60
g0/8  close         60
e1/1  close         60
e1/2  close         60
e1/3  close         60
e1/4  close         60
e2/1  close         60
e2/2  close         60
```

Example

This example shows the sample output for the **show dot1x detect**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x detect
the user detect interval is 25
port : detect
g0/1 : disable
g0/2 : disable
g0/3 : disable
g0/4 : disable
g0/5 : disable
g0/6 : disable
g0/7 : disable
g0/8 : disable
e1/1 : disable
e1/2 : disable
e1/3 : disable
e1/4 : disable
e2/1 : disable
```

```
e2/2 : disable

Total [14] item(s), printed [14] item(s).
```

Example

This example shows the sample output for the **show dot1x eapol-relay**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x eapol-relay
Port  EapolRelay  EapolRelayUplink
g0/1  disabled    false
g0/2  disabled    false
g0/3  disabled    false
g0/4  disabled    false
g0/5  disabled    false
g0/6  disabled    false
g0/7  disabled    false
g0/8  disabled    false
e1/1  disabled    false
e1/2  disabled    false
e1/3  disabled    false
e1/4  disabled    false
e2/1  disabled    false
e2/2  disabled    false

Total entries: 14.
```

Example

This example shows the sample output for the **show dot1x guest-vlan**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x guest-vlan
Port  GuestVlan  Status
g0/1  disable    InConfigVlan
g0/2  disable    InConfigVlan
g0/3  disable    InConfigVlan
g0/4  disable    InConfigVlan
g0/5  disable    InConfigVlan
g0/6  disable    InConfigVlan
g0/7  disable    InConfigVlan
g0/8  disable    InConfigVlan
e1/1  44         InConfigVlan
e1/2  disable    InConfigVlan
e1/3  disable    InConfigVlan
e1/4  disable    InConfigVlan
e2/1  disable    InConfigVlan
e2/2  disable    InConfigVlan

Total entries: 14.
```

Example

This example shows the sample output for the **show dot1x interface**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x interface ethernet 1/3
Authentication of system: disabled
Type of authentication: eap-finish

Total [0] item(s).
```

Example

This example shows the sample output for the **show dot1x max-reauth**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x max-reauth
the max-reauth is 2.
```

Example

This example shows the sample output for the **show dot1x max-req**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x max-req
the max-req is 2.
```

Example

This example shows the sample output for the **show dot1x port-auth**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x port-auth
------------------------------------------------------------------------
port 1 auth is close
port 2 auth is close
port 3 auth is close
port 4 auth is close
port 5 auth is close
port 6 auth is close
port 7 auth is close
port 8 auth is close
port 9 auth is close
port 10 auth is close
port 11 auth is close
port 12 auth is close
port 13 auth is close
port 14 auth is close
------------------------------------------------------------------------
```

Example

This example shows the sample output for the **show dot1x quiet-period-value**

```
Device> enable
Device# configure terminal
```

```
Device(config)# show dot1x quiet-period-value
the quiet-period-value is 0.
```

Example

This example shows the sample output for the **show dot1x session**

```
Device> enable
Device# configure terminal
Device(config)# show dot1x session
Total [0] item(s).
```

show ip route

To display the related information of specified routes as well as static routes, use the **show ip route** command in privileged EXEC and global configuration modes.

show ip route [*ip-address* [*mask*] | **ospf** | **rip** | **static**]

Syntax Description

ip-address	The destination address.
mask	The destination network segment presented with IP address.
ospf	Displays all OSPF routes.
rip	Displays all RIP routes.
static	Displays all static routes.

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show ip route** command:

```
Device> enable
Device# configure terminal
Device(config)# show ip route
Show ip route information

INET route table - vr: 0, table: 254
Route flag: U - up, G - gateway, H - host, R - reject, C - clone, S - static
Destination         Gateway             Flags    Use   Interface       Proto
0.0.0.0/0           10.75.171.1         UGS      659   VLAN-IF100      static
10.75.171.0/24      10.75.171.17        UC       5     VLAN-IF100      local
10.75.171.17        10.75.171.17        UH       0     lo0             local
127.0.0.0/8         127.0.0.1           UR       0     lo0             local
127.0.0.1           127.0.0.1           UH       4     lo0             local
192.168.100.0/24    192.168.100.1       UC       0     METH-IF0        local
192.168.100.1       192.168.100.1       UH       0     lo0             local

Total entries: 7. Printed entries: 7.
```

show radius

To display the RADIUS server details, run the **show radius** command in privileged EXEC mode.

show radius {**attribute** | **config-attribute** | **host** [*radius-server-name*]}

Syntax Description

attribute	Displays the H3C client version information that is sent to the RADIUSRADIU server.
config-attribute	Displays the configured vendor-self attribute type in RADIUS attribute information.
host	Displays RADIUS host configuration information for all RADIUS servers.
host *radius-server-name*	Displays RADIUS host configuration information for the specified RADIUS server.

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows the sample output for the **show radius host** command:

```
Device> enable
Device# configure terminal
Device(config)# show radius host
------------------------------------------------------------------------

ServerName  = binidng
PrimAuthServerIP = 0.0.0.0          PrimAcctServerIP = 0.0.0.0
SecAuthServerIP  = 0.0.0.0          SecAcctServerIP  = 0.0.0.0
PrimAuthPort     = 1812             PrimAcctPort     = 1813
SecAuthPort      = 1812             SecAcctPort      = 1813
Auth-secretKey  = Switch        Acct-secretKey  = Switch
UserNameFormat = with-domain
RealTimeAcctSwitch = open       RealTimeAcctTime = 12
RadiusClientIP  = 0.0.0.0
------------------------------------------------------------------------
ServerName  = r1
PrimAuthServerIP = 0.0.0.0          PrimAcctServerIP = 0.0.0.0
SecAuthServerIP  = 0.0.0.0          SecAcctServerIP  = 0.0.0.0
PrimAuthPort     = 1812             PrimAcctPort     = 1813
SecAuthPort      = 1812             SecAcctPort      = 1813
Auth-secretKey  = Switch        Acct-secretKey  = Switch
UserNameFormat = with-domain
RealTimeAcctSwitch = open       RealTimeAcctTime = 12
RadiusClientIP  = 0.0.0.0
------------------------------------------------------------------------
ServerName  = mmm
PrimAuthServerIP = 0.0.0.0          PrimAcctServerIP = 0.0.0.0
SecAuthServerIP  = 0.0.0.0          SecAcctServerIP  = 0.0.0.0
PrimAuthPort     = 1812             PrimAcctPort     = 1813
SecAuthPort      = 1812             SecAcctPort      = 1813
Auth-secretKey  = Switch        Acct-secretKey  = Switch
```

```
UserNameFormat = with-domain
RealTimeAcctSwitch = open       RealTimeAcctTime = 12
RadiusClientIP  = 0.0.0.0
------------------------------------------------------------------------
ServerName  = eee
PrimAuthServerIP = 0.0.0.0          PrimAcctServerIP = 0.0.0.0
SecAuthServerIP  = 0.0.0.0          SecAcctServerIP  = 0.0.0.0
PrimAuthPort     = 1812             PrimAcctPort     = 1813
SecAuthPort      = 1812             SecAcctPort      = 1813
Auth-secretKey  = Switch        Acct-secretKey  = Switch
UserNameFormat = with-domain
RealTimeAcctSwitch = open       RealTimeAcctTime = 12
RadiusClientIP  = 0.0.0.0
------------------------------------------------------------------------
ServerName  = cisco
PrimAuthServerIP = 0.0.0.0          PrimAcctServerIP = 0.0.0.0
SecAuthServerIP  = 0.0.0.0          SecAcctServerIP  = 0.0.0.0
PrimAuthPort     = 1812             PrimAcctPort     = 1813
SecAuthPort      = 1812             SecAcctPort      = 1813
Auth-secretKey  = Switch        Acct-secretKey  = Switch
UserNameFormat = with-domain
RealTimeAcctSwitch = open       RealTimeAcctTime = 12
RadiusClientIP  = 0.0.0.0
------------------------------------------------------------------------
ServerName  = 3
PrimAuthServerIP = 0.0.0.0          PrimAcctServerIP = 0.0.0.0
SecAuthServerIP  = 0.0.0.0          SecAcctServerIP  = 0.0.0.0
PrimAuthPort     = 1812             PrimAcctPort     = 1813
SecAuthPort      = 1812             SecAcctPort      = 1813
Auth-secretKey  = Switch        Acct-secretKey  = Switch
UserNameFormat = with-domain
RealTimeAcctSwitch = open       RealTimeAcctTime = 12
RadiusClientIP  = 0.0.0.0
------------------------------------------------------------------------
ServerName  = radius1
PrimAuthServerIP = 0.0.0.0          PrimAcctServerIP = 10.1.1.10
SecAuthServerIP  = 0.0.0.0          SecAcctServerIP  = 0.0.0.0
PrimAuthPort     = 1812             PrimAcctPort     = 333
SecAuthPort      = 1812             SecAcctPort      = 1813
Auth-secretKey  = Switch        Acct-secretKey  = Switch
UserNameFormat = with-domain
RealTimeAcctSwitch = open       RealTimeAcctTime = 12
RadiusClientIP  = 0.0.0.0
------------------------------------------------------------------------

Total [7] item(s), printed [7] item(s).
```

show shutdown-control interface

To display the shutdown configuration, use the **show shutdown-control interface** command in privileged EXEC or global configuration mode.

show shutdown-control interface [**ethernet** *slot-number/port-number* [**to ethernet** *slot-number/port-number*]]

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to 8. • GE Ethernet: The range is from 1 to 4. • 10GE Ethernet: The range is from 1 to 2.
to	Displays the information for a range of ports. If you use the **to** keyword, specify the same port type before and after the keyword.

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show shutdown-control interface** command:

```
Device> enable
Device# configure terminal
Device(config)# show shutdown-control interface
port shutdown control recover mode : manual
port shutdown control information :
PortID   Broadcast Broadcast Multicast Multicast Unicast Unicast
         status    value     status    value     status  value
e1/1     disable   -         disable   -         disable -
e1/2     disable   -         disable   -         disable -
e1/3     disable   -         disable   -         disable -
e1/4     disable   -         disable   -         disable -
e2/1     disable   -         disable   -         disable -
e2/2     disable   -         disable   -         disable -
Total entries: 6 .
```

show spanning-tree interface

To display the spanning tree configuration parameters, use the **show spanning-tree interface** command in the privileged EXEC and global configuration modes.

show spanning-tree interface [**brief** | {**ethernet** | **gpon**} *slot-number/port-number* [**to** {**ethernet** | **gpon**} *slot-number/port-number*]]

Syntax Description

slot-number/port-number	The port ID. • *slot-number*: • GPON: The value is 0. • GE Ethernet: The value is 1. • 10GE Ethernet: The value is 2. • *port-number*: • GPON: The range is from 1 to 8. • GE Ethernet: The range is from 1 to 4. • 10GE Ethernet: The range is from 1 to 2.
to	Displays the information for a range of ports. If you use the **to** keyword, specify the same port type before and after the keyword.

Command Modes

Privileged EXEC (#)
Global Configuration (config)

Example

This example shows a sample output for the **show spanning-tree interface** command:

```
Device> enable
Device# configure terminal
Device(config)# show spanning-tree interface
Port g0/1 of bridge is Forwarding
   Spanning tree protocol is enabled
 Port g0/2 of bridge is DOWN
   Spanning tree protocol is enabled
 Port g0/3 of bridge is DOWN
   Spanning tree protocol is enabled
 Port g0/4 of bridge is DOWN
   Spanning tree protocol is enabled
 Port g0/5 of bridge is DOWN
   Spanning tree protocol is enabled
 Port g0/6 of bridge is DOWN
   Spanning tree protocol is enabled
 Port g0/7 of bridge is DOWN
   Spanning tree protocol is enabled
```

```
Port g0/8 of bridge is DOWN
  Spanning tree protocol is enabled
Port e1/1 of bridge is DOWN
  Spanning tree protocol is enabled
Port e1/2 of bridge is DOWN
  Spanning tree protocol is enabled
Port e1/3 of bridge is Forwarding
  Spanning tree protocol is enabled
Port e1/4 of bridge is DOWN
  Spanning tree protocol is enabled
Port e2/1 of bridge is DOWN
  Spanning tree protocol is enabled
Port e2/2 of bridge is DOWN
  Spanning tree protocol is enabled
```

shutdown-control-recover

To enable the port recovery mode and configure the port recovery parameters, use the **shutdown-control-recover** command in global configuration mode. To disable the port recovery mode and restore the default parameter values, use the **no** form of the command.

shutdown-control-recover {**automatic-open-time** *open-time* | **mode** {**automatic** | **manual**}}

no shutdown-control-recover {**automatic-open-time** | **mode**}

Syntax Description

automatic-open-time *open-time*	Configures the time after which the port restarts once the recovery time is expires.
mode automatic	Enables automatic recovery mode.
mode manual	Enables manual recovery mode.

Command Modes

Global Configuration (config)

Example

This example shows how to configure automatic recovery mode on a port using the **shutdown-control-recover** command:

```
Device> enable
Device# configure terminal
Device(config)# shutdown-control-recover mode automatic
Device(config)#
```

spanning-tree (global configuration)

To enable spanning tree globally and configure the spanning tree parameters, use the **spanning-tree** command in global configuration mode. To disable spanning tree, use the **no** form of the command.

spanning-tree [**forward-time** *delay-time* | **hello-time** *hello-time* | **max-age** *age-time* | **mode** {**rstp** | **stp**} | **pathcost-standard** {**dot1d-1998** | **dot1t**} | **priority** *priority-value* | **root-guard action** {**block-port** | **drop-packets**}]

no spanning-tree [**forward-time** | **hello-time** | **max-age** | **mode** | **pathcost-standard** | **priority** | **root-guard action**]

Syntax Description

forward-time *delay-time*	Configures the forwarding delay of the system. The range is 4 to 30 seconds.
hello-time *hello-time*	Configures the hello message time interval. The range is 1 to 10 seconds.
max-age *age-time*	Configures the aging time of the system The range is 6 to 40 seconds.
mode rstp	Configures the RSTP spanning tree mode.
mode stp	Configures the STP spanning tree mode.
pathcost-standard dot1d-1998	Sets pathcost standard for dot1d-1998.
pathcost-standard dot1t	Sets pathcost standard for dot1t.
priority *priority-value*	Configures the switch priority. The range is from 0 to 61440, in steps of 4096.
root-guard action block-port	Enables root protection globally. BPDU configuration messages are discarded and data packets are not forwarded.
root-guard action drop-packets	Enables root protection globally. BPDU configuration messages are discarded and data packets are forwarded.

Command Modes

Global configuration (config)

Example

This example shows how to configure the forwarding delay of the system:

```
Device> enable
Device# configure terminal
```

```
Device(config)# spanning-tree forward-time 10
Device(config)#
```

Example

This example shows how to configure the hello message time interval:

```
Device> enable
Device# configure terminal
Device(config)# spanning-tree hello-time 5
Device(config)#
```

Example

This example shows how to configure the aging time of the system:

```
Device> enable
Device# configure terminal
Device(config)# spanning-tree max-age 10
Device(config)#
```

Example

This example shows how to configure RSTP spanning tree mode:

```
Device> enable
Device# configure terminal
Device(config)# spanning-tree mode rstp
Device(config)#
```

Example

This example shows how to configure STP spanning tree mode:

```
Device> enable
Device# configure terminal
Device(config)# spanning-tree mode stp
Device(config)#
```

Example

This example shows how to configure the pathcost standard:

```
Device> enable
Device# configure terminal
Device(config)# spanning-tree pathcost-standard dot1t
Device(config)#
```

Example

This example shows how to configure the switch priority:

```
Device> enable
Device# configure terminal
```

```
Device(config)# spanning-tree priority 3
Device(config)#
```

Example

This example shows how to enable root guard protection globally and configure the data packets to not be forwarded:

```
Device> enable
Device# configure terminal
Device(config)# spanning-tree root-guard action block-port
Device(config)#
```

spanning-tree (interface configuration)

To enable spanning tree on a specific interface and configure the spanning tree parameters, use the **spanning-tree** command in interface configuration mode. To disable spanning tree, use the **no** form of the command.

spanning-tree [**cost** *cost-value* | **loop-guard** | **mcheck** | **point-to-point** {**auto** | **forcefalse** | **forcetrue**} | **port-priority** *priority-value* | **portfast** | **root-guard** | **transit-limit value**]

no spanning-tree [**cost** | **loop-guard** | **point-to-point** | **port-priority** | **portfast** | **root-guard** | **transit-limit**]

Syntax Description

cost *cost-value*	Modifies the path cost of the STP port. The range is 1 to 200000000.
loop-guard	Enables loop-guard on the port.
mcheck	Configures Mcheck on the port.
point-to-point auto	STP decides the point to point link.
point-to-point forcetrue	Enables the point to point link.
point-to-point forcefalse	Disables the point to point link.
port-priority *priority-value*	Configures the STP priority of the port. The range is 0 to 240.
portfast	Configures the port as an edge port.
root-guard	Enables root protection locally on the port.
transit-limit *value*	Configures the port to send the maximum rate of BPDU messages. The range is 1 to 255.

Command Modes

Interface configuration (config-if)

Example

This example shows how to configure the path cost of an STP port:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/3
Device(config-if-ethernet-1/3)# spanning-tree cost 1000
Device(config-if-ethernet-1/3)#
```

Example

This example shows how to enable loop guard on an STP port:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/3
Device(config-if-ethernet-1/3)# spanning-tree loop-guard
Device(config-if-ethernet-1/3)#
```

Example

This example shows how to configure Mcheck on an STP port:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/3
Device(config-if-ethernet-1/3)# spanning-tree mcheck
Device(config-if-ethernet-1/3)#
```

Example

This example shows how to enable point to point link on an STP port:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/3
Device(config-if-ethernet-1/3)# spanning-tree point-to-point forcetrue
Device(config-if-ethernet-1/3)#
```

Example

This example shows how to configure the STP priority of an STP port:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/3
Device(config-if-ethernet-1/3)# spanning-tree port-priority 3
Device(config-if-ethernet-1/3)#
```

Example

This example shows how to configure the STP port as an edge port:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/3
Device(config-if-ethernet-1/3)# spanning-tree portfast
Device(config-if-ethernet-1/3)#
```

Example

This example shows how to enable root protection on an STP port:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/3
Device(config-if-ethernet-1/3)# spanning-tree root-guard
Device(config-if-ethernet-1/3)#
```

Example

This example shows how to configure an STP port to send the maximum rate of BPDU messages:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/3
Device(config-if-ethernet-1/3)# spanning-tree transit-limit 200
Device(config-if-ethernet-1/3)#
```

time-range

To specify when an access control list (ACL) is in effect, use the **time-range** command in the global configuration mode. To remove the time range, use the **no** form of the command.

```
[no]time-range name
```

Syntax Description

name	Specifies a unique name for the time range. Name has to begin with an alphabetic character.

Command Modes

Global Configuration (config)

Command Default

None

Example

```
Device#configure terminal
Device(config)#time-range weekends
```

username-format

To configure a packet to carry the username when it is passed by the system to the RADIUS server, use the **username-format** command in AAA configuration module.

username-format {**with-domain** | **without-domain**}

Syntax Description

with-domain	Configures the packet to carry the username with the domain.
without-domain	Configures the packet to carry the username without the domain.

Command Modes

AAA configuration (config-aaa)

Example

This example shows how to configure the system to carry the user name when it passes a packet to the RADIUS server using the **username-format** command:

```
Device> enable
Device# configure terminal
Device(config)# aaa
Device(config-aaa)# radius host radius1
Device(config-aaa-radius-radius1)# username-format with-domain
 Modify the username format of RADIUS configuration successfully
```