

HP 5120 EI Switch Series

Security

Command Reference

Part number: 5998-1779

Software version: Release 2220

Document version: 6W100-20130810



Legal and notice information

© Copyright 2013 Hewlett-Packard Development Company, L.P.

No part of this documentation may be reproduced or transmitted in any form or by any means without prior written consent of Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Contents

AAA configuration commands	1
General AAA configuration commands	1
aaa nas-id profile	1
access-limit enable	1
accounting command	2
accounting default	3
accounting lan-access	4
accounting login	4
accounting optional	5
accounting portal	6
authentication default	7
authentication lan-access	8
authentication login	8
authentication portal	9
authentication super	10
authorization command	11
authorization default	12
authorization lan-access	13
authorization login	13
authorization portal	14
authorization-attribute user-profile	15
cut connection	16
display connection	17
display domain	20
domain	22
domain default enable	22
idle-cut enable	23
nas-id bind vlan	24
self-service-url enable	24
state (ISP domain view)	25
Local user configuration commands	26
access-limit	26
authorization-attribute (local user view/user group view)	26
bind-attribute	28
display local-user	29
display user-group	31
expiration-date (local user view)	32
group	33
group-attribute allow-guest	33
local-user	34
password (local user view)	35
service-type	36
state (local user view)	37
user-group	37
validity-date	38
RADIUS configuration commands	39
accounting-on enable	39
attribute 25 car	40
data-flow-format (RADIUS scheme view)	40

display radius scheme	41
display radius statistics	44
display stop-accounting-buffer (for RADIUS)	47
key (RADIUS scheme view)	48
nas-ip (RADIUS scheme view)	49
primary accounting (RADIUS scheme view)	50
primary authentication (RADIUS scheme view)	51
radius client	53
radius dscp	54
radius ipv6 dscp	54
radius nas-ip	55
radius scheme	55
radius trap	56
reset radius statistics	57
reset stop-accounting-buffer (for RADIUS)	57
retry	58
retry realtime-accounting	59
retry stop-accounting (RADIUS scheme view)	60
secondary accounting (RADIUS scheme view)	61
secondary authentication (RADIUS scheme view)	62
security-policy-server	64
server-type	64
state primary	65
state secondary	66
stop-accounting-buffer enable (RADIUS scheme view)	67
timer quiet (RADIUS scheme view)	67
timer realtime-accounting (RADIUS scheme view)	68
timer response-timeout (RADIUS scheme view)	69
user-name-format (RADIUS scheme view)	70
HWTACACS configuration commands	71
data-flow-format (HWTACACS scheme view)	71
display hwtacacs	72
display stop-accounting-buffer (for HWTACACS)	75
hwtacacs nas-ip	75
hwtacacs scheme	76
key (HWTACACS scheme view)	77
nas-ip (HWTACACS scheme view)	78
primary accounting (HWTACACS scheme view)	79
primary authentication (HWTACACS scheme view)	79
primary authorization	80
reset hwtacacs statistics	81
reset stop-accounting-buffer (for HWTACACS)	82
retry stop-accounting (HWTACACS scheme view)	82
secondary accounting (HWTACACS scheme view)	83
secondary authentication (HWTACACS scheme view)	84
secondary authorization	84
stop-accounting-buffer enable (HWTACACS scheme view)	85
timer quiet (HWTACACS scheme view)	86
timer realtime-accounting (HWTACACS scheme view)	86
timer response-timeout (HWTACACS scheme view)	87
user-name-format (HWTACACS scheme view)	88
RADIUS server configuration commands	89
authorization-attribute (RADIUS-server user view)	89
description	89

expiration-date (RADIUS-server user view)	90
password (RADIUS-server user view)	91
radius-server client-ip	91
radius-server user	92
802.1X configuration commands	94
display dot1x	94
dot1x	97
dot1x attempts max-fail	99
dot1x authentication-method	99
dot1x auth-fail vlan	101
dot1x critical vlan	101
dot1x critical recovery-action	103
dot1x domain-delimiter	103
dot1x eapol untag	104
dot1x guest-vlan	105
dot1x handshake	106
dot1x handshake secure	107
dot1x mandatory-domain	107
dot1x max-user	108
dot1x multicast-trigger	110
dot1x port-control	110
dot1x port-method	111
dot1x quiet-period	112
dot1x re-authenticate	113
dot1x retry	114
dot1x timer	115
dot1x unicast-trigger	116
reset dot1x statistics	117
vlan-group	117
vlan-list	118
EAD fast deployment configuration commands	119
dot1x free-ip	119
dot1x timer ead-timeout	119
dot1x url	120
MAC authentication configuration commands	122
display mac-authentication	122
mac-authentication	124
mac-authentication critical vlan	125
mac-authentication domain	126
mac-authentication guest-vlan	127
mac-authentication max-user	128
mac-authentication timer	128
mac-authentication timer auth-delay	129
mac-authentication user-name-format	130
reset mac-authentication statistics	131
Portal configuration commands	132
display portal free-rule	132
display portal interface	133
display portal local-server	134
display portal tcp-cheat statistics	135
display portal user	136
portal auth-fail vlan	137

portal delete-user	138
portal domain	139
portal free-rule	139
portal local-server	140
portal local-server enable	141
portal local-server ip	142
portal max-user	143
portal move-mode auto	143
portal offline-detect interval	144
portal redirect-url	145
portal server banner	145
portal web-proxy port	146
reset portal tcp-cheat statistics	147
Port security configuration commands	148
display port-security	148
display port-security mac-address block	151
display port-security mac-address security	152
port-security authorization ignore	154
port-security enable	155
port-security intrusion-mode	155
port-security mac-address aging-type inactivity	156
port-security mac-address dynamic	157
port-security mac-address security	158
port-security max-mac-count	159
port-security ntk-mode	160
port-security oui	161
port-security port-mode	162
port-security timer autolearn aging	164
port-security timer disableport	164
port-security trap	165
User profile configuration commands	167
display user-profile	167
user-profile enable	168
user-profile	168
Password control configuration commands	170
display password-control	170
display password-control blacklist	171
password	172
password-control { aging composition history length } enable	173
password-control aging	174
password-control alert-before-expire	175
password-control authentication-timeout	176
password-control complexity	176
password-control composition	177
password-control enable	178
password-control expired-user-login	179
password-control history	179
password-control length	180
password-control login idle-time	181
password-control login-attempt	182
password-control password update interval	183
password-control super aging	184
password-control super composition	184

password-control super length	185
reset password-control blacklist	186
reset password-control history-record	186
HABP configuration commands	188
display habp	188
display habp table	189
display habp traffic	189
habp client vlan	190
habp enable	191
habp server vlan	191
habp timer	192
Public key configuration commands	194
display public-key local public	194
display public-key peer	196
peer-public-key end	197
public-key-code begin	198
public-key-code end	198
public-key local create	199
public-key local destroy	200
public-key local export dsa	201
public-key local export rsa	202
public-key peer	203
public-key peer import sshkey	204
PKI configuration commands	205
attribute	205
ca identifier	206
certificate request entity	206
certificate request from	207
certificate request mode	207
certificate request polling	208
certificate request url	209
common-name	210
country	210
crl check	211
crl update-period	211
crl url	212
display pki certificate	212
display pki certificate access-control-policy	214
display pki certificate attribute-group	215
display pki crl domain	216
fqdn	217
ip (PKI entity view)	218
ldap-server	219
locality	219
organization	220
organization-unit	220
pki certificate access-control-policy	221
pki certificate attribute-group	221
pki delete-certificate	222
pki domain	223
pki entity	223
pki import-certificate	224
pki request-certificate domain	224

pki retrieval-certificate	225
pki retrieval-crl domain	226
pki validate-certificate	226
root-certificate fingerprint	227
rule (PKI CERT ACP view)	228
state	228
IPsec configuration commands	230
ah authentication-algorithm	230
connection-name	230
display ipsec policy	231
display ipsec proposal	234
display ipsec sa	235
display ipsec session	238
display ipsec statistics	239
display ipsec tunnel	241
encapsulation-mode	242
esp authentication-algorithm	243
esp encryption-algorithm	243
ike-peer (IPsec policy view)	244
ipsec anti-replay check	245
ipsec anti-replay window	245
ipsec decrypt check	246
ipsec policy (interface view)	246
ipsec policy (system view)	247
ipsec proposal	248
ipsec sa global-duration	249
ipsec session idle-time	249
pfs	250
policy enable	251
proposal (IPsec policy view)	251
qos pre-classify	252
reset ipsec sa	253
reset ipsec session	254
reset ipsec statistics	254
sa authentication-hex	255
sa duration	256
sa encryption-hex	257
sa spi	258
security acl	258
transform	259
tunnel local	260
tunnel remote	261
IKE configuration commands	262
authentication-algorithm	262
authentication-method	262
certificate domain	263
dh	263
display ike dpd	264
display ike peer	265
display ike proposal	266
display ike sa	267
dpd	270
encryption-algorithm	271

exchange-mode	272
id-type	272
ike dpd	273
ike local-name	273
ike next-payload check disabled	274
ike peer (system view)	275
ike proposal	275
ike sa keepalive-timer interval	276
ike sa keepalive-timer timeout	276
ike sa nat-keepalive-timer interval	277
interval-time	278
local-address	278
local-name	279
nat traversal	280
peer	280
pre-shared-key	281
proposal (IKE peer view)	281
remote-address	282
remote-name	283
reset ike sa	284
sa duration	285
time-out	285
SSH2.0 configuration commands	287
SSH2.0 server configuration commands	287
display ssh server	287
display ssh user-information	288
ssh server authentication-retries	289
ssh server authentication-timeout	290
ssh server compatible-ssh 1x	291
ssh server dscp	291
ssh server enable	292
ssh server ipv6 dscp	292
ssh server rekey-interval	293
ssh user	294
SSH2.0 client configuration commands	295
display ssh client source	295
display ssh server-info	296
ssh client authentication server	297
ssh client dscp	298
ssh client first-time	298
ssh client ipv6 dscp	299
ssh client ipv6 source	300
ssh client source	300
ssh2	301
ssh2 ipv6	302
SFTP configuration commands	305
SFTP server configuration commands	305
sftp server enable	305
sftp server idle-timeout	305
SFTP client configuration commands	306
bye	306
cd	307
cdup	307

delete	308
dir	308
display sftp client source	309
exit	310
get	310
help	311
ls	311
mkdir	312
put	312
pwd	313
quit	313
remove	314
rename	314
rmdir	315
sftp	315
sftp client dscp	317
sftp client ipv6 dscp	317
sftp client ipv6 source	318
sftp client source	318
sftp ipv6	319
SCP configuration commands	321
SCP client configuration commands	321
scp	321
SSL configuration commands	323
ciphersuite	323
client-verify enable	324
client-verify weaken	325
close-mode wait	325
display ssl client-policy	326
display ssl server-policy	327
handshake timeout	328
pki-domain	329
prefer-cipher	330
server-verify enable	331
session	331
ssl client-policy	332
ssl server-policy	333
version	333
TCP attack protection configuration commands	335
display tcp status	335
tcp syn-cookie enable	336
IP source guard configuration commands	337
display ip source binding	337
display ipv6 source binding	338
ip source binding (interface view)	340
ip source binding (system view)	341
ip verify source	342
ip verify source max-entries	342
ipv6 source binding (interface view)	343
ipv6 source binding (system view)	344
ipv6 verify source	345
ipv6 verify source max-entries	346

ARP attack protection configuration commands	347
ARP defense against IP packet attacks configuration commands	347
arp resolving-route enable	347
arp source-suppression enable	347
arp source-suppression limit	348
display arp source-suppression	348
ARP packet rate limit configuration commands	349
arp rate-limit	349
arp rate-limit information	350
Source MAC address based ARP attack detection configuration commands	351
arp anti-attack source-mac	351
arp anti-attack source-mac aging-time	351
arp anti-attack source-mac exclude-mac	352
arp anti-attack source-mac threshold	352
display arp anti-attack source-mac	353
ARP packet source mac address consistency check configuration commands	354
arp anti-attack valid-check enable	354
ARP active acknowledgement configuration commands	355
arp anti-attack active-ack enable	355
ARP detection configuration commands	355
arp detection	355
arp detection enable	356
arp detection trust	357
arp detection validate	357
arp restricted-forwarding enable	358
display arp detection	359
display arp detection statistics	359
reset arp detection statistics	360
ARP automatic scanning and fixed ARP configuration commands	361
arp fixup	361
arp scan	362
ARP gateway protection configuration commands	363
arp filter source	363
ARP filtering configuration commands	363
arp filter binding	363
ND attack defense configuration commands	365
Source MAC consistency check commands	365
ipv6 nd mac-check enable	365
ND detection configuration commands	365
display ipv6 nd detection	365
display ipv6 nd detection statistics	366
ipv6 nd detection enable	367
ipv6 nd detection trust	368
reset ipv6 nd detection statistics	368
SAVI configuration commands	370
ipv6 savi dad-delay	370
ipv6 savi dad-preparedelay	370
ipv6 savi down-delay	371
ipv6 savi strict	371
Blacklist configuration commands	373
blacklist enable	373
blacklist ip	373
display blacklist	374

FIPS configuration commands 376

 display fips status376

 fips mode enable.....376

 fips self-test377

Support and other resources 378

 Contacting HP378

 Subscription service378

 Related information378

 Documents378

 Websites.....378

 Conventions379

Index 381

AAA configuration commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

General AAA configuration commands

aaa nas-id profile

Syntax

```
aaa nas-id profile profile-name  
undo aaa nas-id profile profile-name
```

View

System view

Default level

2: System level

Parameters

profile-name: Name of the NAS ID profile, a case-insensitive string of 1 to 16 characters.

Description

Use **aaa nas-id profile** to create a NAS ID profile and enter its view. A NAS ID profile maintains the bindings between NAS IDs and VLANs.

Use **undo aaa nas-id profile** to remove a NAS ID profile.

Related commands: **nas-id bind vlan**.

Examples

```
# Create a NAS ID profile named aaa.  
<Sysname> system-view  
[Sysname] aaa nas-id profile aaa  
[Sysname-nas-id-prof-aaa]
```

access-limit enable

Syntax

```
access-limit enable max-user-number  
undo access-limit enable
```

View

ISP domain view

Default level

2: System level

Parameters

max-user-number: Maximum number of online users that the ISP domain can accommodate, in the range of 1 to 2147483646.

Description

Use **access-limit enable** to set the maximum number of online users in an ISP domain. After the number of online users reaches the allowed maximum number, no more users are accepted.

Use **undo access-limit enable** to restore the default.

By default, there is no limit to the number of online users in an ISP domain.

System resources are limited, and user connections may compete for network resources when there are many users. Setting a proper limit to the number of online users helps provide reliable system performance.

Related commands: **display domain**.

Examples

Set a limit of 500 user connections for ISP domain **test**.

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] access-limit enable 500
```

accounting command

Syntax

accounting command hwtacacs-scheme *hwtacacs-scheme-name*

undo accounting command

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **accounting command** to specify the command line accounting method.

Use **undo accounting command** to restore the default.

By default, the default accounting method for the ISP domain is used for command line accounting.

The specified HWTACACS scheme must have been configured.

Command line accounting can use only a HWTACACS scheme.

Related commands: **accounting default** and **hwtacacs scheme**.

Examples

Configure ISP domain **test** to use HWTACACS scheme **hwtac** for command line accounting.

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] accounting command hwtacacs-scheme hwtac
```

accounting default

Syntax

accounting default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting default

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform any accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **accounting default** to configure the default accounting method for an ISP domain.

Use **undo accounting default** to restore the default.

By default, the default accounting method of an ISP domain is **local**.

The specified RADIUS or HWTACACS scheme must have been configured.

The default accounting method is used for all users who support the specified accounting method and have no specific accounting method configured.

Local accounting is only used for monitoring and controlling the number of local user connections. It does not provide the statistics function that the accounting feature generally provides.

Related commands: **local-user**, **hwtacacs scheme**, and **radius scheme**.

Examples

Configure the default accounting method for ISP domain **test** to use RADIUS accounting scheme **rd** and use local accounting as the backup.

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] accounting default radius-scheme rd local
```

accounting lan-access

Syntax

```
accounting lan-access { local | none | radius-scheme radius-scheme-name [ local | none ] }  
undo accounting lan-access
```

View

ISP domain view

Default level

2: System level

Parameters

local: Performs local accounting.

none: Does not perform any accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **accounting lan-access** to configure the accounting method for LAN users.

Use **undo accounting lan-access** to restore the default.

By default, the default accounting method for the ISP domain is used for LAN users.

The specified RADIUS scheme must have been configured.

Related commands: **local-user**, **accounting default**, and **radius scheme**.

Examples

Configure ISP domain **test** to use local accounting for LAN users.

```
<Sysname> system-view  
[Sysname] domain test  
[Sysname-isp-test] accounting lan-access local
```

Configure ISP domain **test** to use RADIUS accounting scheme **rd** for LAN users and use local accounting as the backup.

```
<Sysname> system-view  
[Sysname] domain test  
[Sysname-isp-test] accounting lan-access radius-scheme rd local
```

accounting login

Syntax

```
accounting login { hwtacacs-scheme hwtacacs-scheme-name [ local ] | local | none | radius-scheme  
radius-scheme-name [ local ] }  
undo accounting login
```

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform any accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **accounting login** to configure the accounting method for login users through the console port or Telnet.

Use **undo accounting login** to restore the default.

By default, the default accounting method for the ISP domain is used for login users.

The specified RADIUS or HWTACACS scheme must have been configured.

Accounting is not supported for login users who use FTP.

Related commands: **local-user**, **accounting default**, **hwtacacs scheme**, and **radius scheme**.

Examples

Configure ISP domain **test** to use local accounting for login users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting login local
```

Configure ISP domain **test** to use RADIUS accounting scheme **rd** for login users and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting login radius-scheme rd local
```

accounting optional

Syntax

accounting optional

undo accounting optional

View

ISP domain view

Default level

2: System level

Parameters

None

Description

Use **accounting optional** to enable the accounting optional feature.

Use **undo accounting optional** to disable the feature.

By default, the feature is disabled.

After you configure the **accounting optional** command for a domain, a user who would otherwise be disconnected can continue to use the network resources when no accounting server is available or when communication with the current accounting server fails. However, the switch no longer sends real-time accounting updates for the user. The accounting optional feature applies to scenarios where accounting is not important.

After you configure the **accounting optional** command, the setting configured by the **access-limit** command in local user view is not effective.

Examples

```
# Enable the accounting optional feature for users in domain test.
```

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] accounting optional
```

accounting portal

Syntax

accounting portal { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting portal

View

ISP domain view

Default level

2: System level

Parameters

local: Performs local accounting.

none: Does not perform any accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **accounting portal** to configure the accounting method for portal users.

Use **undo accounting portal** to restore the default.

By default, the default accounting method for the ISP domain is used for portal users.

The specified RADIUS scheme must have been configured.

Related commands: **local-user**, **accounting default**, and **radius scheme**.

Examples

```
# Configure ISP domain test to use local accounting for portal users.
```

```
<Sysname> system-view
```

```
[Sysname] domain test
[Sysname-isp-test] accounting portal local

# Configure ISP domain test to use RADIUS scheme rd for accounting on portal users and use local
accounting as the backup.

<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting portal radius-scheme rd local
```

authentication default

Syntax

```
authentication default { hwtacacs-scheme hwtacacs-scheme-name [ local ] | local | none |
radius-scheme radius-scheme-name [ local ] }
```

undo authentication default

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authentication default** to configure the default authentication method for an ISP domain.

Use **undo authentication default** to restore the default.

By default, the default authentication method of an ISP domain is **local**.

The specified RADIUS or HWTACACS scheme must have been configured.

The default authentication method is used for all users who support the specified authentication method and have no specific authentication method configured.

Related commands: **local-user**, **hwtacacs scheme**, and **radius scheme**.

Examples

```
# Configure the default authentication method for ISP domain test to use RADIUS authentication scheme
rd and use local authentication as the backup.
```

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication default radius-scheme rd local
```

authentication lan-access

Syntax

```
authentication lan-access { local | none | radius-scheme radius-scheme-name [ local | none ] }  
undo authentication lan-access
```

View

ISP domain view

Default level

2: System level

Parameters

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authentication lan-access** to configure the authentication method for LAN users.

Use **undo authentication lan-access** to restore the default.

By default, the default authentication method for the ISP domain is used for LAN users.

The specified RADIUS scheme must have been configured.

Related commands: **local-user**, **authentication default**, and **radius scheme**.

Examples

Configure ISP domain **test** to use local authentication for LAN users.

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] authentication lan-access local
```

Configure ISP domain **test** to use RADIUS authentication scheme **rd** for LAN users and use local authentication as the backup.

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] authentication lan-access radius-scheme rd local
```

authentication login

Syntax

```
authentication login { hwtaacs-scheme hwtaacs-scheme-name [ local ] | local | none | radius-scheme radius-scheme-name [ local ] }
```

```
undo authentication login
```

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authentication login** to configure the authentication method for login users through the console port, Telnet, or FTP.

Use **undo authentication login** to restore the default.

By default, the default authentication method for the ISP domain is used for login users.

The specified RADIUS or HWTACACS scheme must have been configured.

Related commands: **local-user**, **authentication default**, **hwtacacs scheme**, and **radius scheme**.

Examples

Configure ISP domain **test** to use local authentication for login users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication login local
```

Configure ISP domain **test** to use RADIUS authentication scheme **rd** for login users and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication login radius-scheme rd local
```

authentication portal

Syntax

authentication portal { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication portal

View

ISP domain view

Default level

2: System level

Parameters

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authentication portal** to configure the authentication method for portal users.

Use **undo authentication portal** to restore the default.

By default, the default authentication method for the ISP domain is used for portal users.

The specified RADIUS scheme must have been configured.

Related commands: **local-user**, **authentication default**, and **radius scheme**.

Examples

Configure ISP domain **test** to use local authentication for portal users.

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] authentication portal local
```

Configure ISP domain **test** to use RADIUS scheme **rd** for authentication of portal users and use local authentication as the backup.

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] authentication portal radius-scheme rd local
```

authentication super

Syntax

```
authentication super { hwtacacs-scheme hwtacacs-scheme-name | radius-scheme radius-scheme-name }
```

```
undo authentication super
```

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authentication super** to configure the authentication method for user privilege level switching.

Use **undo authentication super** to restore the default.

By default, the default authentication method for the ISP domain is used for user privilege level switching authentication.

The specified RADIUS or HWTACACS authentication scheme must have been configured.

Related commands: **hwtacacs scheme** and **radius scheme**; **super authentication-mode** (*Fundamentals Command Reference*).

Examples

```
# Configure ISP domain test to use HWTACACS scheme tac for user privilege level switching authentication.
```

```
<Sysname> system-view
```

```
[Sysname] super authentication-mode scheme
```

```
[Sysname] domain test
```

```
[Sysname-domain-test] authentication super hwtacacs-scheme tac
```

authorization command

Syntax

```
authorization command { hwtacacs-scheme hwtacacs-scheme-name [ local | none ] | local | none }
```

```
undo authorization command
```

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform any authorization exchange. In this case, an authenticated user can access only commands of Level 0.

Description

Use **authorization command** to configure the command line authorization method.

Use **undo authorization command** to restore the default.

By default, the default authorization method for the ISP domain is used for command line authorization.

The specified HWTACACS scheme must have been configured.

With command line authorization configured, a user who has logged in to the switch can execute only the commands with a level lower than or equal to that of the local user.

Related commands: **local-user**, **authorization default**, and **hwtacacs scheme**.

Examples

```
# Configure ISP domain test to use local command line authorization.
```

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] authorization command local
```

```
# Configure ISP domain test to use HWTACACS scheme hwtac for command line authorization and use local authorization as the backup.
```

```
<Sysname> system-view
```

```
[Sysname] domain test
[Sysname-isp-test] authorization command hwtacacs-scheme hwtac local
```

authorization default

Syntax

```
authorization default { hwtacacs-scheme hwtacacs-scheme-name [ local ] | local | none | radius-scheme radius-scheme-name [ local ] }
```

```
undo authorization default
```

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform any authorization exchange. After passing authentication, non-login users can access the network, FTP users can access the root directory of the switch, and other login users can access only the commands of Level 0.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authorization default** to configure the default authorization method for an ISP domain.

Use **undo authorization default** to restore the default.

By default, the default authorization method for the ISP domain of an ISP domain is **local**.

The specified RADIUS or HWTACACS scheme must have been configured.

The default authorization method is used for all users who support the specified authorization method and have no specific authorization method are configured.

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

Related commands: **local-user**, **hwtacacs scheme**, and **radius scheme**.

Examples

Configure the default authorization method for ISP domain **test** to use RADIUS authorization scheme **rd** and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization default radius-scheme rd local
```


authorization lan-access

Syntax

```
authorization lan-access { local | none | radius-scheme radius-scheme-name [ local | none ] }  
undo authorization lan-access
```

View

ISP domain view

Default level

2: System level

Parameters

local: Performs local authorization.

none: Does not perform any authorization exchange. In this case, an authenticated LAN user can access the network directly.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authorization lan-access** to configure the authorization method for LAN users.

Use **undo authorization lan-access** to restore the default.

By default, the default authorization method for the ISP domain is used for LAN users.

The specified RADIUS scheme must have been configured.

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

Related commands: **local-user**, **authorization default**, and **radius scheme**.

Examples

Configure ISP domain **test** to use local authorization for LAN users.

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] authorization lan-access local
```

Configure ISP domain **test** to use RADIUS authorization scheme **rd** for LAN users and use local authorization as the backup.

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] authorization lan-access radius-scheme rd local
```

authorization login

Syntax

```
authorization login { hwtacacs-scheme hwtacacs-scheme-name [ local ] | local | none | radius-scheme radius-scheme-name [ local ] }  
undo authorization login
```

View

ISP domain view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, a case-insensitive string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform any authorization exchange. After passing authentication, FTP users can access the root directory of the switch, and other login users can access only the commands of Level 0.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authorization login** to configure the authorization method for login users through the console port, Telnet, or FTP.

Use **undo authorization login** to restore the default.

By default, the default authorization method for the ISP domain is used for login users.

The specified RADIUS or HWTACACS scheme must have been configured.

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

Related commands: **local-user**, **authorization default**, **hwtacacs scheme**, and **radius scheme**.

Examples

Configure ISP domain **test** to use local authorization for login users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization login local
```

Configure ISP domain **test** to use RADIUS authorization scheme **rd** for login users and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization login radius-scheme rd local
```

authorization portal

Syntax

authorization portal { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization portal

View

ISP domain view

Default level

2: System level

Parameters

local: Performs local authorization.

none: Does not perform any authorization exchange. In this case, an authenticated portal user can access the network directly.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Description

Use **authorization portal** to configure the authorization method for portal users.

Use **undo authorization portal** to restore the default.

By default, the default authorization method for the ISP domain is used for portal users.

The specified RADIUS scheme must have been configured.

The RADIUS authorization configuration takes effect only when the authentication method and authorization method of the ISP domain use the same RADIUS scheme.

Related commands: **local-user**, **authorization default**, and **radius scheme**.

Examples

Configure ISP domain **test** to use local authorization for portal users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization portal local
```

Configure ISP domain **test** to use RADIUS scheme **rd** for authorization of portal users and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization portal radius-scheme rd local
```

authorization-attribute user-profile

Syntax

authorization-attribute user-profile *profile-name*

undo authorization-attribute user-profile

View

ISP domain view

Default level

3: Manage level

Parameters

profile-name: Name of the user profile, a case-sensitive string of 1 to 31 characters. For more information about user profile configuration, see *Security Configuration Guide*.

Description

Use **authorization-attribute user-profile** to specify the default authorization user profile for an ISP domain.

Use **undo authorization-attribute user-profile** to restore the default.

By default, an ISP domain has no default authorization user profile.

After a user of an ISP domain passes authentication, if the server (or the switch in the case of local authentication) does not authorize any user profile to the ISP domain, the system uses the user profile specified by the **authorization-attribute user-profile** command as that of the ISP domain.

If you execute the command multiple times, the most recent configuration takes effect.

Examples

```
# Specify the default authorization user profile for domain test as profile1.  
<Sysname> system-view  
[Sysname] domain test  
[Sysname-isp-test] authorization-attribute user-profile profile1
```

cut connection

Syntax

cut connection { **access-type** { **dot1x** | **mac-authentication** | **portal** } | **all** | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* | **vlan** *vlan-id* } [**slot** *slot-number*]

View

System view

Default level

2: System level

Parameters

access-type: Specifies the user connections of the specified access type.

- **dot1x**: Indicates 802.1X authentication.
- **mac-authentication**: Indicates MAC address authentication.
- **portal**: Indicates portal authentication.

all: Specifies all user connections.

domain *isp-name*: Specifies the user connections of an ISP domain. The *isp-name* argument refers to the name of an existing ISP domain and is a string of 1 to 24 characters.

interface *interface-type interface-number*: Specifies the user connections on an interface. Only Layer 2 Ethernet interfaces are supported.

ip *ip-address*: Specifies the user connections for an IP address.

mac *mac-address*: Specifies the user connections for a MAC address, with *mac-address* in the format H-H-H.

ucibindex *ucib-index*: Specifies the user connection that uses the connection index. The *ucib-index* argument ranges from 0 to 4294967295.

user-name *user-name*: Specifies the user connections that use the username. The *user-name* argument is a case-sensitive string of 1 to 80 characters. For a username entered without a domain name, the system assumes that the user is in the default domain or the mandatory authentication domain.

vlan *vlan-id*: Specifies the user connections of a VLAN, with *vlan-id* ranging from 1 to 4094.

slot slot-number: Specifies the user connections on an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

Description

Use **cut connection** to tear down user connections forcibly.

This command applies only to LAN access and portal.

For 802.1X users whose usernames carry the version number or contain spaces, you cannot cut the connections by username.

For 802.1X users whose usernames use a slash (/) or backslash (\) as the domain name delimiter, you cannot cut their connections by username. For example, the **cut connection user-name aaa\bbb** command cannot cut the connections of the user **aaa\bbb**.

An interface that is configured with a mandatory authentication domain treats users of the corresponding access type as users in the mandatory authentication domain. For example, if you configure an 802.1X mandatory authentication domain on an interface, the interface uses the domain's AAA methods for all its 802.1X users. To cut connections of such users, use the **cut connection domain isp-name** command and specify the mandatory authentication domain.

Related commands: **display connection** and **service-type**.

Examples

```
# Tear down all connections of ISP domain test.
```

```
<Sysname> system-view
```

```
[Sysname] cut connection domain test
```

display connection

Syntax

display connection [**access-type** { **dot1x** | **mac-authentication** | **portal** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* | **vlan** *vlan-id*] [**slot** *slot-number*] [[{ **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

access-type: Specifies the user connections of the specified access type.

- **dot1x:** Indicates 802.1X authentication.
- **mac-authentication:** Indicates MAC address authentication.
- **portal:** Indicates portal authentication.

domain *isp-name:* Specifies the user connections of an ISP domain. The *isp-name* argument refers to the name of an existing ISP domain and is a case-insensitive string of 1 to 24 characters.

interface *interface-type interface-number:* Specifies the user connections on an interface. Only Layer 2 Ethernet interfaces are supported.

ip *ip-address:* Specifies the user connections of an IP address.

mac *mac-address*: Specifies the user connections of a MAC address, with *mac-address* in the format H-H-H.

ucibindex *ucib-index*: Specifies the user connection that uses the connection index. The value range is from 0 to 4294967295.

user-name *user-name*: Specifies the user connections that use the username. The *user-name* argument is a case-sensitive string of 1 to 80 characters. For a username entered without a domain name, the system assumes that the user is in the default domain name or the mandatory authentication domain.

vlan *vlan-id*: Specifies the user connections of a VLAN, with *vlan-id* ranging from 1 to 4094.

slot *slot-number*: Specifies the user connections on an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display connection** to display information about AAA user connections.

This command does not display information about FTP user connections.

With no parameter specified, this command displays brief information about all AAA user connections.

If you specify the **ucibindex** *ucib-index* option, this command displays detailed information. Otherwise, this command displays brief information.

If an interface is configured with a mandatory authentication domain (for example, an 802.1X mandatory authentication domain), the switch uses the mandatory authentication domain to perform authentication, authorization, and accounting for users who access the interface through the specified access type. To display connections of such users, use the **display connection domain** *isp-name* command and specify the mandatory authentication domain.

How the switch displays the username of a user on an interface configured with a mandatory authentication domain depends on the format of the username entered by the user at login:

- If the username does not contain the character @, the switch displays the username in the format *username @mandatory authentication domain name*.
- If the username contains the character @, the switch displays the entered username. For example, if a user entered the username **aaa@123** at login and the name of the mandatory authentication domain is **dom**, the switch displays the username **aaa@123**, rather than **aaa@123@dom**.

For 802.1X users whose usernames use a slash (/) or backslash (\) as the domain name delimiter, you cannot query the connections by username. For example, the **display connection user-name** *aaa\bbb* command cannot display the connections of the user **aaa\bbb**.

Related commands: **cut connection**.

Examples

Display information about all AAA user connections.

```
<Sysname> display connection
```

```
Slot: 1
Index=0 , Username=telnet@system
IP=10.0.0.1
IPv6=N/A
```

```
Total 1 connection(s) matched on slot 1.
Total 1 connection(s) matched.
```

Display information about AAA user connections using the index of 0.

```
<Sysname> display connection ucibindex 0
Slot: 1
Index=0 , Username=telnet@system
IP=10.0.0.1
IPv6=N/A
Access=Admin ,AuthMethod=PAP
Port Type=Virtual ,Port Name=N/A
Initial VLAN=999, Authorized VLAN=20
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
Start=2011-01-16 10:53:03 ,Current=2011-01-16 10:57:06 ,Online=00h04m03s
Total 1 connection matched.
Slot: 2
Total 0 connection matched.
```

Table 1 Command output

Field	Description
Slot	IRF member device ID
Username	Username of the connection, in the format <i>username@domain</i> .
MAC	MAC address of the user.
IP	IPv4 address of the user.
IPv6	IPv6 address of the user.
Access	User access type.
ACL Group	Authorization ACL group. If no authorization ACL group is assigned, this field displays Disable .
User Profile	Authorization user profile.
CAR(kbps)	Authorized CAR parameters.
UpPeakRate	Uplink peak rate.
DnPeakRate	Downlink peak rate.
UpAverageRate	Uplink average rate.
DnAverageRate	Downlink average rate.

display domain

Syntax

```
display domain [ isp-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

isp-name: Name of an existing ISP domain, a string of 1 to 24 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display domain** to display the configuration of ISP domains.

If you do not specify any ISP domain, the command displays the configuration of all ISP domains.

Related commands: **access-limit enable**, **domain**, and **state**.

Examples

Display the configuration of all ISP domains.

```
<Sysname> display domain
```

```
0  Domain : system
   State : Active
   Access-limit : Disabled
   Accounting method : Required
   Default authentication scheme : local
   Default authorization scheme : local
   Default accounting scheme : local
   Domain User Template:
   Idle-cut : Disabled
   Self-service : Disabled
   Authorization attributes :

1  Domain : test
   State : Active
   Access-limit : Disabled
   Accounting method : Required
   Default authentication scheme : local
   Default authorization scheme : local
   Default accounting scheme : local
```



```

Lan-access authentication scheme : radius:test, local
Lan-access authorization scheme  : hwtacacs:hw, local
Lan-access accounting scheme    : local
Domain User Template:
Idle-cut : Disabled
Self-service : Disabled
Authorization attributes :
    User-profile : profile1

Default Domain Name: system
Total 2 domain(s).

```

Table 2 Command output

Field	Description
Domain	ISP domain name.
State	Status of the ISP domain: active or blocked. Users in an active ISP domain can request network services, and users in a blocked ISP domain cannot.
Access-limit	Limit on the number of user connections. If there is no limit on the number, this field displays Disabled .
Accounting method	Indicates whether accounting is required. If accounting is required, when no accounting server is available or communication with the accounting server fails, user connections are torn down. Otherwise, users can continue to use network services.
Default authentication scheme	Default authentication method.
Default authorization scheme	Default authorization method.
Default accounting scheme	Default accounting method.
DSCP	DSCP value in IP packets from authenticated users in the ISP domain.
Lan-access authentication scheme	Authentication method for LAN users.
Lan-access authorization scheme	Authorization method for LAN users.
Lan-access accounting scheme	Accounting method for LAN users.
Domain User Template	Indicates some functions and attributes set for users in the domain.
Idle-cut	Indicates whether the idle cut function is enabled. With the idle cut function enabled for a domain, the system logs out any user in the domain whose traffic is less than the specified minimum traffic during the idle timeout period.
Self-service	Indicates whether the self service function is enabled. With the self service function enabled, users can launch a browser and enter the self service URL in the address bar to access the self service pages and perform self service operations.
Authorization attributes	Default authorization attributes for the ISP domain.
User-profile	Default authorization user profile.

domain

Syntax

domain *isp-name*

undo domain *isp-name*

View

System view

Default level

3: Manage level

Parameters

isp-name: Specifies the ISP domain name, a case-insensitive string of 1 to 24 characters that cannot contain slash (/), backslash (\), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), quotation marks ("), vertical bar (|), or at sign (@).

Description

Use **domain** *isp-name* to create an ISP domain and enter ISP domain view.

Use **undo domain** to remove an ISP domain.

By default, there is a system predefined ISP domain named **system** in the system.

All ISP domains are in active state when they are created.

You cannot delete the system predefined ISP domain **system**, and can only modify its configuration.

To delete the ISP domain that is used as the default ISP domain, you must change it to a non-default ISP domain first by using the **undo domain default enable** command.

Related commands: **state** and **display domain**.

Examples

Create ISP domain **test**, and enter ISP domain view.

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test]
```

domain default enable

Syntax

domain default enable *isp-name*

undo domain default enable

View

System view

Default level

3: Manage level

Parameters

isp-name: Name of the ISP domain, a case-insensitive string of 1 to 24 characters.

Description

Use **domain default enable** to specify the default ISP domain. Users without any domain name carried in the usernames are considered to be in the default domain.

Use **undo domain default enable** to restore the default.

By default, the default ISP domain is the system predefined ISP domain **system**.

There can be only one default ISP domain.

The specified domain must already exist. Otherwise, users without any domain name carried in the username cannot pass authentication.

To delete the ISP domain that is used as the default ISP domain, you must change it to a non-default ISP domain first by using the **domain default disable** command.

Related commands: **domain**, **state**, and **display domain**.

Examples

Create a new ISP domain named **test**, and configure it as the default ISP domain.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] quit
[Sysname] domain default enable test
```

idle-cut enable

Syntax

idle-cut enable *minute* [*flow*]

undo idle-cut enable

View

ISP domain view

Default level

2: System level

Parameters

minute: Idle timeout period, in the range of 1 to 600 minutes.

flow: Minimum traffic during the idle timeout period, which is in the range of 1 to 10240000 bytes and defaults to 10240.

Description

Use **idle-cut enable** to enable the idle cut function and set the relevant parameters. With the idle cut function enabled for a domain, the switch checks the traffic of each online user in the domain at the idle timeout interval, and logs out any user in the domain whose traffic during the idle timeout period is less than the specified minimum traffic.

Use **undo idle-cut enable** to restore the default.

By default, the function is disabled.

You can also set the idle timeout period on the server to make the server log out users whose traffic during the idle timeout period is less than 10240 bytes, but your setting on the server takes effect only when you disable the idle cut function on the switch.

Related commands: **domain**.

Examples

```
# Enable the idle cut function and set the idle timeout period to 50 minutes and the traffic threshold to 1024 bytes for ISP domain test.
```

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] idle-cut enable 50 1024
```

nas-id bind vlan

Syntax

nas-id *nas-identifier* **bind vlan** *vlan-id*

undo nas-id *nas-identifier* **bind vlan** *vlan-id*

View

NAS ID profile view

Default level

2: System level

Parameters

nas-identifier: NAS ID, a case-sensitive string of 1 to 20 characters

vlan-id: ID of the VLAN to be bound with the NAS ID, in the range of 1 to 4094.

Description

Use **nas-id bind vlan** to bind a NAS ID with a VLAN.

Use **undo nas-id bind vlan** to remove a NAS ID-VLAN binding.

By default, no NAS ID-VLAN binding exists.

In a NAS ID profile view, you can configure multiple NAS ID-VLAN bindings.

A NAS ID can be bound with more than one VLAN, but one VLAN can be bound with only one NAS ID. If you bind a VLAN with different NAS IDs, only the last binding takes effect.

Related commands: **aaa nas-id profile**.

Examples

```
# Bind NAS ID 222 with VLAN 2.
```

```
<Sysname> system-view
[Sysname] aaa nas-id profile aaa
[Sysname-nas-id-prof-aaa] nas-id 222 bind vlan 2
```

self-service-url enable

Syntax

self-service-url enable *url-string*

undo self-service-url enable

View

ISP domain view

Default level

2: System level

Parameters

url-string: URL of the self-service server, a string of 1 to 64 characters. It must start with `http://` and contain no question mark. This URL was specified by the RADIUS server administrator during RADIUS server installation.

Description

Use **self-service-url enable** to enable the self-service server location function and specify the URL of the self-service server.

Use **undo self-service-url enable** to restore the default.

By default, the self-service server location function is disabled.

With the self-service function, users can manage and control their accounts and passwords. Only the RADIUS server systems provided by IMC support the self-service function.

Examples

For ISP domain **test**, enable the self-service server location function and specify the URL of the self-service server for changing user password to `http://10.153.89.94/selfservice`.

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] self-service-url enable http://10.153.89.94/selfservice
```

state (ISP domain view)

Syntax

state { active | block }

undo state

View

ISP domain view

Default level

2: System level

Parameters

active: Places the ISP domain in active state to allow the users in the ISP domain to request network services.

block: Places the ISP domain in blocked state to prevent users in the ISP domain from requesting network services.

Description

Use **state** to set the status of an ISP domain.

Use **undo state** to restore the default.

By default, an ISP domain is in active state.

By blocking an ISP domain, you disable users of the domain that are offline from requesting network services. The online users are not affected.

Examples

```
# Place the current ISP domain test to the state of blocked.
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] state block
```

Local user configuration commands

access-limit

Syntax

```
access-limit max-user-number
undo access-limit
```

View

Local user view

Default level

3: Manage level

Parameters

max-user-number: Maximum number of concurrent users of the current local user account, in the range of 1 to 1024.

Description

Use **access-limit** to limit the number of concurrent users of a local user account.

Use **undo access-limit** to remove the limitation.

By default, there is no limit to the number of users who concurrently use the same local user account.

This command takes effect only when local accounting is used for the user account.

This limit is not effective for FTP users because accounting is not available for FTP users.

Related commands: **display local-user**.

Examples

```
# Limit the maximum number of concurrent users of local user account abc to 5.
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] access-limit 5
```

authorization-attribute (local user view/user group view)

Syntax

```
authorization-attribute { acl acl-number | idle-cut minute | level level | user-profile profile-name |  
  user-role { guest | guest-manager | security-audit } | vlan vlan-id | work-directory directory-name } *  
undo authorization-attribute { acl | idle-cut | level | user-profile | user-role | vlan | work-directory }  
*
```

View

Local user view, user group view

Default level

3: Manage level

Parameters

acl *acl-number*: Specifies the authorization ACL. The ACL number must be in the range of 2000 to 5999. After passing authentication, a local user is authorized to access the network resources specified by this ACL.

idle-cut *minute*: Sets the idle timeout period. With the idle cut function enabled, an online user whose idle period exceeds the specified idle timeout period is logged out. The *minute* argument indicates the idle timeout period, in the range of 1 to 120 minutes.

level *level*: Specifies the user level, which can be 0 for visit level, 1 for monitor level, 2 for system level, and 3 for manage level. A smaller number means a lower level. If the user interfaces' authentication mode is **scheme**, which commands users can use after login in depends on this argument. By default, the user level is 0, and users can use only commands of level 0 after login.

user-profile *profile-name*: Specifies the authorization user profile. *profile-name* is a case-sensitive string of 1 to 32 characters. It can contain letters, digits, and underscores (_) and must start with a letter. After a user passes authentication and gets online, the switch uses the settings in the user profile to restrict the access behavior of the user. For more information about user profiles, see *Security Configuration Guide*.

user-role: Specifies the role for the local user. This keyword is available in only local user view. Users playing different roles can access different levels of commands. If you specify no role for a local user, the access right of the user after login depends on other authorization attributes. Supported roles include:

- **guest**: A guest user account is usually created through the Web interface.
- **guest-manager**: After passing authentication, a guest manager can only use the Web interface to access guest-related pages to, for example, create, modify, or change guest user accounts.
- **security-audit**: After passing authentication, a security log administrator can manage security log files, for example, save security log files. For more information about the commands that a security log administrator can use, see *Network Management and Monitoring Command Reference*.

vlan *vlan-id*: Specifies the authorized VLAN. The *vlan-id* argument is in the range of 1 to 4094. After passing authentication, a local user can access the resources in this VLAN.

work-directory *directory-name*: Specifies the work directory, if the user or users use the FTP or SFTP service. The *directory-name* argument is a case-insensitive string of 1 to 135 characters. The directory must already exist. By default, an FTP or SFTP user can access the root directory of the switch.

Description

Use **authorization-attribute** to configure authorization attributes for the local user or user group. After the local user or a local user of the user group passes authentication, the switch assigns these attributes to the user.

Use **undo authorization-attribute** to remove authorization attributes and restore the defaults.

By default, no authorization attribute is configured for a local user or user group.

Every configurable authorization attribute has its definite application environments and purposes. Consider the service types of users when assigning authorization attributes.

Authorization attributes configured for a user group are effective for all local users in the group. You can group local users to improve configuration and management efficiency.

An authorization attribute configured in local user view takes precedence over the same attribute configured in user group view. If an authorization attribute is configured in user group view but not in local user view, the setting in user group view takes effect.

If only one user is playing the role of security log administrator in the system, you cannot delete the user account, or remove or change the user's role, unless you configure another user as a security log administrator first.

A local user can play only one role at a moment. If you execute the command multiple times, the most recent configuration takes effect.

Examples

Configure the authorized VLAN of local user **abc** as VLAN 2.

```
<Sysname> system-view
```

```
[Sysname] local-user abc
```

```
[Sysname-luser-abc] authorization-attribute vlan 2
```

Configure the authorized VLAN of user group **abc** as VLAN 3.

```
<Sysname> system-view
```

```
[Sysname] user-group abc
```

```
[Sysname-ugroup-abc] authorization-attribute vlan 3
```

bind-attribute

Syntax

bind-attribute { **ip** *ip-address* | **location port** *slot-number subslot-number port-number* | **mac** *mac-address* | **vlan** *vlan-id* } *

undo bind-attribute { **ip** | **location** | **mac** | **vlan** } *

View

Local user view

Default level

3: Manage level

Parameters

ip *ip-address*: Specifies the IP address of the user.

location port *slot-number subslot-number port-number*: Specifies the port to which the user is bound, where *slot-number* is in the range of 0 to 255, *subslot-number* is in the range of 0 to 15, and *port-number* is in the range of 0 to 255.

mac *mac-address*: Specifies the MAC address of the user in the format H-H-H.

vlan *vlan-id*: Specifies the VLAN to which the user belongs, where *vlan-id* is in the range of 1 to 4094.

Description

Use **bind-attribute** to configure binding attributes for a local user.

Use **undo bind-attribute** to remove binding attributes of a local user.

By default, no binding attribute is configured for a local user.

Binding attributes are checked upon authentication of a local user. If the binding attributes of a local user do not match the configured ones, the user fails the checking and the authentication.

Binding attribute checking does not take the service types of the users into account. A configured binding attribute is effective for all types of users. Be cautious when deciding which binding attributes should be configured for which type of local users. For example, an IP address binding applies only to 802.1X authentication that supports IP address upload. If you configure an IP address binding for an authentication method that does not support IP address upload, for example, MAC authentication, the local authentication fails.

Examples

```
# Configure the bound IP of local user abc as 3.3.3.3.
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] bind-attribute ip 3.3.3.3
```

display local-user

Syntax

```
display local-user [ idle-cut { disable | enable } | service-type { ftp | lan-access | portal | ssh | telnet | terminal | web } | state { active | block } | user-name user-name | vlan vlan-id ] [ slot slot-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

idle-cut { **disable** | **enable** }: Specifies local users with the idle cut function disabled or enabled.

service-type: Specifies the local users who use a specific type of service.

- **ftp**: FTP users.
- **lan-access**: Users accessing the network through Ethernet, such as 802.1X users.
- **portal**: Portal users.
- **ssh**: SSH users.
- **telnet**: Telnet users.
- **terminal**: Users logging in through the console port.
- **web**: Web users.

state { **active** | **block** }: Specifies local users in the state of active or blocked. A local user in active state can access network services, but a local user in blocked state cannot.

user-name *user-name*: Specifies all local users using the specified username. The username is a case-sensitive string of 1 to 55 characters and does not contain the domain name.

vlan *vlan-id*: Specifies all local users in a VLAN. The VLAN ID ranges from 1 to 4094.

slot *slot-number*: Specifies the local users on an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display local-user** to display configuration and statistics information about local users.

If you do not specify any parameter, the command displays information about all local users.

Related commands: **local-user**.

Examples

Display information about all local users.

```
<Sysname> display local-user
```

The contents of local user abc:

```
State:                Active
ServiceType:          lan-access
Access-limit:         Enabled           Current AccessNum: 0
Max AccessNum:        300
User-group:           system
Bind attributes:
  IP address:          1.2.3.4
  Bind location:       1/4/1 (SLOT/SUBSLOT/PORT)
  MAC address:         0001-0002-0003
  Vlan ID:             100
```

Authorization attributes:

```
Idle TimeOut:         10(min)
Work Directory:       flash:/
User Privilege:       3
Acl ID:               2000
Vlan ID:              100
User Profile:         prof1
Expiration date:      12:12:12-2018/09/16
Password aging:       Enabled (30 days)
Password length:      Enabled (4 characters)
Password composition: Enabled (4 types, 2 characters per type)
```

Total 1 local user(s) matched.

Table 3 Command output

Field	Description
State	Status of the local user: active or blocked.
ServiceType	Service types that the local user can use, including FTP, LAN access, portal, SSH, Telnet, terminal, and Web.
Access-limit	Whether or not to limit the number of concurrent connections of the username.
Current AccessNum	Number of connections that currently use the username.

Field	Description
Max AccessNum	Maximum number of concurrent connections of the username.
Bind attributes	Binding attributes of the local user.
VLAN ID	VLAN to which the user is bound.
Calling Number	Calling number bound for the ISDN user.
Authorization attributes	Authorization attributes of the local user.
Idle TimeOut	Idle timeout period of the user, in minutes.
Work Directory	Directory that the FTP user can access.
VLAN ID	Authorized VLAN of the local user.
User Profile	User profile for local user authorization.
Expiration date	Expiration time of the local user.
Password aging	Aging time of the local user password.
Password length	Minimum length of the local user password.
Password composition	Password composition policy of the local user.

display user-group

Syntax

display user-group [*group-name*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

group-name: User group name, a case-insensitive string of 1 to 32 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display user-group** to display user group configuration. If you do not specify any user group name, the command displays information about all users groups.

Related commands: **user-group**.

Examples

Display the configuration of user group **abc**.

```
<Sysname> display user-group abc
```

The contents of user group abc:

Authorization attributes:

```
Idle-cut:          120(min)
Work Directory:    FLASH:
Level:            1
Acl Number:       2000
Vlan ID:          1
User-Profile:     1
Password aging:    Enabled (1 days)
Password length:   Enabled (4 characters)
Password composition: Enabled (1 types, 1 characters per type)
```

Total 1 user group(s) matched.

Table 4 Command output

Field	Description
Idle-cut	Idle timeout interval, in minutes.
Work Directory	Directory that FTP/SFTP users in the group can access.
Level	Local user level.
ACL Number	Authorization ACL.
VLAN ID	Authorized VLAN.
Password aging	Aging time of the local user password.
Password length	Minimum length of the local user password.
Password composition	Password composition policy of the local users in the group.

expiration-date (local user view)

Syntax

expiration-date *time*

undo expiration-date

View

Local user view

Default level

3: Manage level

Parameters

time: Expiration time of the local user, in the format HH:MM:SS-MM/DD/YYYY, HH:MM:SS-YYYY/MM/DD, MM/DD/YYYY-HH:MM:SS, or YYYY/MM/DD-HH:MM:SS. HH:MM:SS indicates the time, where HH ranges from 0 to 23, and MM and SS range from 0 to 59. MM/DD/YYYY or YYYY/MM/DD indicates the date, where YYYY ranges from 2000 to 2035, MM ranges from 1 to 12, and the range of DD depends on the month. Except for the zeros in 00:00:00, leading zeros can be omitted. For example, 2:2:0-2011/2/2 equals 02:02:00-2011/02/02.

Description

Use **expiration-date** to set the expiration time of a local user.

Use **undo expiration-date** to remove the configuration.

By default, a local user has no expiration time and no time validity checking is performed.

For temporary network access requirements, create a guest account and specify a validity time and an expiration time for the account to control the validity of the account. When a user uses the guest account for local authentication and passes the authentication, the switch checks whether the current system time is between the validity time and the expiration time. If so, it permits the user to access the network. Otherwise, it denies the access request of the user.

Related commands: **validity-date**.

Examples

```
# Set the expiration time of user abc to 12:10:20 on Jan 31, 2011.
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] expiration-date 12:10:20-2011/01/31
```

group

Syntax

```
group group-name
undo group
```

View

Local user view

Default level

3: Manage level

Parameters

group-name: User group name, a case-insensitive string of 1 to 32 characters.

Description

Use **group** to assign a local user to a user group.

Use **undo group** to restore the default.

By default, a local user belongs to the system default user group **system**.

Examples

```
# Assign local user 111 to user group abc.
<Sysname> system-view
[Sysname] local-user 111
[Sysname-luser-111] group abc
```

group-attribute allow-guest

Syntax

```
group-attribute allow-guest
undo group-attribute allow-guest
```

View

User group view

Default level

3: Manage level

Parameters

None

Description

Use **group-attribute allow-guest** to set the guest attribute for a user group so that guest users created by a guest manager through the Web interface can join the group.

Use **undo group-attribute allow-guest** to restore the default.

By default, the guest attribute is not set for a user group, and guest users created by a guest manager through the Web interface cannot join the group.

The guest attribute is set for the system predefined user group **system** by default, and you cannot remove the attribute for the user group.

Examples

Set the guest attribute for user group **test**.

```
<Sysname> system-view
[Sysname] user-group test
[Sysname-ugroup-test] group-attribute allow-guest
```

local-user

Syntax

local-user *user-name*

undo local-user { *user-name* | **all** [**service-type** { **ftp** | **lan-access** | **portal** | **ssh** | **telnet** | **terminal** | **web** }] }

View

System view

Default level

3: Manage level

Parameters

user-name: Name for the local user, a case-sensitive string of 1 to 55 characters that does not contain the domain name. It cannot contain slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or at sign (@), and cannot be **a**, **al**, or **all**.

all: Specifies all users.

service-type: Specifies the users of a type.

- **ftp**: FTP users.
- **lan-access**: Users accessing the network through an Ethernet, such as 802.1X users.
- **portal**: Portal users.
- **ssh**: SSH users.

- **telnet:** Telnet users.
- **terminal:** Users logging in through the console port.
- **web:** Web users.

Description

Use **local-user** to add a local user and enter local user view.

Use **undo local-user** to remove the specified local users.

By default, no local user is configured.

Related commands: **display local-user** and **service-type**.

Examples

Add a local user named **user1**.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1]
```

password (local user view)

Syntax

In non-FIPS mode:

password [[**hash**] { **cipher** | **simple** } *password*]

undo password

In FIPS mode:

password

View

Local user view

Default level

2: System level

Parameters

hash: Enables hash-based encryption.

{ **cipher** | **simple** } *password*: Specifies a case-sensitive password string. If **hash** is not specified, a ciphertext password must be a string of 1 to 117 characters and a plaintext password must be a string of 1 to 63 characters. If **hash** is specified, a ciphertext password must be a string of 1 to 110 characters and a plaintext password must be a string of 1 to 63 characters.

Description

Use **password** to configure a password for a local user.

Use **undo password** to delete the password of a local user.

If none of the parameters is specified, you enter the interactive mode to set a plaintext password. The interactive mode is available only on switches that support the password control feature. For more information about password control commands, see *Security Command Reference*.

When the password control feature is globally enabled by using the **password-control enable** command, local user passwords, such as the length and complexity, are under the restriction of the password control feature, and are not displayed.

For secrecy, all passwords, including passwords configured in plain text, are saved in cipher text.

Related commands: **display local-user**.

Examples

```
# Set the password of local user user1 to 123456 in plain text.
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] password simple 123456

# Set the password of local user user1 to AAbbcc1234% in interactive mode.
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] password
Password:*****
Confirm :*****
```

service-type

Syntax

In non-FIPS mode:

```
service-type { ftp | lan-access | { ssh | telnet | terminal } * | portal | web }
undo service-type { ftp | lan-access | { ssh | telnet | terminal } * | portal | web }
```

In FIPS mode:

```
service-type { lan-access | { ssh | terminal } * | portal | web }
undo service-type { lan-access | { ssh | terminal } * | portal | web }
```

View

Local user view

Default level

3: Manage level

Parameters

ftp: Authorizes the user to use the FTP service. The user can use the root directory of the FTP server by default.

lan-access: Authorizes the user to use the LAN access service. Such users are mainly Ethernet users, for example, 802.1X users.

ssh: Authorizes the user to use the SSH service.

telnet: Authorizes the user to use the Telnet service.

terminal: Authorizes the user to use the terminal service, allowing the user to log in through the console port.

portal: Authorizes the user to use the portal service.

web: Authorizes the user to use the Web service.

Description

Use **service-type** to specify the service types that a user can use.

Use **undo service-type** to delete service types configured for a user.

By default, a user is authorized with no service.

You can specify multiple service types to the same user.

Examples

```
# Authorize user user1 to use the Telnet service.
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] service-type telnet
```

state (local user view)

Syntax

state { active | block }

undo state

View

Local user view

Default level

2: System level

Parameters

active: Places the local user in active state to allow the local user to request network services.

block: Places the local user in blocked state to prevent the local user from requesting network services.

Description

Use **state** to set the status of a local user.

Use **undo state** to restore the default.

By default, a local user is in active state.

By blocking a user, you disable the user from requesting network services. No other users are affected.

Related commands: **local-user**.

Examples

```
# Place local user user1 to the blocked state.
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] state block
```

user-group

Syntax

user-group group-name

undo user-group group-name

View

System view

Default level

3: Manage level

Parameters

group-name: User group name, a case-insensitive string of 1 to 32 characters.

Description

Use **user-group** to create a user group and enter its view.

Use **undo user-group** to remove a user group.

A user group consists of a group of local users and has a set of local user attributes. You can configure local user attributes for a user group to implement centralized management of user attributes for the local users in the group. Configurable user attributes include password control attributes and authorization attributes.

A user group with one or more local users cannot be removed.

The system predefined user group **system** cannot be removed, but you can change its configurations.

Related commands: **display user-group**.

Examples

Create a user group named **abc** and enter its view.

```
<Sysname> system-view  
[Sysname] user-group abc  
[Sysname-ugroup-abc]
```

validity-date

Syntax

validity-date *time*

undo validity-date

View

Local user view

Default level

3: Manage level

Parameters

time: Validity time of the local user, in the format HH:MM:SS-MM/DD/YYYY, HH:MM:SS-YYYY/MM/DD, MM/DD/YYYY-HH:MM:SS, or YYYY/MM/DD-HH:MM:SS. HH:MM:SS indicates the time, where HH ranges from 0 to 23, and MM and SS range from 0 to 59. MM/DD/YYYY or YYYY/MM/DD indicates the date, where YYYY ranges from 2000 to 2035, MM ranges from 1 to 12, and the range of DD depends on the month. Except for the zeros in 00:00:00, leading zeros can be omitted. For example, 2:2:0-2011/2/2 equals 02:02:00-2011/02/02.

Description

Use **validity-date** to set the validity time of a local user.

Use **undo validity-date** to remove the configuration.

By default, a local user has no validity time and no time validity checking is performed.

For temporary network access requirements, create a guest account and specify a validity time and an expiration time for the account to control the validity of the account. When a user uses the guest account for local authentication and passes the authentication, the switch checks whether the current system time is between the validity time and the expiration time. If so, it permits the user to access the network. Otherwise, it denies the access request of the user.

Related command: **expiration-date**.

Examples

Set the validity time of user **abc** to 12:10:20 on April 30, 2011, and the expiration time to 12:10:20 on May 31, 2011.

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] validity-date 12:10:20-2011/04/30
[Sysname-luser-abc] expiration-date 12:10:20-2011/05/31
```

RADIUS configuration commands

accounting-on enable

Syntax

accounting-on enable [*interval seconds* | **send** *send-times*] *

undo accounting-on enable

View

RADIUS scheme view

Default level

2: System level

Parameters

seconds: Time interval for retransmitting an accounting-on packet in seconds, ranging from 1 to 15. The default setting is 3 seconds.

send-times: Maximum number of accounting-on packet transmission attempts, ranging from 1 to 255. The default setting is 50.

Description

Use **accounting-on enable** to configure the accounting-on feature. This feature enables the switch to, after rebooting, automatically send an accounting-on message to the RADIUS accounting server indicated by the RADIUS scheme to stop accounting for and log out online users.

Use **undo accounting-on enable** to disable the accounting-on feature.

By default, the accounting-on feature is disabled.

Parameters set with the **accounting-on enable** command take effect immediately.

After executing the **accounting-on enable** command, issue the **save** command to make sure that the command takes effect after the switch reboots. For information about the **save** command, see *Fundamentals Command Reference*.

Related commands: **radius scheme**.

Examples

Enable the accounting-on feature for RADIUS authentication scheme **radius1**, set the retransmission interval to 5 seconds, and set the transmission attempts to 15.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] accounting-on enable interval 5 send 15
```

attribute 25 car

Syntax

attribute 25 car
undo attribute 25 car

View

RADIUS scheme view

Default level

2: System level

Parameters

None

Description

Use **attribute 25 car** to specify to interpret the RADIUS class attribute (attribute 25) as CAR parameters.

Use **undo attribute 25 car** to restore the default.

By default, RADIUS attribute 25 is not interpreted as CAR parameters.

Related commands: **display radius scheme** and **display connection**.

Examples

Specify to interpret RADIUS attribute 25 as CAR parameters.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute 25 car
```

data-flow-format (RADIUS scheme view)

Syntax

data-flow-format { data { byte | giga-byte | kilo-byte | mega-byte } | packet { giga-packet | kilo-packet | mega-packet | one-packet } } *
undo data-flow-format { data | packet }

View

RADIUS scheme view

Default level

2: System level

Parameters

data { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** }: Specifies the unit for data flows, which can be byte, kilobyte, megabyte, or gigabyte.

packet { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** }: Specifies the unit for data packets, which can be one-packet, kilo-packet, mega-packet, or giga-packet.

Description

Use **data-flow-format** to set the traffic statistics unit for data flows or packets.

Use **undo data-flow-format** to restore the default.

By default, the unit for data flows is **byte** and that for data packets is **one-packet**.

The unit for data flows and that for packets must be consistent with those on the RADIUS server. Otherwise, accounting cannot be performed correctly.

Related commands: **display radius scheme**.

Examples

Set the traffic statistics unit for data flows and that for packets to kilobytes and kilo-packets respectively in RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] data-flow-format data kilo-byte packet kilo-packet
```

display radius scheme

Syntax

display radius scheme [*radius-scheme-name*] [**slot** *slot-number*] [[{ **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

radius-scheme-name: RADIUS scheme name.

slot *slot-number*: Specifies the RADIUS schemes on an IRF member device. The *slot-number* argument represents the ID of an IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

[: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display radius scheme** to display the configuration of RADIUS schemes.

If you do not specify any RADIUS scheme, the command displays the configuration of all RADIUS schemes.

Related commands: **radius scheme**.

Examples

Display the configuration of all RADIUS schemes.

```
<Sysname> display radius scheme
```

```
-----
SchemeName   : radius1
Index : 0                                Type : extended
Primary Auth Server:
  IP: 1.1.1.1                               Port: 1812   State: active
  Encryption Key : *****
  Probe username : test
  Probe interval : 60 min
Primary Acct Server:
  IP: 1.1.1.1                               Port: 1813   State: active
  Encryption Key : *****
Second Auth Server:
  IP: 1.1.2.1                               Port: 1812   State: active
  Encryption Key : N/A
  Probe username : test
  Probe interval : 60 min
  IP: 1.1.3.1                               Port: 1812   State: active
  Encryption Key : N/A
  Probe username : test
  Probe interval : 60 min
Second Acct Server:
  IP: 1.1.2.1                               Port: 1813   State: block
  Encryption Key : N/A
Auth Server Encryption Key : *****
Acct Server Encryption Key : N/A
Accounting-On packet disable, send times : 50 , interval : 3s
Interval for timeout(second)                : 3
Retransmission times for timeout              : 3
Interval for realtime accounting(minute)      : 12
Retransmission times of realtime-accounting packet : 5
Retransmission times of stop-accounting packet : 500
Quiet-interval(min)                          : 5
Username format                             : without-domain
Data flow unit                              : Byte
Packet unit                                  : one
NAS-IP address                              : 1.1.1.1
Attribute 25                                : car
-----
```

Total 1 RADIUS scheme(s).

Table 5 Command output

Field	Description
SchemeName	Name of the RADIUS scheme.
Index	Index number of the RADIUS scheme.
Type	Type of the RADIUS server: extended or standard.
Primary Auth Server	Information about the primary authentication server.
Primary Acct Server	Information about the primary accounting server.
Second Auth Server	Information about the secondary authentication server.
Second Acct Server	Information about the secondary accounting server.
IP	IP address of the server.
Port	Service port of the server. If no port configuration is performed, the default port number is displayed.
State	Status of the server: active or blocked.
Encryption Key	Shared key for secure authentication or accounting communication, displayed as a series of asterisks (*****). If no shared key is configured, this field displays N/A . This shared key is used only when no specific shared key is specified for the RADIUS server.
Probe username	Username used for server status detection.
Probe interval	Server status detection interval, in minutes.
Auth Server Encryption Key	Shared key for secure authentication communication, displayed as a series of asterisks (*****). If no shared key is configured, this field displays N/A .
Acct Server Encryption Key	Shared key for secure accounting communication, displayed as a series of asterisks (*****). If no shared key is configured, this field displays N/A .
Accounting-On packet disable	The accounting-on feature is disabled.
send times	Retransmission times of accounting-on packets.
interval	Interval at which the switch retransmits accounting-on packets.
Interval for timeout(second)	RADIUS server response timeout period, in seconds.
Retransmission times for timeout	Maximum number of attempts for transmitting a RADIUS packet to a single RADIUS server.
Interval for realtime accounting(minute)	Interval for real-time accounting, in minutes.
Retransmission times of realtime-accounting packet	Maximum number of accounting attempts.
Retransmission times of stop-accounting packet	Maximum number of stop-accounting attempts.
Quiet-interval(min)	Quiet interval for the primary server.
Username format	Format of the usernames to be sent to the RADIUS server.
Data flow unit	Unit for data flows sent to the RADIUS server.
Packet unit	Unit for packets sent to the RADIUS server.

Field	Description
NAS-IP address	Source IP address for RADIUS packets to be sent.
Attribute 25	Interprets RADIUS attribute 25 as the CAR parameters.

display radius statistics

Syntax

display radius statistics [**slot** *slot-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

slot *slot-number*: Specifies the RADIUS packet statistics for an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display radius statistics** to display RADIUS packet statistics.

Related commands: **radius scheme**.

Examples

```
# Display statistics about RADIUS packets.
<Sysname> display radius statistics
Slot 1:state statistic(total=4096):
    DEAD = 4096      AuthProc = 0      AuthSucc = 0
AcctStart = 0        RLTSend = 0        RLWait = 0
    AcctStop = 0      OnLine = 0         Stop = 0
Received and Sent packets statistic:
Sent PKT total   = 1547      Received PKT total = 23
Resend Times      Resend total
1                 508
2                 508
Total             1016
RADIUS received packets statistic:
Code = 2   Num = 15      Err = 0
Code = 3   Num = 4       Err = 0
```



```

Code = 5    Num = 4      Err = 0
Code = 11   Num = 0      Err = 0
Running statistic:
RADIUS received messages statistic:
Normal auth request      Num = 24      Err = 0      Succ = 24
EAP auth request         Num = 0      Err = 0      Succ = 0
Account request          Num = 4      Err = 0      Succ = 4
Account off request      Num = 503    Err = 0      Succ = 503
PKT auth timeout         Num = 15     Err = 5      Succ = 10
PKT acct_timeout         Num = 1509   Err = 503    Succ = 1006
Realtime Account timer   Num = 0      Err = 0      Succ = 0
PKT response             Num = 23     Err = 0      Succ = 23
Accounting on response   Num = 0      Err = 0      Succ = 0
Session ctrl pkt         Num = 0      Err = 0      Succ = 0
Normal author request    Num = 0      Err = 0      Succ = 0
Set policy result        Num = 0      Err = 0      Succ = 0
RADIUS sent messages statistic:
Auth accept              Num = 10
Auth reject              Num = 14
EAP auth replying        Num = 0
Account success          Num = 4
Account failure          Num = 3
Server ctrl req          Num = 0
RecError_MSG_sum = 0
SndMSG_Fail_sum = 0
Timer_Err = 0
Alloc_Mem_Err = 0
State Mismatch = 0
Other_Error = 0
No-response-acct-stop packet = 1
Discarded No-response-acct-stop packet for buffer overflow = 0

```

Table 6 Command output

Field	Description
state statistic	User statistics, by state
DEAD	Number of idle users
AuthProc	Number of users waiting for authentication
AuthSucc	Number of users who have passed authentication
AcctStart	Number of users for whom accounting has been started
RLTSend	Number of users for whom the system sends real-time accounting packets
RLTWait	Number of users waiting for real-time accounting
AcctStop	Number of users in the state of accounting waiting stopped
OnLine	Number of online users
Stop	Number of users in the state of stop

Field	Description
Received and Sent packets statistic	Statistics for packets received and sent by the RADIUS module
Sent PKT total	Number of packets sent
Received PKT total	Number of packets received
Resend Times	Number of transmission attempts
Resend total	Number of packets retransmitted
Total	Total number of packets retransmitted
RADIUS received packets statistic	Statistics for packets received by the RADIUS module
Code	Packet type
Num	Total number of packets
Err	Number of packets that the switch failed to process
Succ	Number of messages that the switch successfully processed
Running statistic	Statistics for RADIUS messages received and sent by the RADIUS module
RADIUS received messages statistic	Statistics for received RADIUS messages
Normal auth request	Number of normal authentication requests
EAP auth request	Number of EAP authentication requests
Account request	Number of accounting requests
Account off request	Number of stop-accounting requests
PKT auth timeout	Number of authentication timeout messages
PKT acct_timeout	Number of accounting timeout messages
Realtime Account timer	Number of real-time accounting requests
PKT response	Number of responses from servers
Accounting on response	Number of accounting-on responses
Session ctrl pkt	Number of session control messages
Normal author request	Number of normal authorization requests
Set policy result	Number of responses to the Set policy packets
RADIUS sent messages statistic	Statistics for sent RADIUS messages
Auth accept	Number of accepted authentication packets
Auth reject	Number of rejected authentication packets
EAP auth replying	Number of replying packets of EAP authentication
Account success	Number of accounting succeeded packets
Account failure	Number of accounting failed packets
Server ctrl req	Number of server control requests
RecError_MSG_sum	Number of received packets in error
SndMSG_Fail_sum	Number of packets that failed to be sent out
Timer_Err	Number of packets for indicating timer startup failures

Field	Description
Alloc_Mem_Err	Number of packets for indication memory allocation failures
State Mismatch	Number of packets for indicating mismatching status
Other_Error	Number of packets for indicating other types of errors
No-response-acct-stop packet	Number of times that no response was received for stop-accounting packets
Discarded No-response-acct-stop packet for buffer overflow	Number of stop-accounting packets that were buffered but then discarded due to full memory

display stop-accounting-buffer (for RADIUS)

Syntax

```
display stop-accounting-buffer { radius-scheme radius-scheme-name | session-id session-id | time-range start-time stop-time | user-name user-name } [ slot slot-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

2: System level

Parameters

radius-scheme *radius-scheme-name*: Specifies buffered stop-accounting requests that are destined for the accounting server defined in a RADIUS scheme. The RADIUS scheme name is a case-insensitive string of 1 to 32 characters.

session-id *session-id*: Specifies the stop-accounting requests buffered for a session. The session ID is a string of 1 to 50 characters.

time-range *start-time stop-time*: Specifies the stop-accounting requests buffered in a time range. The start time and end time must be in the format HH:MM:SS-MM/DD/YYYY or HH:MM:SS-YYYY/MM/DD.

user-name *user-name*: Specifies the stop-accounting requests buffered for a user. The username is a case-sensitive string of 1 to 80 characters. Whether the *user-name* argument should include the domain name depends on the setting configured by the **user-name-format** command for the RADIUS scheme.

slot *slot-number*: Specifies the stop-accounting requests buffered for an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display stop-accounting-buffer** to display information about the stop-accounting requests buffered in the switch.

If the switch sends a stop-accounting request to a RADIUS server but receives no response, it retransmits it up to a certain number of times (defined by the **retry** command). If the switch still receives no response, it considers the stop-accounting attempt a failure, buffers the request, and makes another stop-accounting attempt. The maximum number of the stop-accounting attempts is defined by the **retry stop-accounting** command. If all attempts fail, the switch discards the request.

Related commands: **reset stop-accounting-buffer**, **stop-accounting-buffer enable**, **user-name-format**, **retry**, and **retry stop-accounting**.

Examples

Display information about the stop-accounting requests buffered for user **abc**.

```
<Sysname> display stop-accounting-buffer user-name abc
```

```
Slot 1:
```

RDIdx	Session-ID	user name	Happened time
1	1000326232325010	abc	23:27:16-03/31/2011
1	1000326232326010	abc	23:33:01-03/31/2011

```
Total 2 record(s) Matched
```

key (RADIUS scheme view)

Syntax

key { **accounting** | **authentication** } [**cipher** | **simple**] *key*

undo key { **accounting** | **authentication** }

View

RADIUS scheme view

Default level

2: System level

Parameters

accounting: Sets the shared key for secure RADIUS accounting communication.

authentication: Sets the shared key for secure RADIUS authentication/authorization communication.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

key: Specifies the shared key string. This argument is case sensitive. In non-FIPS mode, a ciphertext shared key must be a string of 1 to 117 characters and a plaintext shared key must be a string of 1 to 64 characters. In FIPS mode, a ciphertext shared key must be a string of 8 to 117 characters, and a plaintext shared key must be a string of 8 to 64 characters that must include numbers, uppercase letters, lowercase letters, and special characters. If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

Description

Use **key** to set the shared key for secure RADIUS authentication/authorization or accounting communication.

Use **undo key** to restore the default.

By default, no shared key is configured.

For secrecy, all shared keys, including shared keys configured in plain text, are saved in cipher text.

The shared keys specified during the configuration of the RADIUS servers, if any, take precedence.

The shared keys configured on the switch must match those configured on the RADIUS servers.

Related commands: **display radius scheme**.

Examples

For RADIUS scheme **radius1**, set the shared key for secure accounting communication to **ok** in plain text.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key accounting simple ok
```

For RADIUS scheme **radius1**, set the shared key for secure accounting communication to **ok** in plain text.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key accounting ok
```

nas-ip (RADIUS scheme view)

Syntax

nas-ip { *ipv4-address* | **ipv6** *ipv6-address* }

undo nas-ip

View

RADIUS scheme view

Default level

2: System level

Parameters

ipv4-address: IPv4 address in dotted decimal notation. It must be an address of the switch and cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

ipv6 *ipv6-address*: Specifies an IPv6 address. It must be an address of the switch and must be a unicast address that is neither a loopback address nor a link-local address.

Description

Use **nas-ip** to specify a source IP address for outgoing RADIUS packets.

Use **undo nas-ip** to restore the default.

By default, the source IP address of an outgoing RADIUS packet is that configured by the **radius nas-ip** command in system view. If the **radius nas-ip** command is not configured, the source IP address is the IP address of the outbound interface.

The source IP address of RADIUS packets that a NAS sends must match the IP address of the NAS that is configured on the RADIUS server. A RADIUS server identifies a NAS by its IP address. Upon receiving

a RADIUS packet, a RADIUS server checks whether the source IP address of the packet is the IP address of any managed NAS. If yes, the server processes the packet. If not, the server drops the packet.

The source IP address specified for outgoing RADIUS packets must be of the same IP version as the IP addresses of the RADIUS servers in the RADIUS scheme. Otherwise, the source IP address configuration does not take effect.

A RADIUS scheme can have only one source IP address for outgoing RADIUS packets. If you specify a new source IP address for the same RADIUS scheme, the new one overwrites the old one.

The setting configured by the **nas-ip** command in RADIUS scheme view is only for the RADIUS scheme, whereas that configured by the **radius nas-ip** command in system view is for all RADIUS schemes. The setting in RADIUS scheme view takes precedence.

Related commands: **radius nas-ip**.

Examples

```
# Set the source IP address for outgoing RADIUS packets to 10.1.1.1.
```

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] nas-ip 10.1.1.1
```

primary accounting (RADIUS scheme view)

Syntax

```
primary accounting { ipv4-address | ipv6 ipv6-address } [ port-number | key [ cipher | simple ] key ] *
undo primary accounting
```

View

RADIUS scheme view

Default level

2: System level

Parameters

ipv4-address: Specifies the IPv4 address of the primary accounting server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary accounting server.

port-number: Specifies the service port number of the primary RADIUS accounting server, which is a UDP port number in the range of 1 to 65535 and defaults to 1813.

key [**cipher** | **simple**] *key*: Sets the shared key for secure communication with the primary RADIUS accounting server.

- **cipher** *key*: Sets a ciphertext shared key, which is a case-sensitive ciphertext string of 1 to 117 characters in non-FIPS mode and 8 to 117 characters in FIPS mode.
- **simple** *key*: Sets a plaintext shared key, which is a case-sensitive string of 1 to 64 characters in non-FIPS mode and 8 to 64 characters that must include numbers, uppercase letters, lowercase letters, and special characters in FIPS mode.
- If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

Description

Use **primary accounting** to specify the primary RADIUS accounting server.

Use **undo primary accounting** to remove the configuration.

By default, no primary RADIUS accounting server is specified.

Make sure the port number and shared key settings of the primary RADIUS accounting server are the same as those configured on the server.

The IP addresses of the accounting servers and those of the authentication/authorization servers must be of the same IP version.

The IP addresses of the primary and secondary accounting servers must be different from each other and use the same IP version. Otherwise, the configuration fails.

The shared key configured by this command takes precedence over that configured by using the **key accounting** [**cipher** | **simple**] key command.

If you change the primary accounting server when the switch has already sent a start-accounting request to the server, the communication with the primary server times out, and the switch looks for a server in active state from the new primary server on.

If you remove an accounting server being used by users, the switch no longer sends real-time accounting or stop-accounting requests for the users, and does not buffer the stop-accounting requests.

For secrecy, all shared keys, including shared keys configured in plain text, are saved in cipher text.

Related commands: **key**.

Examples

For RADIUS scheme **radius1**, set the IP address of the primary accounting server to 10.110.1.2, the UDP port to 1813, and the shared key to **hello** in plain text.

```
<Sysname> system-view
```

```
[Sysname] radius scheme radius1
```

```
[Sysname-radius-radius1] primary accounting 10.110.1.2 1813 key simple hello
```

primary authentication (RADIUS scheme view)

Syntax

primary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key* | **probe username** *name* [**interval** *interval*]] *

undo primary authentication

View

RADIUS scheme view

Default level

2: System level

Parameters

ipv4-address: Specifies the IPv4 address of the primary authentication/authorization server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the primary authentication/authorization server.

port-number: Specifies the service port number of the primary RADIUS authentication/authorization server, which is a UDP port number in the range of 1 to 65535 and defaults to 1812.

key [**cipher** | **simple**] *key*: Sets the shared key for secure communication with the primary RADIUS authentication/authorization server.

- **cipher** *key*: Sets a ciphertext shared key, which is a case-sensitive ciphertext string of 1 to 117 characters in non-FIPS mode and 8 to 117 characters in FIPS mode.

- **simple** *key*: Sets a plaintext shared key, which is a case-sensitive string of 1 to 64 characters in non-FIPS mode and 8 to 64 characters that must include numbers, uppercase letters, lowercase letters, and special characters in FIPS mode.
- If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

probe username: Enables the switch to detect the status of the primary RADIUS authentication/authorization server.

username *name*: Specifies the username in the authentication request that is used to detect the status of the primary RADIUS authentication/authorization server.

interval *interval*: Specifies the interval between two server status detections. The value ranges from 1 to 3600 and defaults to 60, in minutes.

Description

Use **primary authentication** to specify the primary RADIUS authentication/authorization server.

Use **undo primary authentication** to remove the configuration.

By default, no primary RADIUS authentication/authorization server is specified.

Make sure the port number and shared key settings of the primary RADIUS accounting server are the same as those configured on the server.

The IP addresses of the authentication/authorization servers and those of the accounting servers must be of the same IP version.

The IP addresses of the primary and secondary authentication/authorization servers must be different from each other and use the same IP version. Otherwise, the configuration fails.

The shared key configured by this command takes precedence over that configured by using the **key authentication** [**cipher** | **simple**] *key* command.

If you remove the primary authentication server when an authentication process is in progress, the communication with the primary server times out, and the switch looks for a server in active state from the new primary server on.

With the server status detection feature enabled, the switch sends an authentication request that carries the specified username to the primary server at the specified interval. If the switch receives no response from the server within the time interval specified by the **timer response-timeout** command, the switch sends the authentication request again.

If the maximum number of retries (specified by the **retry** command) is reached and the switch still receives no response from the server, the switch considers the server as unreachable. If the switch receives a response from the server before the maximum number of retries is reached, the switch considers the server as reachable. The switch sets the status of the server to **block** or **active** according to the status detection result, regardless of the current status of the server.

For 802.1X authentication, if the status of every server is **block**, the switch assigns the port connected to an authentication user to the specified 802.1X critical VLAN. For more information about the 802.1X critical VLAN, see *Security Configuration Guide*.

To ensure that the switch can set the server to its actual status, set a longer quiet timer for the primary server with the **timer quiet** command. If you set a short quiet timer and configure 802.1X critical VLAN on a port, the switch might frequently change the server status, and the port might frequently join and leave the critical VLAN.

Related commands: **key**.

Examples

For RADIUS scheme **radius1**, set the IP address of the primary authentication/authorization server to 10.110.1.1, the UDP port to 1812, and the shared key to **hello** in plain text.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary authentication 10.110.1.1 1812 key hello
```

In RADIUS scheme **radius1**, set the username used for status detection of the primary authentication/authorization server to **test** in plain text, and set the server status detection interval to 120 minutes.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary authentication 10.110.1.1 probe username test interval 120
```

radius client

Syntax

radius client enable

undo radius client

View

System view

Default level

2: System level

Parameters

None

Description

Use **radius client enable** to enable the RADIUS client service.

Use **undo radius client** to disable the RADIUS client service.

By default, the RADIUS listening port is enabled.

When the listening port of the RADIUS client is disabled, the following events occur:

- No more stop-accounting requests of online users can be sent out or buffered, and the RADIUS server can no longer receive logoff requests from online users. After a user goes offline, the RADIUS server still has the user's record during a certain period of time.
- The buffered accounting packets cannot be sent out and are deleted from the buffer when the configured maximum number of attempts is reached, affecting the precision of user accounting.
- If local authentication, authorization, or accounting is configured as the backup, the switch performs local authentication, authorization, or accounting instead after the RADIUS request fails. Local accounting is only for monitoring and controlling the number of local user connections. It does not provide the statistics function that the accounting feature generally provides.

Examples

Enable the RADIUS client service.

```
<Sysname> system-view
[Sysname] radius client enable
```

radius dscp

Syntax

radius dscp *dscp-value*

undo radius dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use **radius dscp** to set the DSCP value for IPv4 RADIUS protocol packets.

Use **undo radius dscp** to restore the default.

By default, the DSCP value in IPv4 RADIUS protocol packets is 0.

Examples

Set the DSCP value to 6 for IPv4 RADIUS protocol packets.

```
<Sysname> system-view
```

```
[Sysname] radius dscp 6
```

radius ipv6 dscp

Syntax

radius ipv6 dscp *dscp-value*

undo radius ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: DSCP value in the protocol packets, which ranges from 0 to 63.

Description

Use **radius ipv6 dscp** to set the DSCP value for IPv6 RADIUS protocol packets.

Use **undo radius ipv6 dscp** to restore the default.

By default, the DSCP value in IPv6 RADIUS protocol packets is 0.

Examples

Set the DSCP value to 6 for IPv6 RADIUS protocol packets.

```
<Sysname> system-view
```

```
[Sysname] radius ipv6 dscp 6
```

radius nas-ip

Syntax

```
radius nas-ip { ipv4-address | ipv6 ipv6-address }  
undo radius nas-ip { ipv4-address | ipv6 ipv6-address }
```

View

System view

Default level

2: System level

Parameters

ipv4-address: IPv4 address in dotted decimal notation. It must be an address of the switch and cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

ipv6 ipv6-address: Specifies an IPv6 address. It must be a unicast address of the switch that is neither a loopback address nor a link-local address.

Description

Use **radius nas-ip** to specify a source address for outgoing RADIUS packets.

Use **undo radius nas-ip** to remove the configuration.

By default, the source IP address of an outgoing RADIUS packet is the IP address of the outbound interface.

You can specify up to 16 source IP addresses.

The source IP address of RADIUS packets that a NAS sends must match the IP address of the NAS that is configured on the RADIUS server. A RADIUS server identifies a NAS by its IP address. Upon receiving a RADIUS packet, a RADIUS server checks whether the source IP address of the packet is the IP address of any managed NAS. If yes, the server processes the packet. If not, the server drops the packet.

The setting configured by the **nas-ip** command in RADIUS scheme view is only for the RADIUS scheme, whereas that configured by the **radius nas-ip** command in system view is for all RADIUS schemes. The setting in RADIUS scheme view takes precedence.

Related commands: **nas-ip**.

Examples

Set the IP address for the switch to use as the source address of the RADIUS packets to 129.10.10.1.

```
<Sysname> system-view  
[Sysname] radius nas-ip 129.10.10.1
```

radius scheme

Syntax

```
radius scheme radius-scheme-name  
undo radius scheme radius-scheme-name
```

View

System view

Default level

3: Manage level

Parameters

radius-scheme-name: RADIUS scheme name, a case-insensitive string of 1 to 32 characters.

Description

Use **radius scheme** to create a RADIUS scheme and enter RADIUS scheme view.

Use **undo radius scheme** to delete a RADIUS scheme.

By default, no RADIUS scheme is defined.

A RADIUS scheme can be referenced by more than one ISP domain at the same time.

A RADIUS scheme referenced by ISP domains cannot be removed.

Related commands: **display radius scheme**.

Examples

Create a RADIUS scheme named **radius1** and enter RADIUS scheme view.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1]
```

radius trap

Syntax

```
radius trap { accounting-server-down | authentication-error-threshold | authentication-server-down }
undo radius trap { accounting-server-down | authentication-error-threshold | authentication-server-down }
```

View

System view

Default level

2: System level

Parameters

accounting-server-down: Sends traps when the reachability of the accounting server changes.

authentication-error-threshold: Sends traps when the number of authentication failures exceed the specified threshold. The threshold is represented by the ratio of the number of failed request transmission attempts to the total number of transmission attempts. It ranges from 1 to 100 and defaults to 30. This threshold can only be configured through the MIB.

authentication-server-down: Sends traps when the reachability of the authentication server changes.

Description

Use **radius trap** to enable the trap function for RADIUS.

Use **undo radius trap** to disable the trap function for RADIUS.

By default, the trap function is disabled for RADIUS.

With the trap function for RADIUS, a NAS sends a trap message in the following cases:

- The status of a RADIUS server changes. If a NAS sends a request but receives no response before the maximum number of attempts is exceeded, it places the server to blocked state and sends a trap message. If a NAS receives a response from a RADIUS server it considered unreachable, it considers that the RADIUS server is reachable again and also sends a trap message.
- The ratio of the number of failed transmission attempts to the total number of authentication request transmission attempts reaches the threshold.

Examples

```
# Enable the switch to send traps in response to accounting server reachability changes.
<Sysname> system-view
[Sysname] radius trap accounting-server-down
```

reset radius statistics

Syntax

reset radius statistics [**slot** *slot-number*]

View

User view

Default level

2: System level

Parameters

slot *slot-number*: Clears the RADIUS statistics for an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

Description

Use **reset radius statistics** to clear RADIUS statistics.

Related commands: **display radius statistics**.

Examples

```
# Clear RADIUS statistics.
<Sysname> reset radius statistics
```

reset stop-accounting-buffer (for RADIUS)

Syntax

reset stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* } [**slot** *slot-number*]

View

User view

Default level

2: System level

Parameters

radius-scheme *radius-scheme-name*: Clears buffered stop-accounting requests that are destined for the accounting server defined in a RADIUS scheme. The RADIUS scheme name is a case-insensitive string of 1 to 32 characters.

session-id *session-id*: Clears the stop-accounting requests buffered for a session. The session ID is a string of 1 to 50 characters.

time-range *start-time stop-time*: Clears the stop-accounting requests buffered in a time range. The start time and end time must be in the format HH:MM:SS-MM/DD/YYYY or HH:MM:SS-YYYY/MM/DD.

user-name *user-name*: Clears the stop-accounting requests buffered for a user. The username is a case-sensitive string of 1 to 80 characters. Whether the *user-name* argument should include the domain name depends on the setting configured by the **user-name-format** command for the RADIUS scheme.

slot *slot-number*: Clears the stop-accounting requests buffered for an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

Description

Use **reset stop-accounting-buffer** to clear the buffered stop-accounting requests for which no responses have been received.

Related commands: **stop-accounting-buffer enable** and **display stop-accounting-buffer**.

Examples

Clear the stop-accounting requests buffered for user **user0001@test**.

```
<Sysname> reset stop-accounting-buffer user-name user0001@test
```

Clear the stop-accounting requests buffered in the time range from 0:0:0 to 23:59:59 on March 31, 2011.

```
<Sysname> reset stop-accounting-buffer time-range 0:0:0-03/31/2011 23:59:59-03/31/2011
```

retry

Syntax

retry *retry-times*

undo retry

View

RADIUS scheme view

Default level

2: System level

Parameters

retry-times: Maximum number of RADIUS packet transmission attempts, in the range of 1 to 20.

Description

Use **retry** to set the maximum number of attempts for transmitting a RADIUS packet to a single RADIUS server.

Use **undo retry** to restore the default.

By default, the maximum number of RADIUS packet transmission attempts is 3.

Because RADIUS uses UDP packets to transmit data, the communication is not reliable. If the switch does not receive a response to its request from the RADIUS server within the response timeout period, it retransmits the RADIUS request. If the number of transmission attempts exceeds the limit but the switch still receives no response from the RADIUS server, the switch considers the request a failure.

The maximum number of packet transmission attempts multiplied by the RADIUS server response timeout period cannot be greater than 75.

Related commands: **radius scheme** and **timer response-timeout**.

Examples

```
# Set the maximum number of RADIUS request transmission attempts to 5 for RADIUS scheme radius1.
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry 5
```

retry realtime-accounting

Syntax

```
retry realtime-accounting retry-times
undo retry realtime-accounting
```

View

RADIUS scheme view

Default level

2: System level

Parameters

retry-times: Maximum number of accounting attempts, in the range of 1 to 255.

Description

Use **retry realtime-accounting** to set the maximum number of accounting attempts.

Use **undo retry realtime-accounting** to restore the default.

By default, the maximum number of accounting attempts is 5.

A RADIUS server usually checks whether a user is online by using a timeout timer. If it receives no real-time accounting request for a user in the timeout period from the NAS, it considers that there may be link or switch failures and stops accounting for the user. This may happen when some unexpected failure occurs. To cooperate with this feature of the RADIUS server, the NAS must keep pace with the server in disconnecting the user. The maximum number of accounting attempts, together with some other parameters, enables the NAS to promptly disconnect the user.

The maximum number of accounting attempts, together with some other parameters, controls how the NAS sends accounting request packets.

Suppose that the RADIUS server response timeout period is three seconds (set with the **timer response-timeout** command), the maximum number of RADIUS packet transmission attempts is three (set with the **retry** command), the real-time accounting interval is 12 minutes (set with the **timer realtime-accounting** command), and the maximum number of accounting attempts is five (set with the **retry realtime-accounting** command). In this case, the switch generates an accounting request every 12 minutes, and retransmits the request if it sends the request but receives no response within three seconds. If the switch receives no response after transmitting the request three times, it considers the accounting

attempt a failure, and makes another accounting attempt. If five consecutive accounting attempts fail, the switch cuts the user connection.

Related commands: **retry**, **timer response-timeout**, and **timer realtime-accounting**.

Examples

Set the maximum number of accounting attempts to 10 for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry realtime-accounting 10
```

retry stop-accounting (RADIUS scheme view)

Syntax

retry stop-accounting *retry-times*

undo retry stop-accounting

View

RADIUS scheme view

Default level

2: System level

Parameters

retry-times: Maximum number of stop-accounting attempts, in the range of 10 to 65535.

Description

Use **retry stop-accounting** to set the maximum number of stop-accounting attempts.

Use **undo retry stop-accounting** to restore the default.

By default, the maximum number of stop-accounting attempts is 500.

The maximum number of stop-accounting attempts, together with some other parameters, controls how the NAS deals with stop-accounting request packets.

Suppose that the RADIUS server response timeout period is three seconds (set with the **timer response-timeout** command), the maximum number of transmission attempts is five (set with the **retry** command), and the maximum number of stop-accounting attempts is 20 (set with the **retry stop-accounting** command). For each stop-accounting request, if the switch receives no response within three seconds, it retransmits the request. If it receives no responses after retransmitting the request five times, it considers the stop-accounting attempt a failure, buffers the request, and makes another stop-accounting attempt. If 20 consecutive attempts fail, the switch discards the request.

Related commands: **retry**, **retry stop-accounting**, **timer response-timeout**, and **display stop-accounting-buffer**.

Examples

Set the maximum number of stop-accounting attempts to 1000 for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry stop-accounting 1000
```


secondary accounting (RADIUS scheme view)

Syntax

secondary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key*]
*

undo secondary accounting [*ipv4-address* | **ipv6** *ipv6-address*]

View

RADIUS scheme view

Default level

2: System level

Parameters

ipv4-address: Specifies the IPv4 address of the secondary accounting server, in dotted decimal notation.

ipv6 *ipv6-address*: Specifies the IPv6 address of the secondary accounting server.

port-number: Specifies the service port number of the secondary RADIUS accounting server, which is a UDP port number in the range of 1 to 65535 and defaults to 1813.

key [**cipher** | **simple**] *key*: Sets the shared key for secure communication with the secondary RADIUS accounting server.

- **cipher** *key*: Sets a ciphertext shared key, which is a case-sensitive ciphertext string of 1 to 117 characters in non-FIPS mode and 8 to 117 characters in FIPS mode.
- **simple** *key*: Sets a plaintext shared key, which is a case-sensitive string of 1 to 64 characters in non-FIPS mode and 8 to 64 characters that must include numbers, uppercase letters, lowercase letters, and special characters in FIPS mode.
- If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

Description

Use **secondary accounting** to specify secondary RADIUS accounting servers for a RADIUS scheme.

Use **undo secondary accounting** to remove a secondary RADIUS accounting server.

By default, no secondary RADIUS accounting server is specified.

Make sure the port number and shared key settings of the secondary RADIUS accounting server are the same as those configured on the server.

You can configure up to 16 secondary RADIUS accounting servers for a RADIUS scheme. After the configuration, if the primary server fails, the switch looks for a secondary server in active state (a secondary RADIUS accounting server configured earlier has a higher priority) and tries to communicate with it.

The IP addresses of the accounting servers and those of the authentication/authorization servers must be of the same IP version.

The IP addresses of the primary and secondary accounting servers must be different from each other and use the same IP version. Otherwise, the configuration fails.

The shared key configured by this command takes precedence over that configured by using the **key accounting** [**cipher** | **simple**] *key* command.

If you remove a secondary accounting server when the switch has already sent a start-accounting request to the server, the communication with the secondary server times out, and the switch looks for a server in active state from the primary server on.

If you remove an accounting server being used by online users, the switch no longer sends real-time accounting or stop-accounting requests for the users, and does not buffer the stop-accounting requests.

For secrecy, all shared keys, including shared keys configured in plain text, are saved in cipher text.

Related commands: **key**.

Examples

For RADIUS scheme **radius2**, specify two secondary accounting servers with the server IP addresses of 10.110.1.1 and 10.110.1.2 and the UDP port number of 1813. Set the shared keys to **hello** in plain text.

```
<Sysname> system-view
[Sysname] radius scheme radius2
[Sysname-radius-radius2] secondary accounting 10.110.1.1 1813 key hello
[Sysname-radius-radius2] secondary accounting 10.110.1.2 1813 key hello
```

secondary authentication (RADIUS scheme view)

Syntax

secondary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key* | **probe username** *name* [**interval** *interval*]] *

undo secondary authentication [*ipv4-address* | **ipv6** *ipv6-address*]

View

RADIUS scheme view

Default level

2: System level

Parameters

ipv4-address: Specifies the IPv4 address of the secondary authentication/authorization server, in dotted decimal notation.

ipv6 *ipv6-address*: Specifies the IPv6 address of the secondary authentication/authorization server.

port-number: Specifies the service port number of the secondary RADIUS authentication/authorization server, which is a UDP port number in the range of 1 to 65535 and defaults to 1812.

key [**cipher** | **simple**] *key*: Sets the shared key for secure communication with the secondary RADIUS authentication/authorization server.

- **cipher** *key*: Sets a ciphertext shared key, which is a case-sensitive ciphertext string of 1 to 117 characters in non-FIPS mode and 8 to 117 characters in FIPS mode.
- **simple** *key*: Sets a plaintext shared key, which is a case-sensitive string of 1 to 64 characters in non-FIPS mode and 8 to 64 characters that must include numbers, uppercase letters, lowercase letters, and special characters in FIPS mode.
- If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

probe username: Enables the switch to detect the status of the secondary RADIUS authentication/authorization server.

username name: Specifies the username in the authentication request that is used to detect the status of the secondary RADIUS authentication/authorization server.

interval interval: Specifies the interval between two server status detections. The value ranges from 1 to 3600 and defaults to 60, in minutes.

Description

Use **secondary authentication** to specify secondary RADIUS authentication/authorization servers for a RADIUS scheme.

Use **undo secondary authentication** to remove a secondary RADIUS authentication/authorization server.

By default, no secondary RADIUS authentication/authorization server is specified.

Make sure the port number and shared key settings of the secondary RADIUS authentication/authorization server are the same as those configured on the server.

You can configure up to 16 secondary RADIUS authentication/authorization servers for a RADIUS scheme. After the configuration, if the primary server fails, the switch looks for a secondary server in active state (a secondary RADIUS authentication/authorization server configured earlier has a higher priority) and tries to communicate with it.

The IP addresses of the authentication/authorization servers and those of the accounting servers must be of the same IP version.

The IP addresses of the primary and secondary authentication/authorization servers must be different from each other and use the same IP version. Otherwise, the configuration fails.

The shared key configured by this command takes precedence over that configured by using the **key authentication [cipher | simple] key** command.

If you remove a secondary authentication server in use in the authentication process, the communication with the secondary server times out, and the switch looks for a server in active state from the primary server on.

For secrecy, all shared keys, including shared keys configured in plain text, are saved in cipher text.

With the server status detection feature enabled, the switch sends an authentication request that carries the specified username to the secondary server at the specified interval. If the switch receives no response from the server within the time interval specified by the **timer response-timeout** command, the switch sends the authentication request again.

If the maximum number of retries (specified by the **retry** command) is reached and the switch still receives no response from the server, the switch considers the server as unreachable. If the switch receives a response from the server before the maximum number of retries is reached, the switch considers the server as reachable. The switch sets the status of the server to **block** or **active** according to the status detection result, regardless of the current status of the server.

For 802.1X authentication, if the status of every server is **block**, the switch assigns the port connected to an authentication user to the specified 802.1X critical VLAN. For more information about the 802.1X critical VLAN, see *Security Configuration Guide*.

To ensure that the switch can set the server to its actual status, set a longer quiet timer for the secondary server with the **timer quiet** command. If you set a short quiet timer and configure 802.1X critical VLAN on a port, the switch might frequently change the server status, and the port might frequently join and leave the critical VLAN.

Related commands: **key**.

Examples

Specify two secondary authentication/authorization servers for RADIUS scheme **radius2**, with the server IP addresses of 10.110.1.1 and 10.110.1.2, and the UDP port number of 1813. Set the shared keys to **hello** in plain text.

```
<Sysname> system-view
[Sysname] radius scheme radius2
[Sysname-radius-radius2] secondary authentication 10.110.1.1 1812 key simple hello
[Sysname-radius-radius2] secondary authentication 10.110.1.2 1812 key simple hello
```

In RADIUS scheme **radius1**, set the username used for status detection of the secondary authentication/authorization server to **test** in plain text, and set the server status detection interval to 120 minutes.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary authentication 10.110.1.1 probe username test interval 120
```

security-policy-server

Syntax

```
security-policy-server ip-address
undo security-policy-server { ip-address | all }
```

View

RADIUS scheme view

Default level

2: System level

Parameters

ip-address: Specifies a security policy server by its IP address.

all: Specifies all security policy servers.

Description

Use **security-policy-server** to specify a security policy server for a RADIUS scheme.

Use **undo security-policy-server** to remove security policy servers for a RADIUS scheme.

By default, no security policy server is specified for a RADIUS scheme.

You can change security policy servers for a RADIUS scheme only when no user is using the scheme.

Examples

Specify security policy server 10.110.1.2 for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] security-policy-server 10.110.1.2
```

server-type

Syntax

```
server-type { extended | standard }
```

undo server-type

View

RADIUS scheme view

Default level

2: System level

Parameters

extended: Specifies the extended RADIUS server (generally running on IMC), which requires the RADIUS client and RADIUS server to interact according to the procedures and packet formats provisioned by the proprietary RADIUS protocol.

standard: Specifies the standard RADIUS server, which requires the RADIUS client and RADIUS server to interact according to the procedures and packet format of the standard RADIUS protocol (RFC 2865 and 2866 or their successors).

Description

Use **server-type** to configure the RADIUS server type.

Use **undo server-type** to restore the default.

By default, the supported RADIUS server type is **standard**.

Examples

Configure the RADIUS server type of RADIUS scheme **radius1** as **standard**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] server-type standard
```

state primary

Syntax

state primary { accounting | authentication } { active | block }

View

RADIUS scheme view

Default level

2: System level

Parameters

accounting: Sets the status of the primary RADIUS accounting server.

authentication: Sets the status of the primary RADIUS authentication/authorization server.

active: Specifies the active state, the normal operation state.

block: Specifies the blocked state, the out-of-service state.

Description

Use **state primary** to set the status of a primary RADIUS server.

By default, the primary RADIUS server specified for a RADIUS scheme is in active state.

During an authentication or accounting process, the switch first tries to communicate with the primary server if the primary server is in active state. If the primary server is unavailable, the switch changes the

status of the primary server to blocked, starts a quiet timer for the server, and then tries to communicate with a secondary server in active state (a secondary RADIUS server configured earlier has a higher priority). When the quiet timer of the primary server times out, the status of the server changes to active automatically. If you set the status of the server to blocked before the quiet timer times out, the status of the server cannot change back to active automatically unless you set the status to active manually.

When the primary server and secondary servers are both in blocked state, the switch communicates with the primary server.

Related commands: **display radius scheme** and **state secondary**.

Examples

Set the status of the primary server in RADIUS scheme **radius1** to blocked.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state primary authentication block
```

state secondary

Syntax

state secondary { **accounting** | **authentication** } [**ip** *ipv4-address* | **ipv6** *ipv6-address*] { **active** | **block** }

View

RADIUS scheme view

Default level

2: System level

Parameters

accounting: Sets the status of the secondary RADIUS accounting server.

authentication: Sets the status of the secondary RADIUS authentication/authorization server.

ip *ipv4-address*: Specifies the IPv4 address of the secondary RADIUS server.

ipv6 *ipv6-address*: Specifies the IPv6 address of the secondary RADIUS server.

active: Specifies the active state, the normal operation state.

block: Specifies the blocked state, the out-of-service state.

Description

Use **state secondary** to set the status of a secondary RADIUS server.

By default, every secondary RADIUS server specified in a RADIUS scheme is in active state.

If no IP address is specified, this command changes the status of all configured secondary servers for authentication/authorization or accounting.

If the switch finds that a secondary server in active state is unreachable, the switch changes the status of the secondary server to blocked, starts a quiet timer for the server, and continues to try to communicate with the next secondary server in active state (a secondary RADIUS server configured earlier has a higher priority). When the quiet timer of a server times out, the status of the server changes to active automatically. If you set the status of the server to blocked before the quiet timer times out, the status of the server cannot change back to active automatically unless you set the status to active manually. If all configured secondary servers are unreachable, the switch considers the authentication or accounting attempt a failure.

Related commands: **display radius scheme** and **state primary**.

Examples

```
# Set the status of all the secondary servers in RADIUS scheme radius1 to blocked.
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state secondary authentication block
```

stop-accounting-buffer enable (RADIUS scheme view)

Syntax

```
stop-accounting-buffer enable
undo stop-accounting-buffer enable
```

View

RADIUS scheme view

Default level

2: System level

Parameters

None

Description

Use **stop-accounting-buffer enable** to enable the switch to buffer stop-accounting requests to which no responses are received.

Use **undo stop-accounting-buffer enable** to disable the buffering function.

By default, the switch buffers stop-accounting requests to which no responses are received.

Stop-accounting requests affect the charge to users. A NAS must make its best effort to send every stop-accounting request to the RADIUS accounting servers. For each stop-accounting request getting no response in the specified period of time, the NAS buffers and resends the packet until it receives a response or the number of transmission attempts reaches the configured limit. In the latter case, the NAS discards the packet. However, if you have removed the accounting server, stop-accounting messages are not buffered.

Related commands: **reset stop-accounting-buffer** and **display stop-accounting-buffer**.

Examples

```
# Enable the switch to buffer the stop-accounting requests to which no responses are received.
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] stop-accounting-buffer enable
```

timer quiet (RADIUS scheme view)

Syntax

```
timer quiet minutes
undo timer quiet
```

View

RADIUS scheme view

Default level

2: System level

Parameters

minutes: Server quiet period in minutes, in the range of 0 to 255. If you set this argument to 0, when the switch attempts to send an authentication or accounting request but the current server is unreachable, the switch sends the request to the next server in active state, without changing the current server's status. As a result, when the switch attempts to send a request of the same type for another user, it still tries to send the request to the current server because the current server is in active state.

Description

Use **timer quiet** to set the quiet timer for the servers. This timer controls whether the switch changes the status of an unreachable server from active to blocked, and how long the switch keeps an unreachable server in blocked state.

Use **undo timer quiet** to restore the default.

By default, the server quiet period is 5 minutes.

If you determine that the primary server is unreachable because the switch's port connected to the server is out of service temporarily or the server is busy, you can set the server quiet period to 0 so that the switch uses the primary server whenever possible.

Be sure to set the server quiet timer properly. Too short a quiet timer may result in frequent authentication or accounting failures because the switch keeps trying to communicate with an unreachable server that is in active state.

Related commands: **display radius scheme**.

Examples

Set the quiet timer for the servers to 10 minutes.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer quiet 10
```

timer realtime-accounting (RADIUS scheme view)

Syntax

timer realtime-accounting *minutes*

undo timer realtime-accounting

View

RADIUS scheme view

Default level

2: System level

Parameters

minutes: Real-time accounting interval in minutes, zero or a multiple of 3 in the range of 3 to 60.

Description

Use **timer realtime-accounting** to set the real-time accounting interval.

Use **undo timer realtime-accounting** to restore the default.

By default, the real-time accounting interval is 12 minutes.

For real-time accounting, a NAS must transmit the accounting information of online users to the RADIUS accounting server periodically. This command sets the interval.

When the real-time accounting interval on the switch is zero, the switch sends online user accounting information to the RADIUS accounting server at the real-time accounting interval configured on the server (if any) or does not send online user accounting information.

Different real-time accounting intervals impose different performance requirements on the NAS and the RADIUS server. A shorter interval helps achieve higher accounting precision but requires higher performance. Use a longer interval when there are a large number of users (1000 or more).

Table 7 Recommended real-time accounting intervals

Number of users	Real-time accounting interval (minutes)
1 to 99	3
100 to 499	6
500 to 999	12
1000 or more	15 or longer

Related commands: **retry realtime-accounting**.

Examples

Set the real-time accounting interval to 51 minutes for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer realtime-accounting 51
```

timer response-timeout (RADIUS scheme view)

Syntax

timer response-timeout *seconds*

undo timer response-timeout

View

RADIUS scheme view

Default level

2: System level

Parameters

seconds: RADIUS server response timeout period in seconds, in the range of 1 to 10.

Description

Use **timer response-timeout** to set the RADIUS server response timeout timer.

Use **undo timer response-timeout** to restore the default.

By default, the RADIUS server response timeout period is 3 seconds.

If a NAS receives no response from the RADIUS server in a period of time after sending a RADIUS request (authentication/authorization or accounting request), it resends the request so that the user has more opportunity to obtain the RADIUS service. The NAS uses the RADIUS server response timeout timer to control the transmission interval.

The maximum number of RADIUS packet transmission attempts multiplied by the RADIUS server response timeout period cannot be greater than 75.

Related commands: **retry**.

Examples

```
# Set the RADIUS server response timeout timer to 5 seconds for RADIUS scheme radius1.
```

```
<Sysname> system-view  
[Sysname] radius scheme radius1  
[Sysname-radius-radius1] timer response-timeout 5
```

user-name-format (RADIUS scheme view)

Syntax

user-name-format { **keep-original** | **with-domain** | **without-domain** }

View

RADIUS scheme view

Default level

2: System level

Parameters

keep-original: Sends the username to the RADIUS server as it is input.

with-domain: Includes the ISP domain name in the username sent to the RADIUS server.

without-domain: Excludes the ISP domain name from the username sent to the RADIUS server.

Description

Use **user-name-format** to specify the format of the username to be sent to a RADIUS server.

By default, the ISP domain name is included in the username.

A username is generally in the format *userid@isp-name*, of which *isp-name* is used by the switch to determine the ISP domain to which a user belongs. Some earlier RADIUS servers, however, cannot recognize a username including an ISP domain name. Before sending a username including a domain name to such a RADIUS server, the switch must remove the domain name. This command allows you to specify whether to include a domain name in a username to be sent to a RADIUS server.

If a RADIUS scheme defines that the username is sent without the ISP domain name, do not apply the RADIUS scheme to more than one ISP domain, avoiding the confused situation where the RADIUS server regards two users in different ISP domains but with the same *userid* as one.

For 802.1X users using EAP authentication, the **user-name-format** command configured for a RADIUS scheme does not take effect and the switch does not change the usernames from clients before forwarding them to the RADIUS server.

Related commands: **radius scheme**.

Examples

Specify the switch to remove the domain name in the username sent to the RADIUS servers for the RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] user-name-format without-domain
```

HWTACACS configuration commands

data-flow-format (HWTACACS scheme view)

Syntax

```
data-flow-format { data { byte | giga-byte | kilo-byte | mega-byte } | packet { giga-packet | kilo-packet | mega-packet | one-packet } } *
undo data-flow-format { data | packet }
```

View

HWTACACS scheme view

Default level

2: System level

Parameters

data { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** }: Specifies the unit for data flows, which can be byte, kilobyte, megabyte, or gigabyte.

packet { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** }: Specifies the unit for data packets, which can be one-packet, kilo-packet, mega-packet, or giga-packet.

Description

Use **data-flow-format** to set the traffic statistics unit for data flows or packets.

Use **undo data-flow-format** to restore the default.

By default, the unit for data flows is **byte** and that for data packets is **one-packet**.

The unit for data flows and that for packets must be consistent with those on the HWTACACS server. Otherwise, accounting cannot be performed correctly.

Related commands: **display hwtacacs**.

Examples

Set the traffic statistics unit for data flows and that for packets to kilobytes and kilo-packets respectively in HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] data-flow-format data kilo-byte packet kilo-packet
```

display hwtacacs

Syntax

```
display hwtacacs [ hwtacacs-scheme-name [ statistics ] ] [ slot slot-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

2: System level

Parameters

hwtacacs-scheme-name: HWTACACS scheme name.

statistics: Displays the statistics for the HWTACACS servers specified in the HWTACACS scheme. Without this keyword, the command displays the configuration of the HWTACACS scheme.

slot *slot-number*: Specifies the configuration or statistics for an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display hwtacacs** to display the configuration of HWTACACS schemes or the statistics for the HWTACACS servers specified in HWTACACS schemes.

If no HWTACACS scheme is specified, the command displays the configuration of all HWTACACS schemes.

Related commands: **hwtacacs scheme**.

Examples

Display the configuration of HWTACACS scheme **gy**.

```
<Sysname> display hwtacacs gy
```

```
-----
HWTACACS-server template name      : gy
Primary-authentication-server      : 172.31.1.11:49
Primary-authorization-server       : 172.31.1.11:49
Primary-accounting-server          : 172.31.1.11:49
Secondary-authentication-server     : 0.0.0.0:0
Secondary-authorization-server     : 0.0.0.0:0
Secondary-accounting-server        : 0.0.0.0:0
Current-authentication-server       : 172.31.1.11:49
Current-authorization-server       : 172.31.1.11:49
Current-accounting-server          : 172.31.1.11:49
```

```

NAS-IP-address           : 0.0.0.0
key authentication       : *****
key authorization        : *****
key accounting           : *****
Quiet-interval(min)      : 5
Realtime-accounting-interval(min) : 12
Response-timeout-interval(sec) : 5
Acct-stop-PKT retransmit times : 100
Username format          : with-domain
Data traffic-unit        : B
Packet traffic-unit      : one-packet
-----

```

Table 8 Command output

Field	Description
HWTACACS-server template name	Name of the HWTACACS scheme.
Primary-authentication-server	IP address and port number of the primary authentication server. If no primary authentication server is specified, this field displays 0.0.0.0:0 . This rule also applies to the following eight fields.
Primary-authorization-server	IP address and port number of the primary authorization server.
Primary-accounting-server	IP address and port number of the primary accounting server.
Secondary-authentication-server	IP address and port number of the secondary authentication server.
Secondary-authorization-server	IP address and port number of the secondary authorization server.
Secondary-accounting-server	IP address and port number of the secondary accounting server.
Current-authentication-server	IP address and port number of the currently used authentication server.
Current-authorization-server	IP address and port number of the currently used authorization server.
Current-accounting-server	IP address and port number of the currently used accounting server.
NAS-IP-address	IP address of the NAS. If no NAS is specified, this field displays 0.0.0.0 .
key authentication	Key for authentication, displayed as a series of asterisks (*****). If no shared key is configured, field displays a hyphen (-).
key authorization	Key for authorization, displayed as a series of asterisks (*****). If no shared key is configured, field displays a hyphen (-).
key accounting	Key for accounting, displayed as a series of asterisks (*****). If no shared key is configured, field displays a hyphen (-).
Acct-stop-PKT retransmit times	Number of stop-accounting packet transmission attempts.
Data traffic-unit	Unit for data flows.
Packet traffic-unit	Unit for data packets.

Display the statistics for the servers specified in HWTACACS scheme **gy**.

```
<Sysname> display hwtacacs gy statistics
```

```

Slot: 1
---[HWTACACS template gy primary authentication]---
HWTACACS server open number: 10
HWTACACS server close number: 10
HWTACACS authen client access request packet number: 10
HWTACACS authen client access response packet number: 6
HWTACACS authen client unknown type number: 0
HWTACACS authen client timeout number: 4
HWTACACS authen client packet dropped number: 4
HWTACACS authen client access request change password number: 0
HWTACACS authen client access request login number: 5
HWTACACS authen client access request send authentication number: 0
HWTACACS authen client access request send password number: 0
HWTACACS authen client access connect abort number: 0
HWTACACS authen client access connect packet number: 5
HWTACACS authen client access response error number: 0
HWTACACS authen client access response failure number: 0
HWTACACS authen client access response follow number: 0
HWTACACS authen client access response getdata number: 0
HWTACACS authen client access response getpassword number: 5
HWTACACS authen client access response getuser number: 0
HWTACACS authen client access response pass number: 1
HWTACACS authen client access response restart number: 0
HWTACACS authen client malformed access response number: 0
HWTACACS authen client round trip time(s): 5
---[HWTACACS template gy primary authorization]---
HWTACACS server open number: 1
HWTACACS server close number: 1
HWTACACS author client request packet number: 1
HWTACACS author client response packet number: 1
HWTACACS author client timeout number: 0
HWTACACS author client packet dropped number: 0
HWTACACS author client unknown type number: 0
HWTACACS author client request EXEC number: 1
HWTACACS author client response error number: 0
HWTACACS author client response EXEC number: 1
HWTACACS author client round trip time(s): 3
---[HWTACACS template gy primary accounting]---
HWTACACS server open number: 0
HWTACACS server close number: 0
HWTACACS account client request packet number: 0
HWTACACS account client response packet number: 0
HWTACACS account client unknown type number: 0
HWTACACS account client timeout number: 0
HWTACACS account client packet dropped number: 0
HWTACACS account client request command level number: 0
HWTACACS account client request connection number: 0
HWTACACS account client request EXEC number: 0

```

```
HWTACACS account client request network number: 0
HWTACACS account client request system event number: 0
HWTACACS account client request update number: 0
HWTACACS account client response error number: 0
HWTACACS account client round trip time(s): 0
```

display stop-accounting-buffer (for HWTACACS)

Syntax

```
display stop-accounting-buffer hwtacacs-scheme hwtacacs-scheme-name [ slot slot-number ] [ | { begin
| exclude | include } regular-expression ]
```

View

Any view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies buffered stop-accounting requests that are destined for the accounting server defined in an HWTACACS scheme. The HWTACACS scheme name is a case-insensitive string of 1 to 32 characters.

slot *slot-number*: Specifies the stop-accounting requests buffered for an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display stop-accounting-buffer** to display information about buffered stop-accounting requests.

Related commands: **reset stop-accounting-buffer**, **stop-accounting-buffer enable**, and **retry stop-accounting**.

Examples

```
# Display information about stop-accounting requests buffered for HWTACACS scheme hwt1.
Slot 1:
Total 0 record(s) Matched
```

hwtacacs nas-ip

Syntax

```
hwtacacs nas-ip ip-address
```

```
undo hwtacacs nas-ip ip-address
```

View

System view

Default level

2: System level

Parameters

ip-address: IP address in dotted decimal notation. It must be an address of the switch and cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

Description

Use **hwtaacacs nas-ip** to specify a source IP address for outgoing HWTACACS packets.

Use **undo hwtaacacs nas-ip** to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound interface.

The source IP address of HWTACACS packets that a NAS sends must match the IP address of the NAS that is configured on the HWTACACS server. An HWTACACS server identifies a NAS by IP address. Upon receiving an HWTACACS packet, an HWTACACS server checks whether the source IP address of the packet is the IP address of any managed NAS. If yes, the server processes the packet. If not, the server drops the packet.

You can specify up to 16 source IP addresses.

The setting configured by the **nas-ip** command in HWTACACS scheme view is only for the HWTACACS scheme, whereas that configured by the **hwtaacacs nas-ip** command in system view is for all HWTACACS schemes. The setting in HWTACACS scheme view takes precedence.

Related commands: **nas-ip**.

Examples

Set the IP address for the switch to use as the source address of the HWTACACS packets to **129.10.10.1**.

```
<Sysname> system-view  
[Sysname] hwtaacacs nas-ip 129.10.10.1
```

hwtaacacs scheme

Syntax

hwtaacacs scheme *hwtaacacs-scheme-name*

undo hwtaacacs scheme *hwtaacacs-scheme-name*

View

System view

Default level

3: Manage level

Parameters

hwtaacacs-scheme-name: HWTACACS scheme name, a case-insensitive string of 1 to 32 characters.

Description

Use **hwtaacacs scheme** to create an HWTACACS scheme and enter HWTACACS scheme view.

Use **undo hwtaacacs scheme** to delete an HWTACACS scheme.

By default, no HWTACACS scheme exists.

An HWTACACS scheme can be referenced by more than one ISP domain at the same time.

An HWTACACS scheme referenced by ISP domains cannot be removed.

Examples

```
# Create an HWTACACS scheme named hwt1 and enter HWTACACS scheme view.
```

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
```

```
[Sysname-hwtacacs-hwt1]
```

key (HWTACACS scheme view)

Syntax

```
key { accounting | authentication | authorization } [ cipher | simple ] key
```

```
undo key { accounting | authentication | authorization }
```

View

HWTACACS scheme view

Default level

2: System level

Parameters

accounting: Sets the shared key for secure HWTACACS accounting communication.

authentication: Sets the shared key for secure HWTACACS authentication communication.

authorization: Sets the shared key for secure HWTACACS authorization communication.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

key: Specifies the shared key string. This argument is case sensitive. In non-FIPS mode, a ciphertext shared key must be a string of 1 to 373 characters and a plaintext shared key must be a string of 1 to 64 characters. In FIPS mode, a ciphertext shared key must be a string of 8 to 373 characters, and a plaintext shared key must be a string of 8 to 64 characters that must include numbers, uppercase letters, lowercase letters, and special characters. If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

Description

Use **key** to set the shared key for secure HWTACACS authentication, authorization, or accounting communication.

Use **undo key** to remove the configuration.

By default, no shared key is configured.

The shared keys configured on the switch must match those configured on the HWTACACS servers.

For secrecy, all shared keys, including shared keys configured in plain text, are saved in cipher text.

Related commands: **display hwtacacs**.

Examples

```
# Set the shared key for secure HWTACACS accounting communication to hello in plain text.
```

```

<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] key accounting simple hello

# Set the shared key for secure HWTACACS accounting communication to hello in plain text.

<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] key accounting hello

```

nas-ip (HWTACACS scheme view)

Syntax

```

nas-ip ip-address
undo nas-ip

```

View

HWTACACS scheme view

Default level

2: System level

Parameters

ip-address: IP address in dotted decimal notation. It must be an address of the switch and cannot be 0.0.0.0, 255.255.255.255, a class D address, a class E address, or a loopback address.

Description

Use **nas-ip** to specify a source address for outgoing HWTACACS packets.

Use **undo nas-ip** to restore the default.

By default, the source IP address of an outgoing HWTACACS packet is configured by the **hwtacacs nas-ip** command in system view. If the **hwtacacs nas-ip** command is not configured, the source IP address is the IP address of the outbound interface.

The source IP address of HWTACACS packets that a NAS sends must match the IP address of the NAS that is configured on the HWTACACS server. An HWTACACS server identifies a NAS by IP address. Upon receiving an HWTACACS packet, an HWTACACS server checks whether the source IP address of the packet is the IP address of any managed NAS. If yes, the server processes the packet. If not, the server drops the packet.

If you execute the command multiple times, the most recent configuration takes effect.

The setting configured by the **nas-ip** command in HWTACACS scheme view is only for the HWTACACS scheme, whereas that configured by the **hwtacacs nas-ip** command in system view is for all HWTACACS schemes. The setting in HWTACACS scheme view takes precedence.

Related commands: **hwtacacs nas-ip**.

Examples

```

# Set the source address for outgoing HWTACACS packets to 10.1.1.1.

<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] nas-ip 10.1.1.1

```

primary accounting (HWTACACS scheme view)

Syntax

```
primary accounting ip-address [ port-number ]  
undo primary accounting
```

View

HWTACACS scheme view

Default level

2: System level

Parameters

ip-address: IP address of the primary HWTACACS accounting server, in dotted decimal notation. The default setting is 0.0.0.0.

port-number: Service port number of the primary HWTACACS accounting server. It ranges from 1 to 65535 and defaults to 49.

Description

Use **primary accounting** to specify the primary HWTACACS accounting server.

Use **undo primary accounting** to remove the configuration.

By default, no primary HWTACACS accounting server is specified.

The IP addresses of the primary and secondary accounting servers must be different. Otherwise, the configuration fails.

If you execute the command multiple times, the most recent configuration takes effect.

You can remove an accounting server only when it is not used by any active TCP connection to send accounting packets. Removing an accounting server affects only accounting processes that occur after the remove operation.

Related commands: **display hwtacacs**.

Examples

Specify the IP address and port number of the primary accounting server for HWTACACS scheme **test1** as 10.163.155.12 and 49.

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme test1
```

```
[Sysname-hwtacacs-test1] primary accounting 10.163.155.12 49
```

primary authentication (HWTACACS scheme view)

Syntax

```
primary authentication ip-address [ port-number ]  
undo primary authentication
```

View

HWTACACS scheme view

Default level

2: System level

Parameters

ip-address: IP address of the primary HWTACACS authentication server, in dotted decimal notation. The default setting is 0.0.0.0.

port-number: Service port number of the primary HWTACACS authentication server. It ranges from 1 to 65535 and defaults to 49.

Description

Use **primary authentication** to specify the primary HWTACACS authentication server.

Use **undo primary authentication** to remove the configuration.

By default, no primary HWTACACS authentication server is specified.

The IP addresses of the primary and secondary authentication servers must be different. Otherwise, the configuration fails.

If you execute the command multiple times, the most recent configuration takes effect.

You can remove an authentication server only when it is not used by any active TCP connection to send authentication packets. Removing an authentication server affects only authentication processes that occur after the remove operation.

Related commands: **display hwtacacs**.

Examples

Specify the IP address and port number of the primary authentication server for HWTACACS scheme **hwt1** as 10.163.155.13 and 49.

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
```

```
[Sysname-hwtacacs-hwt1] primary authentication 10.163.155.13 49
```

primary authorization

Syntax

primary authorization *ip-address* [*port-number*]

undo primary authorization

View

HWTACACS scheme view

Default level

2: System level

Parameters

ip-address: IP address of the primary HWTACACS authorization server, in dotted decimal notation. The default setting is 0.0.0.0.

port-number: Service port number of the primary HWTACACS authorization server. It ranges from 1 to 65535 and defaults to 49.

Description

Use **primary authorization** to specify the primary HWTACACS authorization server.

Use **undo primary authorization** to remove the configuration.

By default, no primary HWTACACS authorization server is specified.

The IP addresses of the primary and secondary authorization servers must be different. Otherwise, the configuration fails.

If you execute the command multiple times, the most recent configuration takes effect.

You can remove an authorization server only when it is not used by any active TCP connection to send authorization packets. Removing an authorization server affects only authorization processes that occur after the remove operation.

Related commands: **display hwtacacs**.

Examples

```
# Configure the IP address and port number of the primary authorization server for HWTACACS scheme hwt1 as 10.163.155.13 and 49.
```

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
```

```
[Sysname-hwtacacs-hwt1] primary authorization 10.163.155.13 49
```

reset hwtacacs statistics

Syntax

```
reset hwtacacs statistics { accounting | all | authentication | authorization } [ slot slot-number ]
```

View

User view

Default level

1: Monitor level

Parameters

accounting: Clears HWTACACS accounting statistics.

all: Clears all HWTACACS statistics.

authentication: Clears HWTACACS authentication statistics.

authorization: Clears HWTACACS authorization statistics.

slot slot-number: Clears HWTACACS statistics for an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

Description

Use **reset hwtacacs statistics** to clear HWTACACS statistics.

Related commands: **display hwtacacs**.

Examples

```
# Clear all HWTACACS statistics.
```

```
<Sysname> reset hwtacacs statistics all
```

reset stop-accounting-buffer (for HWTACACS)

Syntax

reset stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name* [**slot** *slot-number*]

View

User view

Default level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies buffered stop-accounting requests that are destined for the accounting server defined in an HWTACACS scheme. The HWTACACS scheme name is a case-insensitive string of 1 to 32 characters.

slot *slot-number*: Clears the stop-accounting requests buffered for an IRF member device. The *slot-number* argument represents the ID of the IRF member device. The value range for the argument depends on the number of member devices and their member IDs in the IRF fabric.

Description

Use **reset stop-accounting-buffer** to clear buffered stop-accounting requests that get no responses.

Related commands: **stop-accounting-buffer enable** and **display stop-accounting-buffer**.

Examples

Clear the stop-accounting requests buffered for HWTACACS scheme **hwt1**.

```
<Sysname> reset stop-accounting-buffer hwtacacs-scheme hwt1
```

retry stop-accounting (HWTACACS scheme view)

Syntax

retry stop-accounting *retry-times*

undo retry stop-accounting

View

HWTACACS scheme view

Default level

2: System level

Parameters

retry-times: Maximum number of stop-accounting request transmission attempts, in the range of 1 to 300.

Description

Use **retry stop-accounting** to set the maximum number of stop-accounting request transmission attempts.

Use **undo retry stop-accounting** to restore the default.

By default, the maximum number of stop-accounting request transmission attempts is 100.

Related commands: **reset stop-accounting-buffer** and **display stop-accounting-buffer**.

Examples

```
# Set the maximum number of stop-accounting request transmission attempts to 50 for HWTACACS
scheme hwt1.
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] retry stop-accounting 50
```

secondary accounting (HWTACACS scheme view)

Syntax

```
secondary accounting ip-address [ port-number ]
undo secondary accounting
```

View

HWTACACS scheme view

Default level

2: System level

Parameters

ip-address: IP address of the secondary HWTACACS accounting server, in dotted decimal notation. The default setting is 0.0.0.0.

port-number: Service port number of the secondary HWTACACS accounting server. It ranges from 1 to 65535 and defaults to 49.

Description

Use **secondary accounting** to specify the secondary HWTACACS accounting server.

Use **undo secondary accounting** to remove the configuration.

By default, no secondary HWTACACS accounting server is specified.

The IP addresses of the primary and secondary accounting servers must be different. Otherwise, the configuration fails.

If you execute the command multiple times, the most recent configuration takes effect.

You can remove an accounting server only when it is not used by any active TCP connection to send accounting packets. Removing an accounting server affects only accounting processes that occur after the remove operation.

Related commands: **display hwtacacs**.

Examples

```
# Specify the IP address and port number of the secondary accounting server for HWTACACS scheme
hwt1 as 10.163.155.12 with TCP port number 49.
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary accounting 10.163.155.12 49
```

secondary authentication (HWTACACS scheme view)

Syntax

secondary authentication *ip-address* [*port-number*]

undo secondary authentication

View

HWTACACS scheme view

Default level

2: System level

Parameters

ip-address: IP address of the secondary HWTACACS authentication server, in dotted decimal notation. The default setting is 0.0.0.0.

port-number: Service port number of the secondary HWTACACS authentication server. It ranges from 1 to 65535 and defaults to 49.

Description

Use **secondary authentication** to specify the secondary HWTACACS authentication server.

Use **undo secondary authentication** to remove the configuration.

By default, no secondary HWTACACS authentication server is specified.

The IP addresses of the primary and secondary authentication servers must be different. Otherwise, the configuration fails.

If you execute the command multiple times, the most recent configuration takes effect.

You can remove an authentication server only when it is not used by any active TCP connection to send authentication packets is using it. Removing an authentication server affects only authentication processes that occur after the remove operation.

Related commands: **display hwtacacs**.

Examples

Specify the IP address and port number of the secondary authentication server for HWTACACS scheme **hwt1** as 10.163.155.13 with TCP port number 49.

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
```

```
[Sysname-hwtacacs-hwt1] secondary authentication 10.163.155.13 49
```

secondary authorization

Syntax

secondary authorization *ip-address* [*port-number*]

undo secondary authorization

View

HWTACACS scheme view

Default level

2: System level

Parameters

ip-address: IP address of the secondary HWTACACS authorization server, in dotted decimal notation. The default setting is 0.0.0.0.

port-number: Service port number of the secondary HWTACACS authorization server. It ranges from 1 to 65535 and defaults to 49.

Description

Use **secondary authorization** to specify the secondary HWTACACS authorization server.

Use **undo secondary authorization** to remove the configuration.

By default, no secondary HWTACACS authorization server is specified.

The IP addresses of the primary and secondary authorization servers cannot be the same. Otherwise, the configuration fails.

If you execute the command multiple times, the most recent configuration takes effect.

You can remove an authorization server only when it is not used by any active TCP connection to send authorization packets. Removing an authorization server affects only authorization processes that occur after the remove operation.

Related commands: **display hwtacacs**.

Examples

```
# Configure the secondary authorization server 10.163.155.13 with TCP port number 49.
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authorization 10.163.155.13 49
```

stop-accounting-buffer enable (HWTACACS scheme view)

Syntax

stop-accounting-buffer enable

undo stop-accounting-buffer enable

View

HWTACACS scheme view

Default level

2: System level

Parameters

None

Description

Use **stop-accounting-buffer enable** to enable the switch to buffer stop-accounting requests to which no responses are received.

Use **undo stop-accounting-buffer enable** to disable the buffering function.

By default, the switch buffers stop-accounting requests to which no responses are received.

Stop-accounting requests affect the charge to users. A NAS must make its best effort to send every stop-accounting request to the HWTACACS accounting servers. For each stop-accounting request getting no response in the specified period of time, the NAS buffers and resends the packet until it receives a response or the number of transmission attempts reaches the configured limit. In the latter case, the NAS discards the packet.

Related commands: **reset stop-accounting-buffer** and **display stop-accounting-buffer**.

Examples

```
# In HWTACACS scheme hwt1, enable the switch to buffer the stop-accounting requests getting no responses.
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] stop-accounting-buffer enable
```

timer quiet (HWTACACS scheme view)

Syntax

```
timer quiet minutes
undo timer quiet
```

View

HWTACACS scheme view

Default level

2: System level

Parameters

minutes: Primary server quiet period. The value ranges from 1 to 255, in minutes.

Description

Use **timer quiet** to set the quiet timer for the primary server. When the primary server is found unreachable, the switch changes the status of the server from active to blocked and keeps the server in blocked state until this timer expires.

Use **undo timer quiet** to restore the default.

By default, the primary server quiet period is 5 minutes.

Related commands: **display hwtacacs**.

Examples

```
# Set the quiet timer for the primary server to 10 minutes.
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer quiet 10
```

timer realtime-accounting (HWTACACS scheme view)

Syntax

```
timer realtime-accounting minutes
undo timer realtime-accounting
```

View

HWTACACS scheme view

Default level

2: System level

Parameters

minutes: Real-time accounting interval in minutes, zero or a multiple of 3 in the range of 3 to 60. A value of zero means "Do not send online user accounting information to the HWTACACS server."

Description

Use **timer realtime-accounting** to set the real-time accounting interval.

Use **undo timer realtime-accounting** to restore the default.

By default, the real-time accounting interval is 12 minutes.

For real-time accounting, a NAS must transmit the accounting information of online users to the HWTACACS accounting server periodically. This command is for setting the interval.

Consider the performance of the NAS and the HWTACACS server when you set the real-time accounting interval. A shorter interval requires higher performance. Use a longer interval when there are a large number of users (more than 1000, inclusive).

Table 9 Recommended real-time accounting intervals

Number of users	Real-time accounting interval (minutes)
1 to 99	3
100 to 499	6
500 to 999	12
1000 or more	15 or more

Examples

```
# Set the real-time accounting interval to 51 minutes for HWTACACS scheme hwt1.  
<Sysname> system-view  
[Sysname] hwtacacs scheme hwt1  
[Sysname-hwtacacs-hwt1] timer realtime-accounting 51
```

timer response-timeout (HWTACACS scheme view)

Syntax

timer response-timeout *seconds*

undo timer response-timeout

View

HWTACACS scheme view

Default level

2: System level

Parameters

seconds: HWTACACS server response timeout period in seconds, in the range of 1 to 300.

Description

Use **timer response-timeout** to set the HWTACACS server response timeout timer.

Use **undo timer response-timeout** to restore the default.

By default, the HWTACACS server response timeout time is 5 seconds.

HWTACACS is based on TCP. When the server response timeout timer or the TCP timeout timer times out, the switch is disconnected from the HWTACACS server.

Related commands: **display hwtacacs**.

Examples

```
# Set the HWTACACS server response timeout timer to 30 seconds for HWTACACS scheme hwt1.  
<Sysname> system-view  
[Sysname] hwtacacs scheme hwt1  
[Sysname-hwtacacs-hwt1] timer response-timeout 30
```

user-name-format (HWTACACS scheme view)

Syntax

user-name-format { **keep-original** | **with-domain** | **without-domain** }

View

HWTACACS scheme view

Default level

2: System level

Parameters

keep-original: Sends the username to the HWTACACS server as it is input.

with-domain: Includes the ISP domain name in the username sent to the HWTACACS server.

without-domain: Excludes the ISP domain name from the username sent to the HWTACACS server.

Description

Use **user-name-format** to specify the format of the username to be sent to an HWTACACS server.

By default, the ISP domain name is included in the username.

A username is generally in the format *userid@isp-name*, of which *isp-name* is used by the switch to determine the ISP domain to which a user belongs. Some earlier HWTACACS servers, however, cannot recognize a username including an ISP domain name. Before sending a username including a domain name to such an HWTACACS server, the switch must remove the domain name. This command allows you to specify whether to include a domain name in a username to be sent to an HWTACACS server.

If an HWTACACS scheme defines that the username is sent without the ISP domain name, do not apply the HWTACACS scheme to more than one ISP domain, avoiding the confused situation where the HWTACACS server regards two users in different ISP domains but with the same *userid* as one.

Examples

Specify the switch to remove the ISP domain name in the username sent to the HWTACACS servers for the HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] user-name-format without-domain
```

RADIUS server configuration commands

authorization-attribute (RADIUS-server user view)

Syntax

authorization-attribute { **acl** *acl-number* | **vlan** *vlan-id* } *
undo authorization-attribute { **acl** | **vlan** } *

View

RADIUS-server user view

Default level

2: System level

Parameters

acl *acl-number*: Specifies the number of an ACL in the range of 2000 to 5999.

vlan *vlan-id*: Specifies the ID of a VLAN in the range of 1 to 4094.

Description

Use **authorization-attribute** to specify the authorization attributes (ACL and VLAN) that the RADIUS server assigns to the RADIUS client in a response message after the RADIUS user passes RADIUS authentication. The RADIUS client uses the assigned authorization attributes to control the access of the RADIUS user.

Use **undo authorization-attribute** to remove the configuration.

By default, no authorization attribute is configured.

Related commands: **radius-server user**.

Examples

Configure the authorized VLAN for RADIUS user **user1** as VLAN 3.

```
<Sysname> system-view
[Sysname] radius-server user user1
[Sysname-rdsuser-user1] authorization-attribute vlan 3
```

description

Syntax

description *text*
undo description

View

RADIUS-server user view

Default level

2: System level

Parameters

text: Description of the RADIUS user, a case-sensitive string of 1 to 255 characters.

Description

Use **description** to configure a description for the RADIUS user. The description is used for user information management.

Use **undo description** to remove the user description.

By default, no description is configured for the RADIUS user.

Related commands: **radius-server user**.

Examples

Configure a description of **VIP user** for RADIUS user **user1**.

```
<Sysname> system-view
```

```
[Sysname] radius-server user user1
```

```
[Sysname-rdsuser-user1] description VIP user
```

expiration-date (RADIUS-server user view)

Syntax

expiration-date *time*

undo expiration-date

View

RADIUS-server user view

Default level

2: System level

Parameters

time: Expiration time of the RADIUS user, in the format HH:MM:SS-MM/DD/YYYY or HH:MM:SS-YYYY/MM/DD. HH:MM:SS indicates the time, where HH ranges from 0 to 23, and MM and SS range from 0 to 59. YYYY/MM/DD indicates the date, where YYYY ranges from 2000 to 2035, MM ranges from 1 to 12, and the range of DD depends on the month. Except for the zeros in 00:00:00, leading zeros can be omitted. For example, 2:2:0-2011/2/2 equals 02:02:00-2011/02/02.

Description

Use **expiration-date** to configure the expiration time of a RADIUS user.

Use **undo expiration-date** to remove the configuration.

By default, a RADIUS user has no expiration time and no expiration check is performed.

For temporary network access requirements, create a guest account for the user and specify an expiration time for the account. After the user passes authentication, the RADIUS server checks whether the current system time is before the expiration time. If yes, it permits the user to access the network. Otherwise, it denies the access request of the user.

If you change the system time manually or the system time is changed in any other way, the switch uses the new system time for expiration check.

Related commands: **radius-server user**.

Examples

Configure user **user1** to expire in 12:10:20 on May 31, 2012.

```
<Sysname> system-view
[Sysname] radius-server user user1
[Sysname-rdsuser-user1] expiration-date 12:10:20-2012/05/31
```

password (RADIUS-server user view)

Syntax

password [**cipher** | **simple**] *password*
undo password

View

RADIUS-server user view

Default level

2: System level

Parameters

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 128 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 201 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password string.

Description

Use **password** to configure a password for the RADIUS user.

Use **undo password** to delete the password of the RADIUS user.

By default, no password is configured for the RADIUS user.

For secrecy, all passwords, including passwords configured in plain text, are saved in cipher text.

Related commands: **radius-server user**.

Examples

Set the password of **user1** to 123456 in plain text.

```
<Sysname> system-view
[Sysname] radius-server user user1
[Sysname-rdsuser-user1] password simple 123456
```

radius-server client-ip

Syntax

radius-server client-ip *ip-address* [**key** [**cipher** | **simple**] *string*]
undo radius-server client-ip { *ip-address* | **all** }

View

System view

Default level

2: System level

Parameters

ip-address: Specifies the IPv4 address of the RADIUS client.

key: Sets the shared key for secure communication with the RADIUS client.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

string: Specifies the shared key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 64 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters. If neither **cipher** nor **simple** is specified, you set a plaintext shared key string.

all: Specifies all RADIUS clients.

Description

Use **radius-server client-ip** to specify a RADIUS client.

Use **undo radius-server client-ip** to delete the specified RADIUS client or all RADIUS clients.

The IP address of the RADIUS client specified on the RADIUS server must be consistent with the source IP address of RADIUS packets configured on the RADIUS client.

The shared key specified on the RADIUS server must be consistent with that configured on the RADIUS client.

You can specify multiple RADIUS clients.

For secrecy, all passwords, including passwords configured in plain text, are saved in cipher text.

Examples

Specify RADIUS client 10.1.1.1 and set the shared key to 1234 in plain text.

```
<Sysname> system-view
```

```
[Sysname] radius-server client-ip 10.1.1.1 key simple 1234
```

radius-server user

Syntax

radius-server user *user-name*

undo radius-server user { *user-name* | **all** }

View

System view

Default level

2: System level

Parameters

user-name: *user-name*: RADIUS username, a case-sensitive string of 1 to 64 characters that can contain the domain name. It cannot contain question mark (?), left angle bracket (<), right angle bracket (>),

backslash (\), quotation marks ("), percent sign (%), apostrophe ('), ampersand (&), pound sign (#), or spaces, and cannot be **a**, **al**, or **all**.

all: Removes all RADIUS users.

Description

Use **radius-server user** to create a RADIUS user and enter RADIUS-server user view.

Use **undo radius-server user** to delete the specified RADIUS user or all RADIUS users.

By default, no RADIUS user exists.

If the switch is configured to send usernames that carry the domain name to the RADIUS server, the username of the RADIUS user configured here must contain the domain name. If not, the username of the RADIUS user configured here does not contain the domain name.

Related commands: **user-name-format** (RADIUS scheme view).

Examples

Create RADIUS user **user1** and enter its view.

```
<Sysname> system-view
[Sysname] radius-server user user1
[Sysname-rdsuser-user1]
```

802.1X configuration commands

display dot1x

Syntax

```
display dot1x [ sessions | statistics ] [ interface interface-list ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

sessions: Displays 802.1X session information.

statistics: Displays 802.1X statistics.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 ports or port ranges. The start port number must be smaller than the end number and the two interfaces must be the same type.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display dot1x** to display information about 802.1X.

If you specify neither the **sessions** keyword nor the **statistics** keyword, the command displays all information about 802.1X, including session information, statistics, and configurations.

Related commands: **reset dot1x statistics**, **dot1x**, **dot1x retry**, **dot1x max-user**, **dot1x port-control**, **dot1x port-method**, and **dot1x timer**.

Examples

Display all information about 802.1X.

```
<Sysname> display dot1x
Equipment 802.1X protocol is enabled
CHAP authentication is enabled
EAD quick deploy is enabled
```

Configuration: Transmit Period 30 s, Handshake Period 15 s
Quiet Period 60 s, Quiet Period Timer is disabled
Supp Timeout 30 s, Server Timeout 100 s
Reauth Period 3600 s
The maximal retransmitting times 3

EAD quick deploy configuration:

URL: http://192.168.19.23
Free IP: 192.168.19.0 255.255.255.0
EAD timeout: 30m

The maximum 802.1X user resource number is 1024 per slot

Total current used 802.1X resource number is 1

GigabitEthernet1/0/1 is link-up

802.1X protocol is enabled
Handshake is disabled
Handshake secure is disabled
802.1X unicast-trigger is enabled
Periodic reauthentication is disabled
The port is an authenticator
Authenticate Mode is Auto
Port Control Type is Mac-based
802.1X Multicast-trigger is enabled
Mandatory authentication domain: NOT configured
Guest VLAN: 4
Auth-fail VLAN: NOT configured
Critical VLAN: 3
Critical recovery-action: reinitialize
Max number of on-line users is 256

EAPOL Packet: Tx 1087, Rx 986
Sent EAP Request/Identity Packets : 943
EAP Request/Challenge Packets: 60
EAP Success Packets: 29, Fail Packets: 55
Received EAPOL Start Packets : 60
EAPOL LogOff Packets: 24
EAP Response/Identity Packets : 724
EAP Response/Challenge Packets: 54
Error Packets: 0

1. Authenticated user : MAC address: 0015-e9a6-7cfe

Controlled User(s) amount to 1

Table 10 Command output

Field	Description
Equipment 802.1X protocol is enabled	Specifies whether 802.1X is enabled globally
CHAP authentication is enabled	Specifies whether CHAP authentication is enabled
EAD quick deploy is enabled	Specifies whether EAD fast deployment is enabled
Transmit Period	Username request timeout timer in seconds
Handshake Period	Handshake timer in seconds
Reauth Period	Periodic online user re-authentication timer in seconds
Quiet Period	Quiet timer in seconds
Quiet Period Timer is disabled	Status of the quiet timer. In this example, the quiet timer is enabled.
Supp Timeout	Client timeout timer in seconds
Server Timeout	Server timeout timer in seconds
The maximal retransmitting times	Maximum number of attempts for sending an authentication request to a client
EAD quick deploy configuration	EAD fast deployment configuration
URL	Redirect URL for unauthenticated users using a web browser to access the network
Free IP	Freely accessible network segment
EAD timeout	EAD rule timer in minutes
The maximum 802.1X user resource number per slot	Maximum number of concurrent 802.1X user per card
Total current used 802.1X resource number	Total number of online 802.1X users
GigabitEthernet1/0/1 is link-up	Status of the port. In this example, GigabitEthernet 1/0/1 is up.
802.1X protocol is disabled	Specifies whether 802.1X is enabled on the port
Handshake is disabled	Specifies whether handshake is enabled on the port
Handshake secure is disabled	Specifies whether handshake security is enabled on the port
802.1X unicast-trigger is disabled	Specifies whether unicast trigger is enabled on the port.
Periodic reauthentication is disabled	Specifies whether periodic online user re-authentication is enabled on the port
The port is an authenticator	Role of the port
Authenticate Mode is Auto	Authorization state of the port
Port Control Type is Mac-based	Access control method of the port
802.1X Multicast-trigger is enabled	Specifies whether the 802.1X multicast-trigger function is enabled
Mandatory authentication domain	Mandatory authentication domain on the port
Guest VLAN	802.1X guest VLAN configured on the port. NOT configured is displayed if no guest VLAN is configured.

Field	Description
Auth-fail VLAN	Auth-Fail VLAN configured on the port. NOT configured is displayed if no Auth-Fail VLAN is configured.
Critical VLAN	802.1X critical VLAN configured on the port. NOT configured is displayed if no 802.1X critical VLAN is configured on the port.
Critical recovery-action	Action that the port takes when an active (reachable) authentication server is detected available for the 802.1X users in the critical VLAN: <ul style="list-style-type: none"> • reinitialize—The port triggers authentication. • NOT configured—The port does not trigger authentication.
Max number of on-line users	Maximum number of concurrent 802.1X users on the port
EAPOL Packet	Number of sent (Tx) and received (Rx) EAPOL packets
Sent EAP Request/Identity Packets	Number of sent EAP-Request/Identity packets
EAP Request/Challenge Packets	Number of sent EAP-Request/Challenge packets
EAP Success Packets	Number of sent EAP Success packets
Fail Packets	Number of sent EAP-Failure packets
Received EAPOL Start Packets	Number of received EAPOL-Start packets
EAPOL LogOff Packets	Number of received EAPOL-LogOff packets
EAP Response/Identity Packets	Number of received EAP-Response/Identity packets
EAP Response/Challenge Packets	Number of received EAP-Response/Challenge packets
Error Packets	Number of received error packets
Authenticated user	User that has passed 802.1X authentication
Controlled User(s) amount	Number of authenticated users on the port

dot1x

Syntax

In system view:

```
dot1x [ interface interface-list ]
```

```
undo dot1x [ interface interface-list ]
```

In Ethernet interface view:

```
dot1x
```

```
undo dot1x
```

View

System view, Ethernet interface view

Default level

2: System level

Parameters

interface *interface-list*: Specifies a port list, which can contain multiple ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 ports or port ranges. The start port number must be smaller than the end number and the two ports must be of the same type.

Description

Use **dot1x** in system view to enable 802.1X globally.

Use **undo dot1x** in system view to disable 802.1X globally.

Use **dot1x interface** in system view or **dot1x** in interface view to enable 802.1X for specified ports.

Use **undo dot1x interface** in system view or the **undo dot1x** command in interface view to disable 802.1X for specified ports.

By default, 802.1X is neither enabled globally nor enabled for any port.

802.1X must be enabled both globally in system view and for the intended ports in system view or interface view. Otherwise, it does not function.

You can configure 802.1X parameters either before or after enabling 802.1X.

Related commands: **display dot1x**.

Examples

Enable 802.1X for ports GigabitEthernet 1/0/1, and GigabitEthernet 1/0/5 to GigabitEthernet 1/0/7.

```
<Sysname> system-view
```

```
[Sysname] dot1x interface gigabitethernet 1/0/1 gigabitethernet 1/0/5 to gigabitethernet 1/0/7
```

Or

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x
```

```
[Sysname-GigabitEthernet1/0/1] quit
```

```
[Sysname] interface gigabitethernet 1/0/5
```

```
[Sysname-GigabitEthernet1/0/5] dot1x
```

```
[Sysname-GigabitEthernet1/0/5] quit
```

```
[Sysname] interface gigabitethernet 1/0/6
```

```
[Sysname-GigabitEthernet1/0/6] dot1x
```

```
[Sysname-GigabitEthernet1/0/6] quit
```

```
[Sysname] interface gigabitethernet 1/0/7
```

```
[Sysname-GigabitEthernet1/0/7] dot1x
```

Enable 802.1X globally.

```
<Sysname> system-view
```

```
[Sysname] dot1x
```

dot1x attempts max-fail

Syntax

dot1x attempts max-fail *unsuccessful-attempts*
undo dot1x attempts max-fail

View

Layer 2 Ethernet interface view

Default level:

2: System level

Parameters

unsuccessful-attempts: Sets the maximum number of 802.1X authentication attempts that a MAC-authenticated user can try. The value range is 1 to 50.

Description

Use **dot1x attempts max-fail** to set the maximum number of 802.1X authentication attempts that a MAC-authenticated user can try.

Use **undo dot1x attempts max-fail** to restore the default.

By default, an authenticated MAC authentication user can retry 802.1X authentication until the maximum number of authentication attempts configured on the 802.1X client is reached.

If both MAC authentication and 802.1X authentication are enabled on a port, the device allows an authenticated MAC authentication user to initiate an 802.1X authentication. If the user passes 802.1X authentication, the user goes online as an 802.1X user. If the user fails 802.1X authentication, the user can retry authentication until the maximum number of authentication attempts is reached.

Examples

Set the maximum number of 802.1X authentication attempts to 3 on Ethernet 1/0/1 for MAC authentication users.

```
<Sysname> system-view  
[Sysname] interface ethernet 1/0/1  
[Sysname-Ethernet1/0/1] dot1x attempts max-fail 3
```

dot1x authentication-method

Syntax

dot1x authentication-method { chap | eap | pap }
undo dot1x authentication-method

View

System view

Default level

2: System level

Parameters

chap: Sets the access device to perform Extensible Authentication Protocol (EAP) termination and use the Challenge Handshake Authentication Protocol (CHAP) to communicate with the RADIUS server.

eap: Sets the access device to relay EAP packets, and supports any of the EAP authentication methods to communicate with the RADIUS server.

pap: Sets the access device to perform EAP termination and use the Password Authentication Protocol (PAP) to communicate with the RADIUS server.

Description

Use **dot1x authentication-method** to specify an EAP message handling method.

Use **undo dot1x authentication-method** to restore the default.

By default, the network access device performs EAP termination and uses CHAP to communicate with the RADIUS server.

The network access device terminates or relays EAP packets:

- In EAP termination mode, the access device re-encapsulates and sends the authentication data from the client in standard RADIUS packets to the RADIUS server, and performs either CHAP or PAP authentication with the RADIUS server. In this mode the RADIUS server supports only MD5-Challenge EAP authentication, and "username+password" EAP authentication initiated by an iNode client.
 - PAP transports usernames and passwords in clear text. The authentication method applies to scenarios that do not require high security. To use PAP, the client must be an HP iNode 802.1X client.
 - CHAP transports username in plaintext and encrypted password over the network. It is more secure than PAP.
- In EAP relay mode, the access device relays EAP messages between the client and the RADIUS server. The EAP relay mode supports multiple EAP authentication methods, such as MD5-Challenge, EAP-TL, and PEAP. To use this mode, you must make sure that the RADIUS server supports the EAP-Message and Message-Authenticator attributes, and uses the same EAP authentication method as the client. If this mode is used, the **user-name-format** command configured in RADIUS scheme view does not take effect. For more information about the **user-name-format** command, see "[RADIUS configuration commands](#)."

Local authentication supports PAP and CHAP.

If RADIUS authentication is used, you must configure the network access device to use the same authentication method (PAP, CHAP, or EAP) as the RADIUS server.

Related commands: **display dot1x**.

Examples

Enable the access device to terminate EAP packets and perform PAP authentication with the RADIUS server.

```
<Sysname> system-view
[Sysname] dot1x authentication-method pap
```


dot1x auth-fail vlan

Syntax

dot1x auth-fail vlan *authfail-vlan-id*
undo dot1x auth-fail vlan

View

Ethernet interface view

Default level

2: System level

Parameters

authfail-vlan-id: Specifies the ID of the Auth-Fail VLAN for the port, in the range of 1 to 4094. Make sure that the VLAN has been created.

Descriptions

Use **dot1x auth-fail vlan** to configure an Auth-Fail VLAN for a port. An Auth-Fail VLAN accommodates users that have failed 802.1X authentication because of the failure to comply with the organization security strategy, such as using a wrong password.

Use **undo dot1x auth-fail vlan** to restore the default.

By default, no Auth-Fail VLAN is configured on a port.

You must enable MAC-based VLAN for an Auth-Fail VLAN to take effect on a port that performs MAC-based access control.

When you change the access control method from MAC-based to port-based on a port that carries an Auth-Fail VLAN, the mappings between MAC addresses and the 802.1X Auth-Fail VLAN are removed. You can use the **display mac-vlan** command to display MAC-to-VLAN mappings.

You must enable 802.1X multicast trigger function for an Auth-Fail VLAN to take effect on a port that performs port-based access control.

When you change the access control method from port-based to MAC-based on a port that is in an Auth-Fail VLAN, the port is removed from the Auth-Fail VLAN.

To delete a VLAN that has been configured as an Auth-Fail VLAN, you must remove the Auth-Fail VLAN configuration first.

Related commands: **dot1x** and **dot1x port-method**.

Examples

```
# Configure VLAN 3 as the Auth-Fail VLAN for port GigabitEthernet 1/0/1.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] dot1x auth-fail vlan 3
```

dot1x critical vlan

Syntax

dot1x critical vlan *vlan-id*

undo dot1x critical vlan

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

vlan-id: Specifies a VLAN ID, in the range of 1 to 4094. Make sure the VLAN has been created.

Description

Use **dot1x critical vlan** to configure an 802.1X critical VLAN on a port for 802.1X users that have failed authentication because all the RADIUS authentication servers in their ISP domain are unreachable.

Use **undo dot1x critical vlan** to restore the default.

By default, no 802.1X critical VLAN is configured on a port.

The 802.1X critical VLAN configuration applies to 802.1X users that use only RADIUS authentication servers and have failed authentication because all the servers in their ISP domain become unavailable (inactive), for example, for the loss of network connectivity. If an 802.1X user fails local authentication after RADIUS authentication, the user is not assigned to the critical VLAN.

You can configure only one 802.1X critical VLAN on a port. The 802.1X critical VLANs on different ports can be different.

Assign different IDs to the voice VLAN, the port VLAN, and the 802.1X critical VLAN on a port, so the port can correctly process VLAN tagged incoming traffic.

To have the 802.1X critical VLAN take effect, complete the following tasks:

- Enable 802.1X both globally and on the interface.
- If the port performs port-based access control, enable the 802.1X multicast trigger function.
- If the port performs MAC-based access control, configure the MAC-based VLAN function on the port.

When you change the access control method from MAC-based to port-based on the port, the mappings between MAC addresses and the 802.1X critical VLAN are removed. You can use the **display mac-vlan** command to display MAC-to-VLAN mappings.

When you change the access control method from port-based to MAC-based on a port that is in a critical VLAN, the port is removed from the critical VLAN.

To delete a VLAN that has been configured as an 802.1X critical VLAN, you must remove the 802.1X critical VLAN configuration first.

Related commands: **dot1x**, **dot1x port-method**, and **dot1x critical recovery-action**.

Examples

Specify VLAN 3 as the 802.1X critical VLAN for port GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x critical vlan 3
```

dot1x critical recovery-action

Syntax

dot1x critical recovery-action reinitialize
undo dot1x critical recovery-action

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

reinitialize: Enables the port to trigger 802.1X re-authentication on detection of a reachable RADIUS authentication server for users in the critical VLAN.

Description

Use **dot1x critical recovery-action** to configure the action that a port takes when an active (reachable) RADIUS authentication server is detected for users in the critical VLAN.

Use **undo dot1x critical recovery-action** to restore the default.

By default, when a reachable RADIUS server is detected, the system removes the port or 802.1X users from the critical VLAN without triggering authentication.

The **dot1x critical recovery-action** command takes effect only for the 802.1X users in the critical VLAN on a port. It enables the port to take one of the following actions to trigger 802.1X authentication after removing 802.1X users from the critical VLAN on detection of a reachable RADIUS authentication server:

- If MAC-based access control is used, the port sends a unicast Identity EAP/Request to each 802.1X user.
- If port-based access control is used, the port sends a multicast Identity EAP/Request to all the 802.1X users attached to the port.

For prompt detection of active RADIUS authentication servers, use RADIUS server probing function (see *Security Configuration Guide*).

Examples

Configure port GigabitEthernet 1/0/1 to trigger 802.1X re-authentication on detection of an active RADIUS authentication server for users in the critical VLAN.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x critical recovery-action reinitialize
```

dot1x domain-delimiter

Syntax

dot1x domain-delimiter *string*
undo dot1x domain-delimiter

View

System view

Default level

2: System level

Parameters

string: Specifies a set of 1 to 16 domain name delimiters for 802.1X users. No space is required between delimiters. Available delimiters include the at sign (@), backslash (/), and forward slash (\).

Description

Use **dot1x domain-delimiter** to specify a set of domain name delimiters supported by the access device. Any character in the configured set can be used as the domain name delimiter for 802.1X authentication users.

Use **undo dot1x domain-delimiter** to restore the default.

By default, the access device supports only the at sign (@) delimiter for 802.1X users.

The delimiter set you configured overrides the default setting. If @ is not included in the delimiter set, the access device will not support the 802.1X users that use @ as the domain name delimiter.

If a username string contains multiple configured delimiters, the leftmost delimiter is the domain name delimiter. For example, if you configure @, /, and \ as delimiters, the domain name delimiter for the username string 123/22\@abc is the forward slash (/).

The **cut connection user-name** *user-name* and **display connection user-name** *user-name* commands are not available for 802.1X users that use / or \ as the domain name delimiter. For more information about the two commands, see "[AAA configuration commands](#)."

Examples

Specify the characters @, /, and \ as domain name delimiters.

```
<Sysname> system-view
```

```
[Sysname] dot1x domain-delimiter @\/
```

dot1x eapol untag

Syntax

dot1x eapol untag

undo dot1x eapol untag

View

Layer 2 Ethernet interface view

Default level

3: Manage level

Description

Use **dot1x eapol untag** to configure a port to send EAPOL packets untagged.

By default, whether the port sends EAPOL packets with a VLAN tag depends on the VLAN settings on the port.

EAPOL frames exchanged between the 802.1X client and the network access device must not contain VLAN tags. If any 802.1X user attached to a port is assigned a tagged VLAN, you must enable the port to send EAPOL frames untagged.

Examples

Configure GigabitEthernet 1/0/1 to send EAPOL packets untagged.

```
<Sysname> system-view
[Sysname]interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x eapol untag
```

dot1x guest-vlan

Syntax

In system view:

dot1x guest-vlan *guest-vlan-id* [**interface** *interface-list*]

undo dot1x guest-vlan [**interface** *interface-list*]

In Ethernet interface view:

dot1x guest-vlan *guest-vlan-id*

undo dot1x guest-vlan

View

System view, Ethernet interface view

Default level

2: System level

Parameters

guest-vlan-id: Specifies the ID of the VLAN to be specified as the 802.1X guest VLAN, in the range of 1 to 4094. Make sure that the VLAN has been created.

interface *interface-list*: Specifies a port list. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and <1-10> means that you can provide up to 10 ports or port ranges. The start port number must be smaller than the end number and the two ports must be of the same type. If no interface is specified, you configure an 802.1X guest VLAN for all Layer 2 Ethernet ports.

Description

Use **dot1x guest-vlan** to configure an 802.1X guest VLAN for the specified or all ports.

Use **undo dot1x guest-vlan** to remove the 802.1X guest VLAN on the specified or all ports.

By default, no 802.1X guest VLAN is configured on a port.

You must enable 802.1X for an 802.1X guest VLAN to take effect.

To have the 802.1X guest VLAN take effect, complete the following tasks:

- Enable 802.1X both globally and on the interface.
- If the port performs port-based access control, enable the 802.1X multicast trigger function.
- If the port performs MAC-based access control, configure the MAC-based VLAN function on the port.

When you change the access control method from MAC-based to port-based on a port that carries a guest VLAN, the mappings between MAC addresses and the 802.1X guest VLAN are removed. You can use the **display mac-vlan** command to display MAC-to-VLAN mappings.

When you change the access control method from port-based to MAC-based on a port that is in a guest VLAN, the port is removed from the guest VLAN.

To delete a VLAN that has been configured as a guest VLAN, you must remove the guest VLAN configuration first.

Related commands: **dot1x**, **dot1x port-method**, and **dot1x multicast-trigger**; **mac-vlan enable** and **display mac-vlan** (*Layer 2—LAN Switching Command Reference*).

Examples

Specify VLAN 999 as the 802.1X guest VLAN for port GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] dot1x guest-vlan 999 interface gigabitethernet 1/0/1
```

Specify VLAN 10 as the 802.1X guest VLAN for ports GigabitEthernet 1/0/2 to GigabitEthernet 1/0/5.

```
<Sysname> system-view
```

```
[Sysname] dot1x guest-vlan 10 interface gigabitethernet 1/0/2 to gigabitethernet 1/0/5
```

Specify VLAN 7 as the 802.1X guest VLAN for all ports.

```
<Sysname> system-view
```

```
[Sysname] dot1x guest-vlan 7
```

Specify VLAN 3 as the 802.1X guest VLAN for port GigabitEthernet 1/0/7.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/7
```

```
[Sysname-GigabitEthernet1/0/7] dot1x guest-vlan 3
```

dot1x handshake

Syntax

dot1x handshake

undo dot1x handshake

View

Ethernet Interface view

Default level

2: System level

Parameters

None

Description

Use **dot1x handshake** to enable the online user handshake function. The function enables the device to periodically send handshake messages to the client to check whether a user is online.

Use **undo dot1x handshake** to disable the function.

By default, the function is enabled.

HP recommends that you use the iNode client software to guarantee the normal operation of the online user handshake function.

Examples

```
# Enable the online user handshake function.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/4
[Sysname-GigabitEthernet1/0/4] dot1x handshake
```

dot1x handshake secure

Syntax

dot1x handshake secure

undo dot1x handshake secure

View

Ethernet Interface view

Default level

2: System level

Parameters

None

Description

Use **dot1x handshake secure** to enable the online user handshake security function. The function enables the device to prevent users from using illegal client software.

Use **undo dot1x handshake secure** to disable the function.

By default, the function is disabled.

The online user handshake security function is implemented based on the online user handshake function. To bring the security function into effect, make sure the online user handshake function is enabled.

HP recommends you use the iNode client software and IMC server to guarantee the normal operation of the online user handshake security function.

Related commands: **dot1x handshake**.

Examples

```
# Enable the online user handshake security function.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/4
[Sysname-GigabitEthernet1/0/4] dot1x handshake secure
```

dot1x mandatory-domain

Syntax

dot1x mandatory-domain *domain-name*

undo dot1x mandatory-domain

View

Ethernet interface view

Default level

2: System level

Parameters

domain-name: Specifies the ISP domain name, a case-insensitive string of 1 to 24 characters.

Description

Use **dot1x mandatory-domain** to specify a mandatory 802.1X authentication domain on a port.

Use **undo dot1x mandatory-domain** to remove the mandatory authentication domain.

By default, no mandatory authentication domain is specified.

When authenticating an 802.1X user trying to access the port, the system selects an authentication domain in the following order: the mandatory domain, the ISP domain specified in the username, and the default ISP domain.

To display or cut all 802.1X connections in a mandatory domain, use the **display connection domain isp-name** or **cut connection domain isp-name** command. The output from the **display connection** command without any parameters displays domain names input by users at login. For more information about the **display connection** command or the **cut connection** command, see "[AAA configuration commands](#)."

Related commands: **display dot1x**.

Examples

Configure the mandatory authentication domain **my-domain** for 802.1X users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x mandatory-domain my-domain
```

After 802.1X user **usera** passes the authentication, execute the **display connection** command to display the user connection information on GigabitEthernet 1/0/1. For more information about the **display connection** command, see "[AAA configuration commands](#)."

```
[Sysname-GigabitEthernet1/0/1] display connection interface gigabitethernet 1/0/1
Slot: 1
Index=68 ,Username=usera@my-domian
IP=3.3.3.3
IPv6=N/A
MAC=0015-e9a6-7cfe
```

```
Total 1 connection(s) matched on slot 1.
```

```
Total 1 connection(s) matched.
```

dot1x max-user

Syntax

In system view:

dot1x max-user *user-number* [**interface** *interface-list*]

undo dot1x max-user [**interface** *interface-list*]

In Ethernet interface view:

dot1x max-user *user-number*

undo dot1x max-user

View

System view, Ethernet interface view

Default level

2: System level

Parameters

user-number: Specifies the maximum number of concurrent 802.1X users on a port. The value is in the range of 1 to 256.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 ports or port ranges. The start port number must be smaller than the end number and the two ports must be of the same type.

Description

Use **dot1x max-user** to set the maximum number of concurrent 802.1X users on a port.

Use **undo dot1x max-user** to restore the default.

By default, the maximum number of concurrent 802.1X users on a port is 256.

In system view:

- If you do not specify the *interface-list* argument, the command applies to all ports.
- If you specify the *interface-list* argument, the command applies to the specified ports.

In Ethernet interface view, the *interface-list* argument is not available and the command applies to only the Ethernet port.

Related commands: **display dot1x**.

Examples

Set the maximum number of concurrent 802.1X users on port GigabitEthernet 1/0/1 to 32.

```
<Sysname> system-view
[Sysname] dot1x max-user 32 interface gigabitethernet 1/0/1
```

Or

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x max-user 32
```

Configure GigabitEthernet 1/0/2 through GigabitEthernet 1/0/5 each to support a maximum of 32 concurrent 802.1X users.

```
<Sysname> system-view
[Sysname] dot1x max-user 32 interface gigabitethernet 1/0/2 to gigabitethernet 1/0/5
```

dot1x multicast-trigger

Syntax

dot1x multicast-trigger
undo dot1x multicast-trigger

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **dot1x multicast-trigger** to enable the 802.1X multicast trigger function. The device acts as the initiator and periodically multicasts Identify EAP-Request packets out of a port to detect 802.1X clients and trigger authentication.

Use **undo dot1x multicast-trigger** to disable the function.

By default, the multicast trigger function is enabled.

You can use the **dot1x timer tx-period** command to set the interval for sending multicast Identify EAP-Request packets.

Related commands: **display dot1x**.

Examples

```
# Enable the multicast trigger function on GigabitEthernet 1/0/1.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] dot1x multicast-trigger
```

dot1x port-control

Syntax

In system view:

dot1x port-control { authorized-force | auto | unauthorized-force } [interface interface-list]
undo dot1x port-control [interface interface-list]

In Ethernet interface view:

dot1x port-control { authorized-force | auto | unauthorized-force }
undo dot1x port-control

View

System view, Ethernet interface view

Default level

2: System level

Parameters

authorized-force: Places the specified or all ports in the authorized state, enabling users on the ports to access the network without authentication.

auto: Places the specified or all ports initially in the unauthorized state to allow only EAPOL packets to pass, and after a user passes authentication, sets the port in the authorized state to allow access to the network. You can use this option in most scenarios.

unauthorized-force: Places the specified or all ports in the unauthorized state, denying any access requests from users on the ports.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to interface-type interface-number**] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 ports or port ranges. The start port number must be smaller than the end number and the two ports must be of the same type.

Description

Use **dot1x port-control** to set the authorization state for the specified or all ports.

Use **undo dot1x port-control** to restore the default.

The default port authorization state is **auto**.

In system view, if no *interface-list* argument is specified, the command applies to all ports.

Related commands: **display dot1x**.

Examples

Set the authorization state of port GigabitEthernet 1/0/1 to **unauthorized-force**.

```
<Sysname> system-view
```

```
[Sysname] dot1x port-control unauthorized-force interface gigabitethernet 1/0/1
```

Or

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x port-control unauthorized-force
```

Set the authorization state of ports GigabitEthernet 1/0/2 through GigabitEthernet 1/0/5 to **unauthorized-force**.

```
<Sysname> system-view
```

```
[Sysname] dot1x port-control unauthorized-force interface gigabitethernet 1/0/2 to gigabitethernet 1/0/5
```

dot1x port-method

Syntax

In system view:

```
dot1x port-method { macbased | portbased } [ interface interface-list ]
```

```
undo dot1x port-method [ interface interface-list ]
```

In Ethernet interface view:

```
dot1x port-method { macbased | portbased }
```

undo dot1x port-method

View

System view, Ethernet interface view

Default level

2: System level

Parameters

macbased: Uses MAC-based access control on a port to separately authenticate each user attempting to access the network. In this approach, when an authenticated user logs off, no other online users are affected.

portbased: Uses port-based access control on a port. In this approach, once an 802.1X user passes authentication on the port, any subsequent user can access the network through the port without authentication. When the authenticated user logs off, all other users are logged off.

interface interface-list: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to interface-type interface-number**] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 ports or port ranges for this argument. The start port number must be smaller than the end number and the two ports must be the same type.

Description

Use **dot1x port-method** to specify an access control method for the specified or all ports.

Use **undo dot1x port-method** to restore the default.

By default, MAC-based access control applies.

In system view, if no *interface-list* argument is specified, the command applies to all ports.

Related commands: **display dot1x**.

Examples

Configure port GigabitEthernet 1/0/1 to implement port-based access control.

```
<Sysname> system-view
```

```
[Sysname] dot1x port-method portbased interface gigabitethernet 1/0/1
```

Or

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x port-method portbased
```

Configure ports GigabitEthernet 1/0/2 through GigabitEthernet 1/0/5 to implement port-based access control.

```
<Sysname> system-view
```

```
[Sysname] dot1x port-method portbased interface gigabitethernet 1/0/2 to gigabitethernet 1/0/5
```

dot1x quiet-period

Syntax

dot1x quiet-period

undo dot1x quiet-period

View

System view

Default level

2: System level

Parameters

None

Description

Use **dot1x quiet-period** to enable the quiet timer. When a client fails 802.1X authentication, the device must wait a period of time before it can process authentication requests from the client.

Use **undo dot1x quiet-period** to disable the timer.

By default, the quiet timer is disabled.

Related commands: **display dot1x** and **dot1x timer**.

Examples

```
# Enable the quiet timer.  
<Sysname> system-view  
[Sysname] dot1x quiet-period
```

dot1x re-authenticate

Syntax

dot1x re-authenticate

undo dot1x re-authenticate

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **dot1x re-authenticate** to enable the periodic online user re-authentication function.

Use **undo dot1x re-authenticate** to disable the function.

By default, the periodic online user re-authentication function is disabled.

Periodic re-authentication enables the access device to periodically authenticate online 802.1X users on a port. This function tracks the connection status of online users and updates the authorization attributes assigned by the server, such as the ACL, VLAN, and user profile-based QoS.

You can use the **dot1x timer reauth-period** command to configure the interval for re-authentication.

Related commands: **dot1x timer reauth-period**.

Examples

Enable the 802.1X periodic online user re-authentication function on GigabitEthernet 1/0/1 and set the periodic re-authentication interval to 1800 seconds.

```
<Sysname> system-view
[Sysname] dot1x timer reauth-period 1800
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x re-authenticate
```

dot1x retry

Syntax

dot1x retry *max-retry-value*
undo dot1x retry

View

System view

Default level

2: System level

Parameters

max-retry-value: Specifies the maximum number of attempts for sending an authentication request to a client, in the range of 1 to 10.

Description

Use **dot1x retry** to set the maximum number of attempts for sending an authentication request to a client.

Use **undo dot1x retry** to restore the default.

By default, the maximum number of attempts that the device can send an authentication request to a client is twice.

After the network access device sends an authentication request to a client, if the device receives no response from the client within the username request timeout timer (set with the **dot1x timer tx-period tx-period-value** command) or the client timeout timer (set with the **dot1x timer supp-timeout supp-timeout-value** command), the device retransmits the authentication request. The network access device stops retransmitting the request, if it has made the maximum number of request transmission attempts but still received no response.

This command applies to all ports of the device.

Related commands: **display dot1x**.

Examples

Set the maximum number of attempts for sending an authentication request to a client as 9.

```
<Sysname> system-view
[Sysname] dot1x retry 9
```

dot1x timer

Syntax

```
dot1x timer { handshake-period handshake-period-value | quiet-period quiet-period-value |  
reauth-period reauth-period-value | server-timeout server-timeout-value | supp-timeout  
supp-timeout-value | tx-period tx-period-value }  
  
undo dot1x timer { handshake-period | quiet-period | reauth-period | server-timeout | supp-timeout  
| tx-period }
```

View

System view

Default level

2: System level

Parameters

handshake-period-value: Sets the handshake timer in seconds, in the range of 5 to 1024.

quiet-period-value: Sets the quiet timer in seconds, in the range of 10 to 120.

reauth-period-value: Sets the periodic re-authentication timer in seconds, in the range of 60 to 7200.

server-timeout-value: Sets the server timeout timer in seconds, in the range of 100 to 300.

supp-timeout-value: Sets the client timeout timer in seconds, in the range of 1 to 120.

tx-period-value: Sets the username request timeout timer in seconds, in the range of 10 to 120.

Description

Use **dot1x timer** to set 802.1X timers.

Use **undo dot1x timer** to restore the defaults.

By default, the handshake timer is 15 seconds, the quiet timer is 60 seconds, the periodic re-authentication timer is 3600 seconds, the server timeout timer is 100 seconds, the client timeout timer is 30 seconds, and the username request timeout timer is 30 seconds.

You can set the client timeout timer to a high value in a low-performance network, set the quiet timer to a high value in a vulnerable network or a low value for quicker authentication response, or adjust the server timeout timer to adapt to the performance of different authentication servers. In most cases, the default settings are sufficient.

The network device uses the following 802.1X timers:

- Handshake timer (**handshake-period**)—Sets the interval at which the access device sends client handshake requests to check the online status of a client that has passed authentication. If the device receives no response after sending the maximum number of handshake requests, it considers that the client has logged off.
- Quiet timer (**quiet-period**)—Starts when a client fails authentication. The access device must wait the time period before it can process the authentication attempts from the client.
- Periodic re-authentication timer (**reauth-period**)—Sets the interval at which the network device periodically re-authenticates online 802.1X users. To enable periodic online user re-authentication on a port, use the **dot1x re-authenticate** command. The change to the periodic re-authentication timer applies to the users that have been online only after the old timer expires.

- Server timeout timer (**server-timeout**)—Starts when the access device sends a RADIUS Access-Request packet to the authentication server. If no response is received when this timer expires, the access device retransmits the request to the server.
- Client timeout timer (**supp-timeout**)—Starts when the access device sends an EAP-Request/MD5 Challenge packet to a client. If no response is received when this timer expires, the access device retransmits the request to the client.
- Username request timeout timer (**tx-period**)—Starts when the device sends an EAP-Request/Identity packet to a client in response to an authentication request. If the device receives no response before this timer expires, it retransmits the request. The timer also sets the interval at which the network device sends multicast EAP-Request/Identity packets to detect clients that cannot actively request authentication.

Related commands: **display dot1x**.

Examples

```
# Set the server timeout timer to 150 seconds.
<Sysname> system-view
[Sysname] dot1x timer server-timeout 150
```

dot1x unicast-trigger

Syntax

```
dot1x unicast-trigger
undo dot1x unicast-trigger
```

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **dot1x unicast-trigger** to enable the 802.1X unicast trigger function.

Use **undo dot1x unicast-trigger** to disable the function.

By default, the unicast trigger function is disabled.

The unicast trigger function enables the network access device to initiate 802.1X authentication when it receives a data frame from an unknown source MAC address. The device sends a unicast Identity EAP/Request packet to the unknown source MAC address, and retransmits the packet if it has received no response within a period of time (set with the **dot1x timer tx-period** command). This process continues until the maximum number of request attempts (set with the **dot1x retry** command) is reached.

Related commands: **display dot1x**, **dot1x timer tx-period**, and **dot1x retry**.

Examples

```
# Enable the unicast trigger function for interface GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```


[Sysname-GigabitEthernet1/0/1] dot1x unicast-trigger

reset dot1x statistics

Syntax

reset dot1x statistics [**interface** *interface-list*]

View

User view

Default level

2: System level

Parameters

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 ports or port ranges. The start port number must be smaller than the end number and the two ports must be of the same type.

Description

Use **reset dot1x statistics** to clear 802.1X statistics.

If a list of ports is specified, the command clears 802.1X statistics for all the specified ports. If no ports are specified, the command clears all 802.1X statistics.

Related commands: **display dot1x**.

Examples

Clear 802.1X statistics on port GigabitEthernet 1/0/1.

```
<Sysname> reset dot1x statistics interface gigabitethernet 1/0/1
```

vlan-group

Syntax

vlan-group *group-name*

undo vlan-group *group-name*

View

System view

Default level

3: Manage level

Parameters

group-name: Assigns a name to the group, a cast-sensitive string of 1 to 31 characters.

Description

Use **vlan-group** to create a VLAN group and enter its view.

Use **undo vlan-group** to remove the specified VLAN group.

By default, no VLAN group exists.

You can create a maximum of 100 VLAN groups.

Examples

Create a VLAN group named **test** and enter its view.

```
<Sysname> system-view
```

```
[Sysname] vlan-group test
```

vlan-list

Syntax

vlan-list *vlan-list*

undo vlan-list *vlan-list*

View

VLAN group view

Default level

2: System level

Parameters

vlan-list: Specifies a space-separated list of up to 10 VLAN ID items. Each item specifies a VLAN ID or a VLAN ID range in the form of *vlan-id1* **to** *vlan-id2*.

Description

Use **vlan-list** to specify a list of VLANs.

Use **undo vlan-list** to remove the specified VLANs.

Repeat this command to add VLANs to a VLAN group.

You can specify a VLAN that has not been created. This VLAN is automatically created when it is selected for 802.1X users.

You can specify a VLAN to different VLAN groups.

Examples

Specify VLANs 6, 7, and 8 for VLAN group **test**.

```
<Sysname> system-view
```

```
[Sysname] vlan-group test
```

```
[Sysname-vlan-group-test] vlan-list 6 7 8
```

EAD fast deployment configuration commands

dot1x free-ip

Syntax

```
dot1x free-ip ip-address { mask-address | mask-length }  
undo dot1x free-ip { ip-address { mask | mask-length } | all }
```

View

System view

Default level

2: System level

Parameters

ip-address: Specifies a freely accessible IP address segment, also called "a free IP."

mask: Specifies an IP address mask.

mask-length: Specifies IP address mask length.

all: Removes all free IP addresses.

Description

Use **dot1x free-ip** to configure a free IP. Users can access the segment before passing 802.1X authentication.

Use **undo dot1x free-ip** to remove the specified or all free IP addresses.

By default, no free IP is configured.

When global MAC authentication, Layer-2 portal authentication, or port security is enabled, the free IP does not take effect.

Related commands: **display dot1x**.

Examples

```
# Configure 192.168.0.0/24 as a free IP address.  
<Sysname> system-view  
[Sysname] dot1x free-ip 192.168.0.0 24
```

dot1x timer ead-timeout

Syntax

```
dot1x timer ead-timeout ead-timeout-value  
undo dot1x timer ead-timeout
```

View

System view

Default level

2: System level

Parameters

ead-timeout-value: Specifies the EAD rule timer in minutes, in the range of 1 to 1440.

Description

Use **dot1x timer ead-timeout** to set the EAD rule timer.

Use **undo dot1x timer ead-timeout** to restore the default.

By default, the timer is 30 minutes.

EAD fast deployment automatically creates an ACL rule, or EAD rule, to open access to the redirect URL for each redirected user seeking to access the network. The EAD rule timer sets the lifetime of each ACL rule. When the timer expires or the user passes authentication, the rule is removed. If users fail to download EAD client or pass authentication before the timer expires, they must reconnect to the network to access the free IP.

To prevent ACL rule resources from being used up, you can shorten the timer when the amount of EAD users is large.

Related commands: **display dot1x**.

Examples

Set the EAD rule timer to 5 minutes.

```
<Sysname> system-view
```

```
[Sysname] dot1x timer ead-timeout 5
```

dot1x url

Syntax

dot1x url *url-string*

undo dot1x url

View

System view

Default level

2: System level

Parameters

url-string: Specifies the redirect URL, a case-sensitive string of 1 to 64 characters in the format `http://string`.

Description

Use **dot1x url** to configure a redirect URL. When a user uses a web browser to access networks other than the free IP, the device redirects the user to the redirect URL.

Use **undo dot1x url** to remove the redirect URL.

By default, no redirect URL is defined.

The redirect URL must be on the free IP subnet.

If you configure the **dot1x url** command multiple times, the last configured URL takes effect.

Related commands: **display dot1x** and **dot1x free-ip**.

Examples

Configure the redirect URL as http://192.168.0.1.

```
<Sysname> system-view
```

```
[Sysname] dot1x url http://192.168.0.1
```

MAC authentication configuration commands

display mac-authentication

Syntax

display mac-authentication [**interface** *interface-list*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

interface *interface-list*: Specifies a port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. The start port and end port of a port range must be of the same type and the end port number must be greater than the start port number. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display mac-authentication** to display MAC authentication settings and statistics, including the global settings, and port-specific settings and MAC authentication and online user statistics.

If you specify a list of ports, the command displays port-specific settings and statistics only for the specified ports.

If you do not specify any port, the command displays port-specific settings and statistics for all ports.

Examples

Display all MAC authentication settings and statistics.

```
<Sysname> display mac-authentication
```

```
MAC address authentication is enabled.
```

```
User name format is MAC address in lowercase, like xxxxxxxxxxxxxx
```

```
Fixed username:mac
```

```
Fixed password:not configured
```

```
    Offline detect period is 300s
```

```
    Quiet period is 60s.
```

```
    Server response timeout value is 100s
```

```
    the max allowed user number is 1024 per slot
```

```

Current user number amounts to 0
Current domain: not configured, use default domain

```

Silent Mac User info:

```

          MAC Addr          From Port          Port Index
GigabitEthernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 0, failed: 0
  Max number of on-line users is 256
  Current online user number is 0
MAC Addr          Authenticate state          AuthIndex
...

```

Table 11 Command output

Field	Description
MAC address authentication is enabled	Whether MAC authentication is enabled.
User name format is MAC address in lowercase, like xxxxxxxxxxxx	Type of user account, which can be MAC-based or shared. <ul style="list-style-type: none"> If MAC-based accounts are used, this field displays "User name format is MAC address..." and the format settings for usernames and passwords. For example, MAC addresses without hyphens in lower case. If a shared account is used, this field displays "User name format is fixed account."
Fixed username:	Username of the shared account for MAC authentication users. If MAC-based accounts are used, this field displays mac .
Fixed password:	Password for MAC authentication. <ul style="list-style-type: none"> If MAC-based accounts are used or if a shared account is used but no password is configured, this field displays Not configured. If a shared account is used and a password is configured, this field displays a string of asterisks (*****).
Offline detect period	Setting of the offline detect timer
Quiet period	Setting of the quiet timer
Server response timeout value	Setting of the server timeout timer
the max allowed user number	Maximum number of users each slot supports
Current user number amounts to	Number of online users
Current domain: not configured, use default domain	Authentication domain that is currently used
Silent Mac User info	Information about silent MAC addresses. A MAC address is marked silent when it fails a MAC authentication, and at the same time, a quiet timer starts. Before the timer expires, the device drops any packet from the MAC address and does not perform MAC authentication for the MAC address.
GigabitEthernet1/0/1 is link-up	Status of the link on port GigabitEthernet 1/0/1. In this example, the link is up.

Field	Description
MAC address authentication is enabled	Whether MAC authentication is enabled on port GigabitEthernet 1/0/1.
Authenticate success: 0, failed: 0	MAC authentication statistics, including the number of successful and unsuccessful authentication attempts
Max number of on-line users	Maximum number of concurrent online users allowed on the port. If MAC authentication is not enabled on the port, the field displays 0 .
Current online user number	Number of online users on the port.
MAC Addr	MAC address of the online user.
Authenticate state	User status: <ul style="list-style-type: none"> • MAC_AUTHENTICATOR_CONNECT—The user is logging in. • MAC_AUTHENTICATOR_SUCCESS—The user has passed the authentication. • MAC_AUTHENTICATOR_FAIL—The user failed the authentication. • MAC_AUTHENTICATOR_LOGOFF—The user has logged off.
AuthIndex	Authenticator index.

mac-authentication

Syntax

In system view:

mac-authentication [**interface** *interface-list*]

undo mac-authentication [**interface** *interface-list*]

In Ethernet interface view:

mac-authentication

undo mac-authentication

View

System view, Ethernet interface view

Default level

2: System level

Parameters

interface *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. The start port and end port of a port range must be of the same type and the end port number must be greater than the start port number. A port range defined without the **to interface-type interface-number** portion comprises only one port.

Description

Use **mac-authentication** in system view to enable MAC authentication globally.

Use **mac-authentication interface** *interface-list* in system view to enable MAC authentication on a list of ports, or **mac-authentication** in interface view to enable MAC authentication on a port.

Use **undo mac-authentication** in system view to disable MAC authentication globally.

Use **undo mac-authentication interface** *interface-list* in system view to disable MAC authentication on a list of ports, or **undo mac-authentication** in interface view to disable MAC authentication on a port.

By default, MAC authentication is not enabled globally or on any port.

To use MAC authentication on a port, you must enable the function both globally and on the port.

Examples

Enable MAC authentication globally.

```
<Sysname> system-view
[Sysname] mac-authentication
Mac-auth is enabled globally.
```

Enable MAC authentication on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] mac-authentication interface GigabitEthernet 1/0/1
Mac-auth is enabled on port GigabitEthernet1/0/1.
```

Or

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication
Mac-auth is enabled on port GigabitEthernet1/0/1.
```

mac-authentication critical vlan

Syntax

mac-authentication critical vlan *critical-vlan-id*

undo mac-authentication critical vlan

View

Layer 2 Ethernet port view

Default level

2: System level

Parameters

critical-vlan-id: Specifies a VLAN ID, in the range of 1 to 4094. Make sure the VLAN has been created.

Description

Use **mac-authentication critical vlan** to configure a MAC authentication critical VLAN on a port for MAC authentication users that have failed authentication because all the RADIUS authentication servers in their ISP domain are unreachable.

Use **undo mac-authentication critical vlan** to restore the default.

By default, no MAC authentication critical VLAN is configured on a port.

The MAC authentication critical VLAN configuration applies to MAC authentication users that use only RADIUS authentication servers and have failed authentication because all the servers in their ISP domain

become unavailable (inactive), for example, for the loss of network connectivity. If a MAC authentication user fails local authentication after RADIUS authentication, the user is not assigned to the critical VLAN.

You can configure only one MAC authentication critical VLAN on a port. The MAC authentication critical VLANs on different ports can be different.

To have the MAC authentication critical VLAN take effect on a port, complete the following tasks:

- Enable MAC authentication both globally and on the port.
- Enable MAC-based VLAN on the port.

To delete a VLAN that has been configured as a MAC authentication critical VLAN, you must remove the MAC authentication critical VLAN configuration first.

Related commands: **mac-authentication** and **mac-vlan enable** (*Layer 2—LAN Switching Command Reference*).

Examples

Specify VLAN 5 as the MAC authentication critical VLAN for port GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mac-authentication critical vlan 5
```

mac-authentication domain

Syntax

mac-authentication domain *domain-name*

undo mac-authentication domain

View

System view, Ethernet interface view

Default level

2: System level

Parameters

domain-name: Specifies an authentication domain name, a case-insensitive string of 1 to 24 characters. The domain name cannot contain any forward slash (/), colon (:), asterisk (*), question mark (?), less-than sign (<), greater-than sign (>), or at sign (@).

Description

Use **mac-authentication domain** to specify a global authentication domain in system view or a port specific authentication domain in interface view for MAC authentication users.

Use **undo mac-authentication domain** to restore the default.

By default, the default authentication domain is used for MAC authentication users. For more information about the default authentication domain, see the **domain default enable** command in "AAA configuration commands."

The global authentication domain is applicable to all MAC authentication enabled ports. A port specific authentication domain is applicable only to the port. You can specify different authentication domains on different ports.

A port chooses an authentication domain for MAC authentication users in this order: port specific domain, global domain, and the default authentication domain.

Related commands: **display mac-authentication**.

Examples

Specify the **domain1** domain as the global authentication domain for MAC authentication users.

```
<Sysname> system-view
```

```
[Sysname] mac-authentication domain domain1
```

Specify the **aabbcc** domain as the authentication domain for MAC authentication users on port GigabitEthernet 1/0/1.

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mac-authentication domain aabbcc
```

mac-authentication guest-vlan

Syntax

mac-authentication guest-vlan *guest-vlan-id*

undo mac-authentication guest-vlan

View

Ethernet interface view

Default level

2: System level

Parameters

guest-vlan-id: Specifies a VLAN as the MAC authentication guest VLAN. The value range is from 1 to 4094. Make sure that the VLAN has been created.

Description

Use **mac-authentication guest-vlan** to specify a MAC authentication guest VLAN on a port. Any users that have failed MAC authentication on the port is assigned to this VLAN, so they can access a limited set of network resources, such as a software server, to download anti-virus software, and system patches. After a user in the guest VLAN passes MAC authentication, it is removed from the guest VLAN and can access all authorized network resources.

Use **undo mac-authentication guest-vlan** to remove the MAC authentication guest VLAN from the port. By default, no MAC authentication guest VLAN is configured on a port.

To use the MAC authentication guest VLAN function on a port, you must enable MAC-based VLAN on the port, in addition to enabling MAC authentication both globally and on the port.

To delete a VLAN that has been set as a MAC authentication guest VLAN, remove the guest VLAN configuration first.

Related commands: **mac-authentication** and **mac-vlan enable** (*Layer 2—LAN Switching Command Reference*).

Examples

Configure VLAN 5 as the MAC authentication guest VLAN on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan 5
```

mac-authentication max-user

Syntax

mac-authentication max-user *user-number*

undo mac-authentication max-user

View

Ethernet interface view

Default level

2: System level

Parameters

user-number: Specifies a maximum number of concurrent MAC authentication users on the port. The value is in the range of 1 to 256.

Parameters

Use **mac-authentication max-user** to set the maximum number of concurrent MAC authentication users on a port.

Use **undo mac-authentication max-user** to restore the default.

By default, maximum number of concurrent MAC authentication users on a port is 256.

Examples

Configure port GigabitEthernet 1/0/1 to support up to 32 concurrent MAC authentication users.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication max-user 32
```

mac-authentication timer

Syntax

mac-authentication timer { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }

undo mac-authentication timer { **offline-detect** | **quiet** | **server-timeout** }

View

System view

Default level

2: System level

Parameters

offline-detect *offline-detect-value*: Sets the offline detect timer, in the range of 60 to 2147483647 seconds. This timer sets the interval that the device waits for traffic from a user before it regards the user idle. If a user connection has been idle for two consecutive intervals, the device logs the user out and stops accounting for the user.

quiet *quiet-value*: Sets the quiet timer, in the range of 1 to 3600 seconds. This timer sets the interval that the device must wait before it can perform MAC authentication for a user that has failed MAC authentication. All packets from the MAC address are dropped during the quiet time. This quiet mechanism prevents repeated authentication from affecting system performance.

server-timeout *server-timeout-value*: Sets the server timeout timer in seconds, in the range of 100 to 300. This timer sets the interval that the access device waits for a response from a RADIUS server before it regards the RADIUS server unavailable. If the timer expires during MAC authentication, the user cannot access the network.

Description

Use **mac-authentication timer** to set the MAC authentication timers.

Use **undo mac-authentication timer** to restore the defaults.

By default, the offline detect timer is 300 seconds, the quiet timer is 60 seconds, and the server timeout timer is 100 seconds.

Related commands: **display mac-authentication**.

Examples

```
# Set the server timeout timer to 150 seconds.
<Sysname> system-view
[Sysname] mac-authentication timer server-timeout 150
```

mac-authentication timer auth-delay

Syntax

mac-authentication timer auth-delay *time*
undo mac-authentication timer auth-delay

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

time: Specifies the MAC authentication delay time, in the range of 1 to 180, in seconds.

Description

Use **mac-authentication timer auth-delay** to enable MAC authentication delay and set the delay time.

Use **undo mac-authentication timer auth-delay** to restore the default.

By default, MAC authentication is not delayed.

Examples

```
# Enable MAC authentication delay on GigabitEthernet 1/0/1, and set the delay time to 30 seconds.
<Sysname> system-view
[Sysname] interface gigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication timer auth-delay 30
```

mac-authentication user-name-format

Syntax

```
mac-authentication user-name-format { fixed [ account name ] [ password { cipher | simple } password ]  
| mac-address [ { with-hyphen | without-hyphen } [ lowercase | uppercase ] ] }
```

```
undo mac-authentication user-name-format
```

View

System view

Default level

2: System level

Parameters

fixed: Uses a shared account for all MAC authentication users.

account *name*: Specifies the username for the shared account. The name takes a case-insensitive string of 1 to 55 characters. If no username is specified, the default name **mac** applies.

password: Specifies the password for the shared user account.

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies the password. This argument is case sensitive. If **simple** is specified, the password must be a string of 1 to 63 characters. If **cipher** is specified, the password must be a ciphertext string of 1 to 117 characters.

mac-address: Uses MAC-based user accounts for MAC authentication users. If this option is specified, you must create one user account for each user, and use the MAC address of the user as both the username and password for the account. You can also specify the format of username and password:

- **with-hyphen**—Hyphenates the MAC address, for example xx-xx-xx-xx-xx-xx.
- **without-hyphen**—Excludes hyphens from the MAC address, for example, xxxxxxxxxxxx.
- **lowercase**—Enters letters in lower case.
- **uppercase**—Capitalizes letters.

Description

Use **mac-authentication user-name-format** to configure the type of user accounts for MAC authentication users.

Use **undo mac-authentication user-name-format** to restore the default.

By default, each user's MAC address is used as the username and password for MAC authentication, and letters must be input in lower case without hyphens.

MAC authentication supports the following types of user account:

- One MAC-based user account for each user. A user can pass MAC authentication only when its MAC address matches a MAC-based user account. This approach is suitable for an insecure environment.
- One shared user account for all users. Any user can pass MAC authentication on any MAC authentication enabled port. You can use this approach in a secure environment to limit network resources accessible to MAC authentication users, for example, by assigning an authorized ACL or VLAN for the shared account.

The configuration file saves the password for a shared user account in cipher text, regardless of whether it is specified in cipher text or plain text.

Related commands: **display mac-authentication**.

Examples

Configure a shared account for MAC authentication users: set the username as **abc** and password as **xyz** in plain text.

```
<Sysname> system-view
```

```
[Sysname] mac-authentication user-name-format fixed account abc password simple xyz
```

Use MAC-based user accounts for MAC authentication users, and each MAC address must be hyphenated, and in upper case.

```
<Sysname> system-view
```

```
[Sysname] mac-authentication user-name-format mac-address with-hyphen uppercase
```

reset mac-authentication statistics

Syntax

reset mac-authentication statistics [**interface** *interface-list*]

View

User view

Default level

2: System level

Parameters

interface *interface-list*: Specifies a port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. The start port and end port of a port range must be of the same type and the end port number must be greater than the start port number. A port range defined without the **to interface-type interface-number** portion comprises only one port.

Description

Use **reset mac-authentication statistics** to clear MAC authentication statistics.

If no port list is specified, the command clears all global and port-specific MAC authentication statistics. If a port list is specified, the command clears the MAC authentication statistics on the specified ports.

Related commands: **display mac-authentication**.

Examples

Clear MAC authentication statistics on port GigabitEthernet 1/0/1.

```
<Sysname> reset mac-authentication statistics interface gigabitethernet 1/0/1
```

Portal configuration commands

display portal free-rule

Syntax

display portal free-rule [*rule-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

rule-number: Specifies the number of a portal-free rule. The value range is from 0 to 255.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display portal free-rule** to display information about a specified portal-free rule or all portal-free rules.

Related commands: **portal free-rule**.

Examples

Display information about portal-free rule 1.

```
<Sysname> display portal free-rule 1
```

```
Rule-Number 1:
```

```
Source:
```

```
IP          : 2.2.2.0
```

```
Mask        : 255.255.255.0
```

```
MAC         : 0000-0000-0000
```

```
Interface   : any
```

```
Vlan        : 0
```

```
Destination:
```

```
IP          : 0.0.0.0
```

```
Mask        : 0.0.0.0
```

Table 12 Command output

Field	Description
Rule-Number	Number of the portal-free rule

Field	Description
Source	Source information in the portal-free rule
IP	Source IP address in the portal-free rule
Mask	Subnet mask of the source IP address in the portal-free rule
MAC	Source MAC address in the portal-free rule
Interface	Source interface in the portal-free rule
Vlan	Source VLAN in the portal-free rule
Destination	Destination information in the portal-free rule
IP	Destination IP address in the portal-free rule
Mask	Subnet mask of the destination IP address in the portal-free rule

display portal interface

Syntax

display portal interface *interface-type interface-number* [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display portal interface** to display the portal configuration of an interface.

Examples

```
# Display the portal configuration of GigabitEthernet1/0/1.
<Sysname> display portal interface gigabitethernet1/0/1
  Interface portal configuration:
  GigabitEthernet1/0/1: Portal running
  Portal server: servername
  Authentication type: Direct
  Authentication domain: my-domain
  Authentication network:
```

source address : 0.0.0.0 mask : 0.0.0.0
destination address : 2.2.2.0. mask : 255.255.255.0

Table 13 Command output

Field	Description
Interface portal configuration	Portal configuration on the interface
GigabitEthernet1/0/1	Status of the portal authentication on the interface: <ul style="list-style-type: none">• disabled—Portal authentication is disabled.• enabled—Portal authentication is enabled but is not functioning.• running—Portal authentication is functioning.
Portal server	Portal server referenced by the interface
Authentication type	Authentication mode enabled on the interface
Authentication domain	Mandatory authentication domain of the interface
Authentication network	Information of the portal authentication source subnet and destination subnet.
address	IP address of the portal authentication subnet
mask	Subnet mask of the IP address of the portal authentication subnet

display portal local-server

Syntax

display portal local-server [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

| : Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display portal local-server** to display configuration information about the local portal server, including the supported protocol type, and the referenced SSL server policy.

Related commands: **portal local-server** and **portal local-server bind**.

Examples

```
# Display configuration information about the local portal server.  
<Sysname> display portal local-server
```

```
Protocol:
Local-server IP: 255.255.255.255
Server policy:
```

Table 14 Command output

Field	Description
Protocol	Protocol supported by the local portal server, HTTP or HTTPS.
Server policy	SSL server policy associated with the HTTPS service. If HTTP is configured, this field is empty.

display portal tcp-cheat statistics

Syntax

```
display portal tcp-cheat statistics [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display portal tcp-cheat statistics** to display TCP spoofing statistics.

Examples

```
# Display TCP spoofing statistics.
<Sysname> display portal tcp-cheat statistics
TCP Cheat Statistic:
Total Opens: 0
Resets Connections: 0
Current Opens: 0
Packets Received: 0
Packets Sent: 0
Packets Retransmitted: 0
Packets Dropped: 0
HTTP Packets Sent: 0
Connection State:
    SYN_RECVD: 0
    ESTABLISHED: 0
```

```

CLOSE_WAIT: 0
LAST_ACK: 0
FIN_WAIT_1: 0
FIN_WAIT_2: 0
CLOSING: 0

```

Table 15 Command output

Field	Description
TCP Cheat Statistic	TCP spoofing statistics
Total Opens	Total number of opened connections
Resets Connections	Number of connections reset through RST packets
Current Opens	Number of connections being set up
Packets Received	Number of received packets
Packets Sent	Number of sent packets
Packets Retransmitted	Number of retransmitted packets
Packets Dropped	Number of dropped packets
HTTP Packets Sent	Number of HTTP packets sent
Connection State	Statistics of connections in various states
ESTABLISHED	Number of connections in ESTABLISHED state
CLOSE_WAIT	Number of connections in CLOSE_WAIT state
LAST_ACK	Number of connections in LAST-ACK state
FIN_WAIT_1	Number of connections in FIN_WAIT_1 state
FIN_WAIT_2	Number of connections in FIN_WAIT_2 state
CLOSING	Number of connections in CLOSING state

display portal user

Syntax

display portal user { **all** | **interface** *interface-type interface-number* } [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Specifies all interfaces.

interface *interface-type interface-number*: Specifies an interface by its type and name.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display portal user** to display information about portal users on a specified interface or all interfaces.

Examples

Display information about portal users on all interfaces.

```
<Sysname> display portal user all
```

```
Index:2
```

```
State:ONLINE
```

```
SubState:NONE
```

```
ACL:NONE
```

```
Work-mode:Stand-alone
```

MAC	IP	Vlan	Interface
-----	----	------	-----------

000d-88f8-0eab	2.2.2.2	1	GigabitEthernet1/0/1
----------------	---------	---	----------------------

Total 1 user(s) matched, 1 listed.

Table 16 Command output

Field	Description
Index	Index of the portal user
State	Current status of the portal user
SubState	Current sub-status of the portal user
ACL	Authorization ACL of the portal user
Work-mode	User's working mode
MAC	MAC address of the portal user
IP	IP address of the portal user
Vlan	VLAN to which the portal user belongs
Interface	Interface to which the portal user is attached
Total 1 user(s) matched, 1 listed	Total number of portal users

portal auth-fail vlan

Syntax

portal auth-fail vlan *authfail-vlan-id*

undo portal auth-fail vlan

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

authfail-vlan-id: Specifies the Auth-Fail VLAN ID. After an Auth-Fail VLAN is specified, a client failing portal authentication will be added to the Auth-Fail VLAN.

Description

Use **portal auth-fail vlan** to specify an Auth-Fail VLAN for portal authentication on the current port.

Use **undo portal auth-fail vlan** to restore the default setting.

By default, no Auth-Fail VLAN is specified for portal authentication on a port.

The specified VLAN must exist.

To make the Auth-Fail VLAN take effect, you need to enable the MAC VLAN function on the port.

You can specify different Auth-Fail VLANs for portal authentication on different ports. A port can be specified with only one Auth-Fail VLAN for portal authentication.

Examples

Configure VLAN 5 as the Auth-VLAN of portal authentication on port GigabitEthernet 1/0/1, so that the port will add users failing portal authentication to this VLAN.

```
<Sysname> system-view
[Sysname] vlan 5
[Sysname-vlan5] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] mac-vlan enable
[Sysname-GigabitEthernet1/0/1] portal auth-fail vlan 5
```

portal delete-user

Syntax

portal delete-user { *ip-address* | **all** | **interface** *interface-type interface-number* }

View

System view

Default level

2: System level

Parameters

ip-address: Logs off the user with the specified IP address.

all: Logs off all users.

interface *interface-type interface-number*: Logs off all users on the specified interface.

Description

Use **portal delete-user** to log off portal users.

Related commands: **display portal user**.

Examples

Log out the portal user whose IP address is 1.1.1.1.

```
<Sysname> system-view
[Sysname] portal delete-user 1.1.1.1
```

portal domain

Syntax

portal domain *domain-name*

undo portal domain

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

domain-name: Specifies the ISP domain name, a case-insensitive string of 1 to 24 characters. The domain specified by this argument must already exist.

Description

Use **portal domain** to specify an authentication domain for an interface. Then, the device will use the authentication domain for authentication, authorization and accounting (AAA) of the portal users on the interface.

Use **undo portal domain** to restore the default.

By default, no authentication domain is specified for portal users on an interface.

Related commands: **display portal interface**.

Examples

Configure the authentication domain to be used for IPv4 portal users on port GigabitEthernet 1/0/1 as **my-domain**.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] portal domain my-domain
```

portal free-rule

Syntax

portal free-rule *rule-number* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *netmask* } | **any** } } | **source** **any** }*

undo portal free-rule { *rule-number* | **all** }

View

System view

Default level

2: System level

Parameters

rule-number: Specifies a number for the portal-free rule, in the range 0 to 255.

any: Imposes no limitation on the previous keyword.

ip *ip-address*: Specifies an IP address.

mask { *mask-length* | *netmask* }: Specifies the mask of the IP address, which can be in dotted decimal notation or an integer in the range of 0 to 32.

all: Specifies all portal-free rules.

Description

Use **portal free-rule** to configure a portal-free rule and specify the source filtering condition, destination filtering condition, or both.

Use **undo portal free-rule** to remove a specified portal-free rule or all portal-free rules.

You cannot configure a portal-free rule to have the same filtering criteria as that of an existing one. When attempted, the system prompts that the rule already exists.

You can only add or remove a portal-free rule. You cannot modify it.

For Layer 2 portal authentication, you can configure only portal-free rules that are from any source address to any or a specific destination address. With such a portal-free rule configured, users can access the specified address without portal authentication.

Related commands: **display portal free-rule**.

Examples

```
# Configure a portal-free rule, allowing packets destined for 10.10.10.1/24 to bypass portal authentication.
```

```
<Sysname> system-view
```

```
[Sysname] portal free-rule 16 destination ip 10.10.10.1 mask 24 source any
```

portal local-server

Syntax

```
portal local-server { http | https server-policy policy-name }
```

```
undo portal local-server { http | https }
```

View

System view

Default level

2: System level

Parameters

http: Specifies that the local portal server use HTTP to exchange authentication packets with clients.

https: Specifies that the local portal server use HTTPS to exchange authentication packets with clients.

server-policy *policy-name*: Specifies the SSL server policy to be associated with the HTTPS service. *policy-name* indicates an SSL server policy name, a case-insensitive string of 1 to 16 characters.

Description

Use **portal local-server** to configure the protocol type to be supported by the local portal server and load the default authentication page file.

Use **undo portal local-server** to cancel the configuration.

By default, the local portal server does not support any protocol type.

When executing this command, the local portal server will load the default authentication page file, which is supposed to be saved in the root directory of the device. To ensure that the local portal server uses the user-defined default authentication pages, edit and save them properly before executing this command. Otherwise, the system default authentication pages will be used.

If you specify HTTP in this command, the redirection URL for HTTP packets is in the format of `http://IP address of the device/portal/logon.htm`, and clients and the portal server exchange authentication information through HTTP.

If you specify HTTPS in this command, the redirection URL for HTTP packets is in the format of `https://IP address of the device/portal/logon.htm`, and clients and the portal server exchange authentication information through HTTPS.

You cannot remove an SSL server policy using the **undo ssl server-policy** command if the policy has been referenced by the HTTPS service.

On the device, all the SSL server policies referenced by the HTTPS service must be the same.

If an online portal user exists on the device, you cannot remove or change the configured protocol type, or modify the SSL server policies referenced.

To change the SSL server policy referenced by HTTPS service, you must cancel the HTTPS configuration using the **undo portal local-server https** command, and then specify the desired SSL server policy.

Related commands: **display portal local-server** and **ssl server-policy**.

Examples

Configure the local portal server to support HTTP.

```
<Sysname> system-view
```

```
[Sysname] portal local-server http
```

Configure the local portal server to support HTTPS and reference SSL server policy **policy1**, which has been configured already.

```
<Sysname> system-view
```

```
[Sysname] portal local-server https server-policy policy1
```

Change the referenced SSL server policy to **policy2**.

```
[Sysname] undo portal local-server https
```

```
[Sysname] portal local-server https server-policy policy2
```

portal local-server enable

Syntax

portal local-server enable

undo portal

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **portal local-server enable** to enable Layer 2 portal authentication on the current port.

Use **undo portal** to restore the default.

By default, portal authentication is disabled on a Layer 2 port.

For normal operation of portal authentication on a Layer 2 port, HP recommends disabling port security, guest VLAN of 802.1X, and EAD fast deployment of 802.1X on the port. For information about port security and 802.1X features, see *Security Configuration Guide*.

Before enabling portal authentication on a Layer 2 port, be sure to specify the listening IP address of the local portal server.

Related command: **portal local-server ip**.

Examples

```
# Enable Layer 2 portal authentication on GigabitEthernet1/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] portal local-server enable
```

portal local-server ip

Syntax

portal local-server ip *ip-address*

undo portal local-server ip

View

System view

Default level

2: System level

Parameters

ip-address: Specifies the listening IP address of the local portal server. This IP address is that of a Layer 3 interface on the access device and can reach the portal client.

Description

Use **portal local-server ip** to specify the listening IP address of the local portal server for Layer 2 portal authentication. With a listening IP address specified, the device will redirect Web requests from portal clients to the authentication page at the listening IP address.

Use **undo portal local-server ip** to restore the default.

By default, no listening IP address is specified for the local portal server.

HP recommends configuring a loopback interface's address as the listening IP address because:

- The status of a loopback interface is stable. This can avoid authentication page access failures caused by interface failures.
- A loopback interface does not forward received packets. This can avoid impacting system performance when there are many network access requests.

Examples

```
# Specify 1.1.1.1 as the listening IP address of the local portal server for Layer 2 portal authentication.
```

```
<Sysname> system-view
[Sysname] interface loopback 1
[Sysname-LoopBack1] ip address 1.1.1.1 32
[Sysname-LoopBack1] quit
[Sysname] portal local-server ip 1.1.1.1
```

portal max-user

Syntax

```
portal max-user max-number
undo portal max-user
```

View

System view

Default level

2: System level

Parameters

max-number: Specifies the maximum number of online portal users allowed in the system. The value is in the range of 1 to 1000.

Description

Use **portal max-user** to set the maximum number of online portal users allowed in the system.

Use **undo portal max-user** to restore the default.

By default, the maximum number of portal users allowed on the switch is 1000.

If the maximum number of portal users specified in the command is less than that of the current online portal users, the command can be executed successfully and will not impact the online portal users, but the system will not allow new portal users to log in until the number drops down below the limit.

Examples

```
# Set the maximum number of portal users allowed in the system to 100.
```

```
<Sysname> system-view
[Sysname] portal max-user 100
```

portal move-mode auto

Syntax

```
portal move-mode auto
undo portal move-mode
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **portal move-mode auto** to enable support for portal user moving. Then, if an authenticated user moves from a port of the device to another port of the device without logging off, the user can continue to access the network (without re-authentication) if the following conditions are satisfied:

- The new port is up.
- The original port and the new port belong to the same VLAN.
- The authorization information of the user, if any, is assigned to the new port successfully.

If any condition is not satisfied, the device re-authenticates the user on the new port.

Use **undo portal move-mode** to disable support for portal user moving.

By default, support for portal user moving is disabled, and if an authenticated user moves from a port of the device to another port of the device without logging off, the user cannot get online when the original port is still up, because the original port is still maintaining the authentication information of the user.

If the original port goes down after a user moves from the port to another port, the authentication information of the user is lost and the user has to be re-authenticated.

Support for portal user moving applies to scenarios where hubs, Layer 2 switches, or APs exist between users and the access devices.

Examples

```
# Enable support for portal user moving.  
<Sysname> system-view  
[Sysname] portal move-mode auto
```

portal offline-detect interval

Syntax

```
portal offline-detect interval offline-detect-interval  
undo portal offline-detect interval
```

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

offline-detect-value: Specifies the online Layer 2 portal user detection interval, in the range of 60 to 65535.

Description

Use **portal offline-detect interval** to set the online Layer 2 portal user detection interval. Then, after a Layer 2 portal user gets online, the device starts a detection timer for the user, and checks whether the user has sent any packet to the device at this interval. If the device receives no packets from the user during two detection intervals or finds that the user's MAC address entry has been aged out, the device considers that the user has gone offline and clears the authentication information of the user.

Use **undo portal offline-detect interval** to restore the default.

By default, the online Layer 2 portal user detection interval is 300 seconds.

This detection interval must be equal to or less than the MAC address entry aging time. Otherwise, many portal users will be considered offline due to aged MAC address entries.

Examples

```
# Set the online Layer 2 portal user detection interval to 3600 seconds on port GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] portal offline-detect interval 3600
```

portal redirect-url

Syntax

```
portal redirect-url url-string [ wait-time period ]
undo portal redirect-url
```

View

System view

Default level

2: System level

Parameters

url-string: Specifies an auto redirection URL for authenticated portal users, a string of 1 to 127 characters. It must start with `http://` or `https://` and must be a fully qualified URL.

wait-time period: Specifies the time that the device must wait before redirecting a user passing portal authentication to the auto redirection URL. It ranges from 1 to 90 and defaults to 5, in seconds.

Description

Use **portal redirect-url** to specify the auto redirection URL for authenticated portal users.

Use **undo portal redirect-url** to restore the default.

By default, a user authenticated is redirected to the URL the user typed in the address bar before portal authentication.

The **wait-time period** option is effective to only local portal authentication.

If a Layer 2 portal user is to be assigned a VLAN after passing portal authentication, the user may need to update the IP address after getting online. In this case, the redirection wait time must be longer than the user IP address update time. Otherwise, the user may not be able to open the URL because the expected IP address update is not complete yet.

Examples

```
# Configure the device to redirect a portal user to http://www.testpt.cn 3 seconds after the user passes
portal authentication.
<Sysname> system-view
[Sysname] portal redirect-url http://www.testpt.cn wait-time 3
```

portal server banner

Syntax

```
portal server banner banner-string
```

undo portal server banner

View

System view

Default level

2: System level

Parameters

banner-string: Specifies a welcome banner for the Web page, a case-sensitive string of 1 to 50 characters. It cannot contain the less-than sign (<) or the and sign (&). If multiple continuous spaces exist in the string, the browser will recognize them as one.

Description

Use **portal server banner** to configure the welcome banner of the default Web page provided by the local portal server.

Use **undo portal server banner** to restore the default.

By default, no Web page welcome banner is configured.

The configured welcome banner is applied to only the default authentication pages, rather than the customized authentication pages.

Examples

Configure the welcome banner of the default Web page provided by the local portal server as **Welcome to Portal Authentication**.

```
<Sysname> system-view
```

```
[Sysname] portal server banner Welcome to Portal Authentication
```

portal web-proxy port

Syntax

portal web-proxy port *port-number*

undo portal web-proxy port { **all** | *port-number* }

View

System view

Default level

2: System level

Parameters

all: Specifies all web proxy server port numbers.

port-number: Specifies the port number used by a web proxy server, in the range of 1 to 65535.

Description

Use **portal web-proxy port** to add the port number of a web proxy server, so that HTTP requests forwarded by the web proxy server trigger portal authentication.

Use **undo portal web-proxy port** to delete one or all web proxy server port numbers.

By default, no web proxy server port number is configured on the device and proxied HTTP requests cannot trigger portal authentication.

Up to four web proxy server port numbers can be added.

If a user's browser uses the Web Proxy Auto-Discovery (WPAD) protocol to discover web proxy servers, you must add the port numbers of the web proxy servers on the device, and configure portal-free rules to allow user packets destined for the IP address of the WPAD server to pass without authentication.

You must add the port numbers of the web proxy servers on the device, and users must make sure their browsers that use a web proxy server do not use the proxy server for the listening IP address of the local portal server. Thus, HTTP packets that the portal user sends to the local portal server are not sent to the web proxy server.

Examples

Add web proxy server port number 8080 on the device, so that users using a web proxy server with the port number can be redirected to the portal authentication page.

```
<Sysname> system-view
[Sysname] portal web-proxy port 8080
```

reset portal tcp-cheat statistics

Syntax

reset portal tcp-cheat statistics

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **reset portal tcp-cheat statistics** to clear TCP spoofing statistics.

Examples

Clear TCP spoofing statistics.

```
<Sysname> reset portal tcp-cheat statistics
```

Port security configuration commands

display port-security

Syntax

display port-security [**interface** *interface-list*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

interface *interface-list*: Specifies Ethernet ports by an Ethernet port list in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> means that you can specify up to 10 ports or port ranges. The starting port and ending port of a port range must be of the same type, and the ending port number must be greater than the starting port number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display port-security** to display port security configuration information, operation information, and statistics for one or more ports.

If the **interface** *interface-list* parameter is not provided, the command displays port security information, operation information, and status about all ports.

Related commands: **port-security enable**, **port-security port-mode**, **port-security ntk-mode**, **port-security intrusion-mode**, **port-security max-mac-count**, **port-security mac-address security**, **port-security authorization ignore**, **port-security oui**, and **port-security trap**.

Examples

Display port security configuration information, operation information, and statistics for all ports.

```
<Sysname> display port-security
Equipment port-security is enabled
AddressLearn trap is enabled
Intrusion trap is enabled
Dot1x logon trap is enabled
Dot1x logoff trap is enabled
Dot1x logfailure trap is enabled
RALM logon trap is enabled
```



```

RALM logoff trap is enabled
RALM logfailure trap is enabled
AutoLearn aging time is 1 minutes
Disableport Timeout: 20s
OUI value:
  Index is 1,  OUI value is 000d1a
  Index is 2,  OUI value is 003c12

GigabitEthernet1/0/1 is link-down
  Port mode is userLoginWithOUI
  NeedToKnow mode is NeedToKnowOnly
  Intrusion Portection mode is DisablePort
  Max MAC address number is 50
  Stored MAC address number is 0
  Authorization is ignored
  Security MAC address learning mode is sticky
  Security MAC address aging type is absolute
GigabitEthernet1/0/2 is link-down
  Port mode is noRestriction
  NeedToKnow mode is disabled
  Intrusion mode is NoAction
  Max MAC address number is not configured
  Stored MAC address number is 0
  Authorization is permitted
  Security MAC address learning mode is sticky
  Security MAC address aging type is absolute

```

Table 17 Command output

Field	Description
Equipment port-security	Whether the port security is enabled or not.
AddressLearn trap	Whether trapping for MAC address learning is enabled or not. If it is enabled, the port sends trap information after it learns a new MAC address.
Intrusion trap	Whether trapping for intrusion protection is enabled or not. If it is enabled, the port sends trap information after it detects illegal packets.
Dot1x logon trap	Whether trapping for 802.1X logon is enabled or not. If it is enabled, the port sends trap information after a user passes 802.1X authentication.
Dot1x logoff trap	Whether trapping for 802.1X logoff is enabled or not. If it is enabled, the port sends trap information after an 802.1X user logs off.
Dot1x logfailure	Whether trapping for 802.1X authentication failure is enabled or not. If it is enabled, the port sends trap information after a user fails 802.1X authentication.
RALM logon trap	Whether trapping for MAC authentication success is enabled or not. If it is enabled, the port sends trap information when a user passes MAC address authentication.
RALM logoff trap	Whether trapping for MAC authenticated user logoff is enabled or not. If it is enabled, traps are sent when a MAC address authenticated user logs off.

Field	Description
RALM logfailure trap	Whether trapping for MAC authentication failure is enabled or not. If it is enabled, the port sends trap information when a user fails MAC address authentication.
AutoLearn aging time	Secure MAC aging timer. The timer applies to sticky or dynamic secure MAC addresses.
Disableport Timeout	Silence timeout period of the port that receives illegal packets, in seconds.
OUI value	List of OUI values allowed
Port mode	Port security mode: <ul style="list-style-type: none"> • noRestrictions • autoLearn • macAddressWithRadius • macAddressElseUserLoginSecure • macAddressElseUserLoginSecureExt • secure • userLogin • userLoginSecure • userLoginSecureExt • macAddressOrUserLoginSecure • macAddressOrUserLoginSecureExt • userLoginWithOUI
NeedToKnow mode	Need to know (NTK) mode: <ul style="list-style-type: none"> • NeedToKnowOnly—Allows only unicast packets with authenticated destination MAC addresses. • NeedToKnowWithBroadcast—Allows only unicast packets and broadcasts with authenticated destination MAC addresses. • NeedToKnowWithMulticast—Allows unicast packets, multicasts and broadcasts with authenticated destination MAC addresses.
Intrusion mode	Intrusion protection action mode: <ul style="list-style-type: none"> • BlockMacAddress—Adds the source MAC address of the illegal packet to the blocked MAC address list. • DisablePort—Shuts down the port that receives illegal packets permanently. • DisablePortTemporarily—Shuts down the port that receives illegal packets for some time. • NoAction—Performs no intrusion protection.
Max MAC address number	Maximum number of MAC addresses that port security allows on the port.
Stored MAC address number	Number of MAC addresses stored
Authorization	Whether the authorization information from the server is ignored or not: <ul style="list-style-type: none"> • permitted—Authorization information from the RADIUS server takes effect. • ignored—Authorization information from the RADIUS server does not take effect.
Security MAC address learning mode	Secure MAC address learning mode: <ul style="list-style-type: none"> • sticky—Learns MAC addresses as sticky MAC addresses. • dynamic—Learns MAC addresses as dynamic secure MAC addresses.

Field	Description
Security MAC address aging type	Secure MAC address aging type: <ul style="list-style-type: none"> absolute—Timer aging inactivity—Inactivity aging

display port-security mac-address block

Syntax

```
display port-security mac-address block [ interface interface-type interface-number ] [ vlan vlan-id ]
[ count ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

2: System level

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

vlan *vlan-id*: Specifies a VLAN by its ID, in the range of 1 to 4094.

count: Displays only the count of the blocked MAC addresses.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display port-security mac-address block** to display information about blocked MAC addresses.

With no keyword or argument specified, the command displays information about all blocked MAC addresses.

Related commands: **port-security intrusion-mode**.

Examples

Display information about all blocked MAC addresses.

```
<Sysname> display port-security mac-address block
MAC ADDR           From Port                               VLAN ID
000f-3d80-0d2d     GigabitEthernet1/0/1          30
```

```
--- On slot 1, 1 mac address(es) found ---
```

```
--- 1 mac address(es) found ---
```

Display the count of all blocked MAC addresses.

```
<Sysname> display port-security mac-address block count
```

```

--- On slot 1, 1 mac address(es) found ---

--- 1 mac address(es) found ---
# Display information about all blocked MAC addresses in VLAN 30.
<Sysname> display port-security mac-address block vlan 30
MAC ADDR          From Port          VLAN ID
000f-3d80-0d2d    GigabitEthernet1/0/1          30

--- On slot 1, 1 mac address(es) found ---

--- 1 mac address(es) found ---
# Display information about all blocked MAC addresses of port GigabitEthernet 1/0/1.
<Sysname> display port-security mac-address block interface gigabitethernet 1/0/1
MAC ADDR          From Port          VLAN ID
000f-3d80-0d2d    GigabitEthernet1/0/1          30

--- On slot 1, 1 mac address(es) found ---

--- 1 mac address(es) found ---
# Display information about all blocked MAC addresses of port GigabitEthernet 1/0/1 in VLAN 30.
<Sysname> display port-security mac-address block interface gigabitethernet 1/0/1 vlan
30
MAC ADDR          From Port          VLAN ID
000f-3d80-0d2d    GigabitEthernet1/0/1          30
--- On slot 1, 1 mac address(es) found ---

--- 1 mac address(es) found ---

```

Table 18 Command output

Field	Description
MAC ADDR	Blocked MAC address
From Port	Port having received frames with the blocked MAC address being the source address
VLAN ID	ID of the VLAN to which the port belongs
On slot x, y mac address(es) found	Number of blocked MAC addresses on IRF member x (IRF devices)
x mac address(es) found	Total number of blocked MAC addresses

display port-security mac-address security

Syntax

```

display port-security mac-address security [ interface interface-type interface-number ] [ vlan vlan-id ]
[ count ] [ [ { begin | exclude | include } regular-expression ]

```

View

Any view

Default level

2: System level

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

vlan *vlan-id*: Specifies a VLAN by its ID, in the range of 1 to 4094.

count: Displays only the count of the secure MAC addresses.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display port-security mac-address security** to display information about secure MAC addresses. Secure MAC addresses are those that are automatically learned by the port in autoLearn mode or configured by the **port-security mac-address security** command.

With no keyword or argument specified, the command displays information about all secure MAC addresses.

Related commands: **port-security mac-address security**.

Examples

Display information about all secure MAC addresses.

```
<Sysname> display port-security mac-address security
MAC ADDR          VLAN ID  STATE          PORT INDEX          AGING TIME(s)
0002-0002-0002    1        Security       GigabitEthernet1/0/1 NOAGED
000d-88f8-0577    1        Security       GigabitEthernet1/0/1 NOAGED
```

```
--- 2 mac address(es) found ---
```

Display only the count of the secure MAC addresses.

```
<Sysname> display port-security mac-address security count
2 mac address(es) found
```

Display information about secure MAC addresses in VLAN 1.

```
<Sysname> display port-security mac-address security vlan 1
MAC ADDR          VLAN ID  STATE          PORT INDEX          AGING TIME(s)
0002-0002-0002    1        Security       GigabitEthernet1/0/1 NOAGED
000d-88f8-0577    1        Security       GigabitEthernet1/0/1 NOAGED
```

```
--- 2 mac address(es) found ---
```

Display information about secure MAC addresses on port GigabitEthernet 1/0/1.

```
<Sysname> display port-security mac-address security interface gigabitethernet 1/0/1
```

```

MAC ADDR          VLAN ID  STATE          PORT INDEX          AGING TIME(s)
000d-88f8-0577    1       Security      GigabitEthernet1/0/1  NOAGED

--- 1 mac address(es) found ---

# Display information about secure MAC addresses of port GigabitEthernet 1/0/1 in VLAN 1.
<Sysname> display port-security mac-address security interface gigabitethernet 1/0/1 vlan
1
MAC ADDR          VLAN ID  STATE          PORT INDEX          AGING TIME(s)
000d-88f8-0577    1       Security      GigabitEthernet1/0/1  NOAGED

--- 1 mac address(es) found ---

```

Table 19 Command output

Field	Description
MAC ADDR	Secure MAC address
VLAN ID	ID of the VLAN to which the port belongs
STATE	Type of the MAC address added. "Security" means it is a secure MAC address.
PORT INDEX	Port to which the secure MAC address belongs
AGING TIME(s)	Period of time before the secure MAC address ages out. "NOAGED" is displayed for secure MAC addresses.
x mac address(es) found	Number of secure MAC addresses stored

port-security authorization ignore

Syntax

port-security authorization ignore

undo port-security authorization ignore

View

Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **port-security authorization ignore** to configure a port to ignore the authorization information from the server (an RADIUS server or the local device).

Use **undo port-security authorization ignore** to restore the default.

By default, a port uses the authorization information from the server.

After a user passes RADIUS or local authentication, the server performs authorization based on the authorization attributes configured for the user's account. For example, it may assign a VLAN.

Related commands: **display port-security**.

Examples

Configure port GigabitEthernet 1/0/1 to ignore the authorization information from the authentication server.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security authorization ignore
```

port-security enable

Syntax

port-security enable
undo port-security enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **port-security enable** to enable port security.

Use **undo port-security enable** to disable port security.

By default, port security is disabled.

You must disable global 802.1X and MAC authentication before you enable port security on a port.

Enabling or disabling port security resets the following security settings to the default:

- 802.1X access control mode is MAC-based, and the port authorization state is auto.
- Port security mode is noRestrictions.

You cannot disable port security when online users are present.

Related commands: **display port-security**, **dot1x**, **dot1x port-method**, **dot1x port-control**, and **mac-authentication**.

Examples

```
# Enable port security.
<Sysname> system-view
[Sysname] port-security enable
```

port-security intrusion-mode

Syntax

port-security intrusion-mode { blockmac | disableport | disableport-temporarily }
undo port-security intrusion-mode

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

blockmac: Adds the source MAC addresses of illegal frames to the blocked MAC address list and discards frames with blocked source MAC addresses. This implements illegal traffic filtering on the port. A blocked MAC address is restored to normal after being blocked for three minutes, which is fixed and cannot be changed. To view the blocked MAC address list, use the **display port-security mac-address block** command.

disableport: Disables the port permanently upon detecting an illegal frame received on the port.

disableport-temporarily: Disables the port for a specific period of time whenever it receives an illegal frame. Use **port-security timer disableport** to set the period.

Description

Use **port-security intrusion-mode** to configure the intrusion protection feature so that the port takes the pre-defined actions when intrusion protection is triggered on the port.

Use **undo port-security intrusion-mode** to restore the default.

By default, intrusion protection is disabled.

To restore the connection of the port, use the **undo shutdown** command.

Related commands: **display port-security**, **display port-security mac-address block**, and **port-security timer disableport**.

Examples

Configure port GigabitEthernet 1/0/1 to block the source MAC addresses of illegal frames after intrusion protection is triggered.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
```

port-security mac-address aging-type inactivity

Syntax

port-security mac-address aging-type inactivity

undo port-security mac-address aging-type inactivity

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **port-security mac-address aging-type inactivity** to enable inactivity aging for secure MAC addresses (sticky or dynamic).

Use **undo port-security mac-address aging-type inactivity** to restore the default.

By default, the inactivity aging function is disabled.

If only an aging timer is configured, the aging timer counts up regardless of whether traffic data has been sent from the sticky MAC address. When you use an aging timer together with the inactivity aging function, the aging timer restarts once traffic data is detected from the sticky MAC address. The inactivity aging function prevents the unauthorized use of a secure MAC address when the authorized user is offline, and removes outdated secure MAC addresses so new secure MAC addresses can be learned.

Related commands: **port-security timer autolearn aging** and **port-security mac-address dynamic**.

Examples

```
# Enable inactivity aging for secure MAC addresses on interface GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] port-security mac-address aging-type inactivity
```

port-security mac-address dynamic

Syntax

port-security mac-address dynamic

undo port-security mac-address dynamic

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

None

Description

Use **port-security mac-address dynamic** to enable the dynamic secure MAC function. This function converts sticky MAC addresses to dynamic, and disables saving them to the configuration file.

Use **undo port-security mac-address dynamic** to restore the default.

By default, sticky MAC addresses can be saved to the configuration file, and once saved, survive a device reboot.

After you execute the **port-security mac-address dynamic** command on a port, you cannot manually configure sticky MAC address, and secure MAC addresses automatically learned by the port in autoLearn mode are also dynamic. All dynamic MAC addresses are lost at reboot. Use this command when you want to clear all sticky MAC addresses after a device reboot.

After you execute the **undo port-security mac-address dynamic** command on a port, all dynamic secure MAC addresses on the port are converted to sticky MAC addresses, and you can manually configure sticky MAC address.

You can display dynamic secure MAC addresses by using the **display port-security mac-address security** command.

Related commands: **display port-security mac-address security** and **mac-address dynamic**.

Examples

Enable the dynamic secure MAC function on interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security mac-address dynamic
```

port-security mac-address security

Syntax

In Layer 2 Ethernet interface view:

port-security mac-address security [**sticky**] *mac-address* **vlan** *vlan-id*

undo port-security mac-address security [**sticky**] *mac-address* **vlan** *vlan-id*

In system view:

port-security mac-address security [**sticky**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

undo port-security mac-address security [[*mac-address* [**interface** *interface-type interface-number*]] **vlan** *vlan-id*]

View

Layer 2 Ethernet interface view, system view

Default level

2: System level

Parameters

sticky: Specifies a sticky MAC address. If you do not provide this keyword, the command configures a static secure MAC address.

mac-address: Secure MAC address, in the H-H-H format.

interface *interface-type interface-number*: Specifies a Layer 2 Ethernet port by its type and number.

vlan *vlan-id*: Specifies the VLAN that has the secure MAC address. The *vlan-id* argument represents the ID of the VLAN in the range of 1 to 4094. Make sure that you have assigned the Layer 2 port to the specified VLAN.

Description

Use **port-security mac-address security** to add a secure MAC address.

Use **undo port-security mac-address security** to remove a secure MAC address.

By default, no secure MAC address entry is configured.

Secure MAC addresses are MAC addresses configured or learned in autoLearn mode. They can survive link down/up events, and once saved, can survive a device reboot. You can bind a MAC address to only one port in a VLAN.

When a port is operating in autoLearn mode, you can add important or frequently used MAC addresses as sticky or static secure MAC addresses to avoid the secure MAC address limit causing authentication failure.

Static secure MAC addresses never age out unless you remove them by using the **undo port-security mac-address security** command, changing the port security mode, or disabling the port security feature.

Sticky MAC addresses can be manually configured or automatically learned in autoLearn mode. Sticky MAC addresses do not age out by default. You can use the **port-security timer autolearn aging** command to set an aging timer for them. When the timer expires, the sticky MAC addresses are removed.

You cannot change the type of a secure address entry that has been added or add two entries that are identical except for their entry type. For example, you cannot add the **port-security mac-address security sticky 1-1-1 vlan 10** entry when a **port-security mac-address security 1-1-1 vlan 10** entry exists. To add the new entry, you must delete the old entry.

To enable port security on a port, use the **port-security enable** command, and to set the port in autoLearn mode, use the **port-security port-mode autolearn** command.

Related commands: **display port-security** and **port-security timer autolearn aging**.

Examples

Enable port security, set port GigabitEthernet 1/0/1 in autoLearn mode, and add a static secure MAC address 0001-0001-0002 in VLAN 10.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
[Sysname-GigabitEthernet1/0/1] port-security port-mode autolearn
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] port-security mac-address security 0001-0001-0002 interface gigabitethernet
1/0/1 vlan 10
```

Enable port security, set port GigabitEthernet 1/0/1 in autoLearn mode, and add a static secure MAC address 0001-0002-0003 in VLAN 4 in interface view.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
[Sysname-GigabitEthernet1/0/1] port-security port-mode autolearn
[Sysname-GigabitEthernet1/0/1] port-security mac-address security 0001-0002-0003 vlan 4
```

port-security max-mac-count

Syntax

port-security max-mac-count *count-value*

undo port-security max-mac-count

View

Ethernet interface view

Default level

2: System level

Parameters

count-value: Specifies the maximum number of MAC addresses that port security allows on the port. The value is in the range of 1 to 1024.

Description

Use **port-security max-mac-count** to set the maximum number of MAC addresses that port security allows on a port.

Use **undo port-security max-mac-count** to restore the default setting.

By default, port security has no limit on the number of MAC addresses on a port.

In autoLearn mode, this command sets the maximum number of secure MAC addresses (both configured and automatically learned) on the port.

In any other mode that enables 802.1X, MAC authentication, or both, this command sets the maximum number of authenticated MAC addresses on the port. The actual maximum number of concurrent users that the port accepts equals this limit or the authentication method's limit on the number of concurrent users, whichever is smaller. For example, in userLoginSecureExt mode, if 802.1X allows less concurrent users than port security's limit on the number of MAC addresses, port security's limit takes effect.

You cannot change port security's limit on the number of MAC addresses when the port is operating in **autoLearn** mode.

Related commands: **display port-security**.

Examples

```
# Set port security's limit on the number of MAC addresses to 100 on port GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
```

port-security ntk-mode

Syntax

```
port-security ntk-mode { ntk-withbroadcasts | ntk-withmulticasts | ntkonly }
undo port-security ntk-mode
```

View

Ethernet interface view

Default level

2: System level

Parameters

ntk-withbroadcasts: Forwards only broadcast frames and unicast frames with authenticated destination MAC addresses.

ntk-withmulticasts: Forwards only broadcast frames, multicast frames, and unicast frames with authenticated destination MAC addresses.

ntkonly: Forwards only unicast frames with authenticated destination MAC addresses.

Description

Use **port-security ntk-mode** to configure the NTK feature.

Use **undo port-security ntk-mode** to restore the default.

By default, NTK is disabled on a port and all frames are allowed to be sent.

The need to know (NTK) feature checks the destination MAC addresses in outbound frames to allow frames to be sent to only devices passing authentication, preventing illegal devices from intercepting network traffic.

Related commands: **display port-security**.

Examples

Set the NTK mode of port GigabitEthernet 1/0/1 to **ntkonly**, allowing the port to forward received packets to only devices passing authentication.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
```

port-security oui

Syntax

port-security oui *oui-value* **index** *index-value*

undo port-security oui index *index-value*

View

System view

Default level

2: System level

Parameters

oui-value: Specifies an organizationally unique identifier (OUI) string, a 48-bit MAC address in the H-H-H format. The system uses only the 24 high-order bits as the OUI value.

index-value: Specifies the OUI index, in the range of 1 to 16.

Description

Use **port-security oui** to configure an OUI value for user authentication. This value is used when the port security mode is userLoginWithOUI.

Use **undo port-security oui** to delete the OUI value with the specified OUI index.

By default, no OUI value is configured.

An OUI, the first 24 binary bits of a MAC address, is assigned by IEEE to uniquely identify a device vendor. Use this command when you configure a device to allow packets from certain wired devices to pass authentication or to allow packets from certain wireless devices to initiate authentication. For example, when a company allows only IP phones of vendor A in the Intranet, use this command to set the OUI of vendor A.

Related commands: **display port-security**.

Examples

```
# Configure an OUI value of 000d2a, setting the index to 4.
<Sysname> system-view
[Sysname] port-security oui 000d-2a10-0033 index 4
```

port-security port-mode

Syntax

```
port-security port-mode { autolearn | mac-authentication | mac-else-userlogin-secure |
mac-else-userlogin-secure-ext | secure | userlogin | userlogin-secure | userlogin-secure-ext |
userlogin-secure-or-mac | userlogin-secure-or-mac-ext | userlogin-withoui }
undo port-security port-mode
```

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

Keyword	Security mode	Description
autolearn	autoLearn	<p>In this mode, a port can learn MAC addresses, and allows frames sourced from learned or configured the MAC addresses to pass. The dynamically learned MAC addresses are secure MAC addresses. You can also configure secure MAC addresses by using the port-security mac-address security command. A secure MAC address never ages out by default. In addition, you can configure MAC addresses manually by using the mac-address dynamic and mac-address static commands for a port in autoLearn mode.</p> <p>When the number of secure MAC addresses reaches the upper limit set by the port-security max-mac-count command, the port changes to secure mode.</p>
mac-authentication	macAddressWithRadius	<p>In this mode, a port performs MAC authentication for users and services multiple users.</p>
mac-else-userlogin-secure	macAddressElseUserLoginSecure	<p>This mode is the combination of the macAddressWithRadius and userLoginSecure modes, with MAC authentication having a higher priority.</p> <ul style="list-style-type: none">• A port in this mode performs MAC authentication 30 seconds after receiving a non-802.1X frame..• Upon receiving an 802.1X frame, the port performs MAC authentication and then, if MAC authentication fails, 802.1X authentication.
mac-else-userlogin-secure-ext	macAddressElseUserLoginSecureExt	<p>Similar to the macAddressElseUserLoginSecure mode except that a port in this mode supports multiple 802.1X and MAC authentication users.</p>

Keyword	Security mode	Description
secure	secure	In this mode, MAC address learning is disabled on the port and you can configure MAC addresses by using the mac-address static and mac-address dynamic commands. The port permits only frames sourced from secure MAC addresses and MAC addresses you manually configured by using the mac-address static and mac-address dynamic commands.
userlogin	userLogin	In this mode, a port performs 802.1X authentication and implements port-based access control. If one 802.1X user passes authentication, all the other 802.1X users of the port can access the network without authentication.
userlogin-secure	userLoginSecure	In this mode, a port performs 802.1X authentication and implements MAC-based access control. It services only one user passing 802.1X authentication.
userlogin-secure-ext	userLoginSecureExt	Similar to the userLoginSecure mode except that this mode supports multiple online 802.1X users.
userlogin-secure-or-mac	macAddressOrUserLoginSecure	This mode is the combination of the userLoginSecure and macAddressWithRadius modes. The port performs MAC authentication 30 seconds after receiving a non-802.1X frame and performs 802.1X authentication upon receiving 802.1X frames.
userlogin-secure-or-mac-ext	macAddressOrUserLoginSecureExt	Similar to the macAddressOrUserLoginSecure mode except that a port in this mode supports multiple 802.1X and MAC authentication users.
userlogin-withoui	userLoginWithOUI	Similar to the userLoginSecure mode. In addition, a port in this mode also permits frames from a user whose MAC address contains a specific OUI (organizationally unique identifier). The port performs 802.1X authentication upon receiving 802.1X frames, and performs OUI check upon receiving non-802.1X frames.

Description

Use **port-security port-mode** to set the port security mode of a port.

Use **undo port-security port-mode** to restore the default.

By default, a port operates in noRestrictions mode, where port security does not take effect.

To change the security mode of a port security enabled port, you must set the port in noRestrictions mode first. When the port has online users, you cannot change port security mode.



IMPORTANT:

If you are configuring the autoLearn mode, first set port security's limit on the number of MAC addresses by using the **port-security max-mac-count** command. You cannot change the setting when the port is operating in autoLearn mode.

When port security is enabled, you cannot manually enable 802.1X or MAC authentication, or change the access control mode or port authorization state. The port security automatically modifies these settings in different security modes.

Related commands: **display port-security**.

Examples

```
# Enable port security and set port GigabitEthernet 1/0/1 in secure mode.
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security port-mode secure

# Change the port security mode of port GigabitEthernet 1/0/1 to userLogin.
[Sysname-GigabitEthernet1/0/1] undo port-security port-mode
[Sysname-GigabitEthernet1/0/1] port-security port-mode userlogin
```

port-security timer autolearn aging

Syntax

```
port-security timer autolearn aging time-value
undo port-security timer autolearn aging
```

View

System view

Default level

2: System level

Parameters

time-value: Sets the aging timer in minutes for secure MAC addresses. The value is in the range of 0 to 129600. To disable the aging timer, set the timer to 0.

Description

Use **port-security timer autolearn aging** to set the secure MAC aging timer. The timer applies to all sticky or dynamic secure MAC addresses.

Use **undo port-security timer autolearn aging** to restore the default.

By default, secure MAC addresses never age out.

Related commands: **display port-security** and **port-security mac-address security**.

Examples

```
# Set the secure MAC aging timer to 30 minutes.
<Sysname> system-view
[Sysname] port-security timer autolearn aging 30
```

port-security timer disableport

Syntax

```
port-security timer disableport time-value
undo port-security timer disableport
```

View

System view

Default level

2: System level

Parameters

time-value: Specifies the silence period during which the port remains disabled, in seconds. It is in the range of 20 to 300.

Description

Use **port-security timer disableport** to set the silence period during which the port remains disabled.

Use **undo port-security timer disableport** to restore the default.

By default, the silence period is 20 seconds.

If you configure the intrusion protection policy as disabling the port temporarily whenever it receives an illegal frame, use this command to set the silence period.

Related commands: **display port-security**.

Examples

Configure the intrusion protection policy as disabling the port temporarily whenever it receives an illegal frame and set the silence period to 30 seconds.

```
<Sysname> system-view
[Sysname] port-security timer disableport 30
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
```

port-security trap

Syntax

```
port-security trap { addresslearned | dot1xlogfailure | dot1xlogoff | dot1xlogon | intrusion |
ralmlogfailure | ralmlogoff | ralmlogon }

undo port-security trap { addresslearned | dot1xlogfailure | dot1xlogoff | dot1xlogon | intrusion |
ralmlogfailure | ralmlogoff | ralmlogon }
```

View

System view

Default level

2: System level

Parameters

addresslearned: Enables MAC address learning traps. The port security module sends traps when a port learns a new MAC address.

dot1xlogfailure: Enables 802.1X authentication failure traps. The port security module sends traps when an 802.1X authentication fails.

dot1xlogon: Enables 802.1X authentication success traps. The port security module sends traps when an 802.1X authentication is passed.

dot1xlogoff: Enables 802.1X user logoff event traps. The port security module sends traps when an 802.1X user is logged off.

intrusion: Enables intrusion traps. The port security module sends traps when it detects illegal frames.

ralmlogfailure: Enables MAC authentication failure traps. The port security module sends traps when a MAC authentication fails.

ralmlogoff: Enables MAC authentication user logoff traps. The port security module sends traps when a MAC authentication user is logged off.

ralmlogon: Enables MAC authentication success traps. The port security module sends traps when a MAC authentication is passed.

NOTE:

RALM (RADIUS Authenticated Login using MAC-address) means RADIUS authentication based on MAC address.

Description

Use **port-security trap** to enable port security traps.

Use **undo port-security trap** to disable port security traps.

By default, port security traps are disabled.

You can enable certain port security traps for monitoring user behaviors.

Related commands: **display port-security**.

Examples

Enable MAC address learning traps.

```
<Sysname> system-view
```

```
[Sysname] port-security trap addresslearned
```

User profile configuration commands

display user-profile

Syntax

display user-profile [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display user-profile** to display information about all user profiles that have been created.

Examples

Display information about all user profiles that have been created.

```
<Sysname> display user-profile
Status      User profile
enabled     a123
-----Total user profiles:      1-----
-----Enabled user profiles:    1-----
```

Table 20 Command output

Field	Description
Status	Status of the user profile: <ul style="list-style-type: none">• enabled• disabled
User profile	User profile name
Total user profiles	Total number of user profiles that have been created
Enabled user profiles	Total number of user profiles that have been enabled

user-profile enable

Syntax

```
user-profile profile-name enable  
undo user-profile profile-name enable
```

View

System view

Default level

2: System level

Parameters

profile-name: Specifies a user profile name, a case-sensitive string of 1 to 31 characters. It can only contain English letters, digits, and underlines, and it must start with an English letter. The user profile must already exist.

Description

Use **user-profile enable** to enable a user profile that has been created. If the user profile does not exist, the command fails. Only enabled user profiles can be applied to authenticated users.

Use **undo user-profile enable** to disable the specified user profile. Disabling a user profile logs out users that are using the user profile. To edit or remove the configurations in a user profile, disable the user profile first.

By default, a created user profile is disabled.

Examples

```
# Enable user profile a123.  
<Sysname> system-view  
[Sysname] user-profile a123 enable
```

user-profile

Syntax

```
user-profile profile-name  
undo user-profile profile-name
```

View

System view

Default level

2: System level

Parameters

profile-name: Assigns a name to the user profile. The name is a case-sensitive string of 1 to 31 characters. It can only contain English letters, digits, and underlines, and it must start with an English letter. A user profile name must be globally unique.

Description

Use **user-profile** to create a user profile. This command also places you in user profile view.

Use **undo user-profile** to remove an existing disabled user profile. You cannot remove a user profile that is enabled.

By default, no user profiles exist on the device.

Related commands: **user-profile enable**.

Examples

Create user profile **a123**.

```
<Sysname> system-view
[Sysname] user-profile a123
[Sysname-user-profile-a123]
```

Enter the user profile view of **a123**.

```
<Sysname> system-view
[Sysname] user-profile a123
[Sysname-user-profile-a123]
```

Password control configuration commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

display password-control

Syntax

```
display password-control [ super ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

2: System level

Parameters

super: Displays the password control information of the super passwords. Without this keyword, the command displays the password control information for all passwords.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display password-control** to display password control configuration information.

Examples

Display the global password control configuration information.

```
<Sysname> display password-control
```

Global password control configurations:

Password control:	Disabled
Password aging:	Enabled (90 days)
Password length:	Enabled (10 characters)
Password composition:	Enabled (1 types, 1 characters per type)
Password history:	Enabled (max history records:4)
Early notice on password expiration:	7 days
User authentication timeout:	60 seconds
Maximum failed login attempts:	3 times
Login attempt-failed action:	Lock for 1 minutes
Minimum password update time:	24 hours
User account idle-time:	90 days

```

Login with aged password:          3 times in 30 days
Password complexity:              Disabled (username checking)
                                   Disabled (repeated characters checking)

```

Display the password control configuration information for super passwords.

```

<Sysname> display password-control super
Super password control configurations:
Password aging:                  Enabled (90 days)
Password length:                Enabled (10 characters)
Password composition:           Enabled (1 types, 1 characters per type)

```

Table 21 Command output

Field	Description
Password control	Whether the global password control feature is enabled.
Password aging	Whether password aging is enabled and, if enabled, the aging time.
Password length	Whether the minimum password length restriction function is enabled and, if enabled, the setting.
Password composition	Whether the password composition restriction function is enabled and, if enabled, the settings.
Password history	Whether the password history function is enabled and, if enabled, the setting.
Early notice on password expiration	Number of days during which the user is notified of the pending password expiration.
User authentication timeout	Password authentication timeout time.
Maximum failed login attempts	Allowed maximum number of consecutive failed login attempts for FTP and VTY users.
Login attempt-failed action	Action to be taken after a user fails to login for the specified number of attempts.
Minimum password update time	Minimum password update interval.
User account idle-time	Maximum account idle time.
Login with aged password	Number of times and maximum number of days a user can log in using an expired password.
Password complexity	Whether the following password complexity checking is enabled: <ul style="list-style-type: none"> • username checking—Checks whether a password contains the username or the reverse of the username. • repeated characters checking—Checks whether a password contains any character that is repeated consecutively three or more times.

display password-control blacklist

Syntax

```

display password-control blacklist [ user-name name | ip ipv4-address | ipv6 ipv6-address ] [ { begin
| exclude | include } regular-expression ]

```

View

Any view

Default level

2: System level

Parameters

user-name *name*: Specifies a user by the name, a string of 1 to 80 characters.

ip *ipv4-address*: Specifies the IPv4 address of a user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a user.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display password-control blacklist** to display information about users blacklisted due to authentication failure.

With no arguments provided, this command displays information about all users in the blacklist.

Examples

Display information about users blacklisted due to authentication failure.

```
<Sysname> display password-control blacklist
```

```
Username: test
```

```
IP: 192.168.44.1          Login failed times: 1          Lock flag: unlock
```

```
Total 1 blacklist item(s) matched. 1 listed.
```

Table 22 Command output

Field	Description
Username	Username of the user
IP	IP address of the user
Login failed times	Number of login failures
Lock flag	Whether the user is prohibited from logging in: <ul style="list-style-type: none">• unlock—Not prohibited• lock—Prohibited temporarily or permanently, depending on the password-control login-attempt command

password

Syntax

password

undo password

View

Local user view

Default level

2: System level

Parameters

None

Description

Use **password** to set a password for a local user in interactive mode.

Use **undo password** to remove the password for a local user.

Valid characters for a local user password are from the following four types:

- Uppercase letters A to Z
- Lowercase letters a to z
- Digits 0 to 9
- 32 special characters: blank space, tilde (~), back quote (`), exclamation point (!), at sign (@), pound sign (#), dollar sign (\$), percent sign (%), caret (^), ampersand sign (&), asterisk (*), left parenthesis ("("), right parenthesis (")"), underscore (_), plus sign (+), minus sign (-), equal sign (=), left brace ({), right brace (}), vertical bar (|), left bracket ([), right bracket (]), back slash (\), colon (:), quotation marks ("), semi-colon (;), apostrophe ('), left angle bracket (<), right angle bracket (>), comma (,), dot (.), and slash (/)

A local user password configured in interactive mode must satisfy the password control requirement. For example, if the minimum password length is set to 8, the password must contain at least eight characters.

Examples

Set a password for local user **test** in interactive mode.

```
<Sysname> system-view
[Sysname] local-user test
[Sysname-luser-test] password
Password:*****
Confirm :*****
Updating user(s) information, please wait....
```

password-control { aging | composition | history | length } enable

Syntax

password-control { aging | composition | history | length } enable

undo password-control { aging | composition | history | length } enable

View

System view

Default level

2: System level

Parameters

aging: Enables the password aging function.

composition: Enables the password composition restriction function.

history: Enables the password history control function.

length: Enables the minimum password length restriction function.

Description

Use **password-control { aging | composition | history | length } enable** to enable the password aging, composition restriction, history, or minimum password length restriction function.

Use **undo password-control { aging | composition | history | length } enable** to disable the specified function.

By default, the four password control functions are all enabled.

For these four functions to take effect, the password control feature must be enabled globally.

You must enable a function for its relevant configurations to take effect. For example, if the minimum password length restriction function is not enabled, the setting by the **password-control length** command does not take effect.

The system stops recording history passwords after you execute the **undo password-control history enable** command, but it does not delete the prior records.

Related commands: **password-control enable** and **display password-control**.

Examples

```
# Enable the password control feature globally.
<Sysname> system-view
[Sysname] password-control enable

# Enable the password composition restriction function.
[Sysname] password-control composition enable

# Enable the password aging function.
[Sysname] password-control aging enable

# Enable the minimum password length restriction function.
[Sysname] password-control length enable

# Enable password history control.
[Sysname] password-control history enable
```

password-control aging

Syntax

password-control aging *aging-time*

undo password-control aging

View

System view, user group view, local user view

Default level

2: System level

Parameters

aging-time: Specifies the password aging time in days, in the range of 1 to 365.

Description

Use **password-control aging** to set the password aging time.

Use **undo password-control aging** to restore the default.

By default, the global password aging time is 90 days, the password aging time of a user group equals the global setting, and the password aging time of a local user equals that of the user group to which the local user belongs.

A password aging time setting with a smaller application range has a higher priority. That is, the system prefers the setting for a local user. If there is no setting for the local user, the system will use the setting for the user group. If there is no setting for the user group, the system will use the global setting.

If you do not set the aging time for super passwords, the global password aging time applies.

Related commands: **display password-control**, **local-user**, and **user-group**.

Examples

Set the global password aging time to 80 days.

```
<Sysname> system-view  
[Sysname] password-control aging 80
```

Set the password aging time for user group **test** to 90 days.

```
[Sysname] user-group test  
[Sysname-ugroup-test] password-control aging 90  
[Sysname-ugroup-test] quit
```

Set the password aging time for local user **abc** to 100 days.

```
[Sysname] local-user abc  
[Sysname-luser-abc] password-control aging 100
```

password-control alert-before-expire

Syntax

password-control alert-before-expire *alert-time*

undo password-control alert-before-expire

View

System view

Default level

2: System level

Parameters

alert-time: Specifies the number of days before a user's password expires during which the user is notified of the pending password expiration, in the range of 1 to 30.

Description

Use **password-control alert-before-expire** to set the number of days before a user's password expires during which the user is notified of the pending password expiration.

Use **undo password-control alert-before-expire** to restore the default.

By default, a user is notified of pending password expiration 7 days before the user's password expires.

Examples

Configure the device to notify a user about pending password expiration 10 days before the user's password expires.

```
<Sysname> system-view
```

```
[Sysname] password-control alert-before-expire 10
```

password-control authentication-timeout

Syntax

password-control authentication-timeout *authentication-timeout*

undo password-control authentication-timeout

View

System view

Default level

2: System level

Parameters

authentication-timeout: Specifies the user authentication timeout time in seconds, in the range of 30 to 120.

Description

Use **password-control authentication-timeout** to set the user authentication timeout time.

Use **undo password-control authentication-timeout** to restore the default.

By default, the user authentication timeout time is 60 seconds.

Examples

Set the user authentication timeout time to 40 seconds.

```
<Sysname> system-view
```

```
[Sysname] password-control authentication-timeout 40
```

password-control complexity

Syntax

password-control complexity { same-character | user-name } check

undo password-control complexity { same-character | user-name } check

View

System view

Default level

2: System level

Parameters

same-character: Refuses a password that contains any character repeated consecutively three or more times.

user-name: Refuses a password that contains the username or the reverse of the username.

Description

Use **password-control complexity** to configure the password complexity checking policy. Weak passwords will be refused.

Use **undo password-control complexity check** to remove a password complexity checking item.

By default, no user password complexity checking is performed, and a password can contain the username, the reverse of the username, or a character repeated three or more times consecutively.

Related commands: **display password-control**.

Examples

Configure the password complexity checking policy, refusing any password that contains the username or the reverse of the username.

```
<Sysname> system-view
```

```
[Sysname] password-control complexity user-name check
```

password-control composition

Syntax

password-control composition type-number *type-number* [**type-length** *type-length*]

undo password-control composition

View

System view, user group view, local user view

Default level

2: System level

Parameters

type-number *type-number*: Specifies the minimum number of character types that a password must contain. The value range for the *type-number* argument is 1 to 4 in non-FIPS mode and fixed at 4 in FIPS mode.

type-length *type-length*: Specifies the minimum number of characters that are from each character type in the password. The value range for the *type-length* argument is 1 to 63.

Description

Use **password-control composition** to configure the password composition policy.

Use **undo password-control composition** to restore the default.

In non-FIPS mode, the default global password composition policy is as follows: A password must contain at least one type of characters from uppercase letters, lowercase letters, digits or special characters (see "[password](#)"), and each type contains at least one character. The default password composition policy of a user group is the same as the global policy, and the default password composition policy of a local user is the same as that of the user group to which the local user belongs.

In FIPS mode, all passwords configured in any view must contain four types of characters from uppercase letters, lowercase letters, digits and special characters. The default password composition policy of a user group is the same as the global policy, and the default password composition policy of a local user is the same as that of the user group to which the local user belongs.

A password composition policy with a smaller application range has a higher priority. That is, the system prefers the settings for a local user. If there is no setting for the local user, the system will use the settings for the user group. If there is no setting for the user group, the system will use the global settings.

If you do not configure a password composition policy for super passwords, the global password composition policy applies.

Related commands: **display password-control**, **local-user**, and **user-group**.

Examples

Specify that all passwords must each contain at least three types of characters and each type must contain at least five characters.

```
<Sysname> system-view
```

```
[Sysname] password-control composition type-number 3 type-length 5
```

Specify that the passwords in user group **test** must each contain at least three types of characters and each type must contain at least five characters.

```
[Sysname] user-group test
```

```
[Sysname-ugroup-test] password-control composition type-number 3 type-length 5
```

```
[Sysname-ugroup-test] quit
```

Specify that the password of local user **abc** must contain at least three types of characters and each type must contain at least five characters.

```
[Sysname] local-user abc
```

```
[Sysname-luser-abc] password-control composition type-number 3 type-length 5
```

password-control enable

Syntax

password-control enable

undo password-control enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **password-control enable** to enable the global password control feature.

Use **undo password-control enable** to disable the global password control feature.

By default, the global password control feature is disabled.

Password control functions can take effect only after the global password control feature is enabled.

Disabling global password control (by using the **undo password-control enable** command) does not clear the history password records. To clear existing history password records, execute the **reset password-control history-record** command.

Related commands: **display password-control**.

Examples

```
# Enable the password control feature globally.  
<Sysname> system-view  
[Sysname] password-control enable
```

password-control expired-user-login

Syntax

```
password-control expired-user-login delay delay times times  
undo password-control expired-user-login
```

View

System view

Default level

2: System level

Parameters

delay *delay*: Specifies the maximum number of days during which a user can log in using an expired password. It must be in the range of 1 to 90.

times *times*: Specifies the maximum number of times a user can log in after the password expires, in the range of 0 to 10. 0 means that a user cannot log in after the password expires.

Description

Use **password-control expired-user-login** to set the maximum number of days and maximum number of times that a user can log in after the password expires.

Use **undo password-control expired-user-login** to restore the defaults.

By default, a user can log in three times within 30 days after the password expires.

Related commands: **display password-control**.

Examples

```
# Specify that a user can log in five times within 60 days after the password expires.  
<Sysname> system-view  
[Sysname] password-control expired-user-login delay 60 times 5
```

password-control history

Syntax

```
password-control history max-record-num  
undo password-control history
```

View

System view

Default level

2: System level

Parameters

max-record-num: Specifies the maximum number of history password records for each user, in the range of 2 to 15.

Description

Use **password-control history** to set the maximum number of history password records for each user.

Use **undo password-control history** to restore the default.

By default, the maximum number of history password records for each user is 4.

When the number of history passwords recorded for a user reaches the maximum, the new history password record of the user overwrites the oldest one.

Examples

```
# Set the maximum number of history password records for each user to 10.  
<Sysname> system-view  
[Sysname] password-control history 10
```

password-control length

Syntax

password-control length *length*

undo password-control length

View

System view, user group view, local user view

Default level

2: System level

Parameters

length: Specifies the minimum password length in characters. The value range for this argument is 4 to 32 in non-FIPS mode and 8 to 32 in FIPS mode.

Description

Use **password-control length** to set the minimum password length.

Use **undo password-control length** to restore the default.

By default, the global minimum password length is 10 characters, the minimum password length of a user group equals the global setting, and the minimum password length of a local user equals that of the user group to which the local user belongs.

A minimum password length setting with a smaller application range has a higher priority. That is, the system prefers the setting for a local user. If there is no setting for the local user, the system will use the setting for the user group. If there is no setting for the user group, the system will use the global setting.

If you do not set the minimum password length for super passwords, the global minimum password length applies.

When global password control is enabled but the minimum password length restriction function and FIPS mode are disabled, the minimum password length is four characters, and the password must have at least four different characters.

When global password control and FIPS mode are enabled but the minimum password length restriction function is disabled, the minimum password length is eight characters, and the password must have at least four different characters.

Related commands: **display password-control**, **local-user**, and **user-group**.

Examples

```
# Set the global minimum password length to 9 characters.
<Sysname> system-view
[Sysname] password-control length 9

# Set the minimum password length to 9 characters for user group test.
[Sysname] user-group test
[Sysname-ugroup-test] password-control length 9
[Sysname-ugroup-test] quit

# Set the minimum password length to 9 characters for local user abc.
[Sysname] local-user abc
[Sysname-luser-abc] password-control length 9
```

password-control login idle-time

Syntax

```
password-control login idle-time idle-time
undo password-control login idle-time
```

View

System view

Default level

2: System level

Parameters

idle-time: Specifies the maximum account idle time, in the range of 0 to 365, in days. 0 means no restriction for account idle time.

Description

Use **password-control login idle-time** to set the maximum account idle time. If a user account is idle for this period of time, it becomes invalid.

Use **undo password-control login idle-time** to restore the default.

By default, the maximum account idle time is 90 days.

Related commands: **display password-control**.

Examples

```
# Set the maximum account idle time to 30 days.
<Sysname> system-view
[Sysname] password-control login idle-time 30
```

password-control login-attempt

Syntax

```
password-control login-attempt login-times [ exceed { lock | lock-time time | unlock } ]  
undo password-control login-attempt
```

View

System view

Default level

2: System level

Parameters

login-times: Specifies the maximum number of consecutive failed login attempts, in the range of 2 to 10.

exceed: Specifies the action to be taken when a user fails to log in after the specified number of attempts.

lock: Permanently prohibits a user who fails to log in after the specified number of attempts from logging in.

lock-time time: Forces a user who fails to log in after the specified number of attempts to wait for a period of time before trying again. The *time* argument is in minutes and in the range of 1 to 360.

unlock: Allows a user who fails to log in after the specified number of attempts to continue trying to log in.

Description

Use **password-control login-attempt** to specify the maximum number of consecutive failed login attempts and the action to be taken when a user fails to log in after the specified number of attempts.

Use **undo password-control login-attempt** to restore the default.

By default, the maximum number of consecutive failed login attempts is three and a user failing to log in after the specified number of attempts must wait for one minute before trying again.

If prohibited permanently, a user can log in only after you remove the user from the blacklist.

If prohibited temporarily, a user can log in again after the lock time elapses or an administrator removes the user from the blacklist.

If not prohibited to log in, a user is removed from the blacklist as long as the user logs in successfully or after the blacklist aging time (one minute) elapses.

Related commands: **display password-control**, **display password-control blacklist**, and **reset password-control blacklist**.

Examples

Set the maximum number of login attempts to four and permanently prohibit a user failing to log in after four attempts from logging in.

```
<Sysname> system-view
```

```
[Sysname] password-control login-attempt 4 exceed lock
```

Later, if a user tries to log in but fails four times, you can find it in the blacklist, with its status changed from **unlock** to **lock**:

```
[Sysname] display password-control blacklist
```

```
Username: test
```

```
IP: 192.168.44.1
```

```
Login failed times: 4
```

```
Lock flag: lock
```

```
Total 1 blacklist item(s) matched.
```

The user can no longer log in.

Set the maximum number of login attempts to two and prohibit a user failing to log in after two attempts from logging in within three minutes.

```
<Sysname> system-view
```

```
[Sysname] password-control login-attempt 2 exceed lock-time 3
```

Later, if a user tries to log in but fails two times, you can find it in the blacklist, with its status changed from **unlock** to **lock**:

```
[Sysname] display password-control blacklist
```

```
Username: test
```

```
IP: 192.168.44.1          Login failed times: 2          Lock flag: lock
```

```
Total 1 blacklist item(s) matched.
```

After three minutes, the user is removed from the blacklist and can log in again.

password-control password update interval

Syntax

password-control password update interval *interval*

undo password-control password update interval

View

System view

Default level

2: System level

Parameters

interval: Specifies the minimum password update interval, in the range of 0 to 168, in hours. 0 means no requirements for password update interval.

Description

Use **password-control password update interval** to set the minimum password update interval, that is, the minimum interval at which users can change their passwords.

Use **undo password-control password update interval** to restore the default.

By default, the minimum password update interval is 24 hours.

This function is not effective in the case that a user is prompted to change the password when the user logs in for the first time or after the password is aged out.

Related commands: **display password-control**.

Examples

Set the minimum password update interval to 36 hours.

```
<Sysname> system-view
```

```
[Sysname] password-control password update interval 36
```

password-control super aging

Syntax

password-control super aging *aging-time*
undo password-control super aging

View

System view

Default level

2: System level

Parameters

aging-time: Specifies the super password aging time in days, in the range of 1 to 365.

Description

Use **password-control super aging** to set the aging time for super passwords.

Use **undo password-control super aging** to restore the default.

By default, the aging time for super passwords is the same as the global password aging time.

If you do not specify an aging time for super passwords, the system applies the global password aging time to super passwords.

If you have specified an aging time for super passwords, the system applies the aging time to super passwords.

Related commands: **password-control aging**.

Examples

```
# Set the aging time for super passwords to 10 days.  
<Sysname> system-view  
[Sysname] password-control super aging 10
```

password-control super composition

Syntax

password-control super composition type-number *type-number* [**type-length** *type-length*]
undo password-control super composition

View

System view

Default level

2: System level

Parameters

type-number *type-number*: Specifies the minimum number of character types that a super password must contain. The value range for the *type-number* argument is 1 to 4 in non-FIPS mode and fixed at 4 in FIPS mode.

type-length *type-length*: Specifies the minimum number of characters that are from each character type in a super password. The value range for the *type-length* argument is 1 to 16.

Description

Use **password-control super composition** to configure the composition policy for super passwords.

Use **undo password-control super composition** to restore the default.

By default, the super password composition policy is the same as the global password composition policy.

If you do not specify a composition policy for super passwords, the system applies the global password composition policy to super passwords.

If you have specified a composition policy for super passwords, the system applies the composition policy to super passwords.

Related commands: **password-control composition**.

Examples

Specify that super passwords must each contain at least three types of characters and each type must contain at least five characters.

```
<Sysname> system-view
```

```
[Sysname] password-control super composition type-number 3 type-length 5
```

password-control super length

Syntax

password-control super length *length*

undo password-control super length

View

System view

Default level

2: System level

Parameters

length: Specifies the minimum length for super passwords in characters. The value range for this argument is 4 to 16 in non-FIPS mode and 8 to 16 in FIPS mode.

Description

Use **password-control super length** to set the minimum length for super passwords.

Use **undo password-control super length** to restore the default.

By default, the minimum super password length is the same as the global minimum password length.

If you do not specify the minimum length of super passwords, the system applies the global minimum password length to super passwords.

If you have specified the minimum length of super passwords, the system applies the specified minimum length to super passwords.

Related commands: **password-control length**.

Examples

Set the minimum length for super passwords to 10 characters.

```
<Sysname> system-view
```

```
[Sysname] password-control super length 10
```

reset password-control blacklist

Syntax

```
reset password-control blacklist [ all | user-name name ]
```

View

User view

Default level

3: Manage level

Parameters

all: Removes all users from the blacklist.

user-name name: Specifies the username of the user to be removed from the blacklist. The *name* argument is a case-sensitive string of 1 to 80 characters.

Description

Use **reset password-control blacklist** to remove all or one user from the blacklist.

Related commands: **display password-control blacklist**.

Examples

```
# Delete the user named test from the blacklist.
```

```
<Sysname> reset password-control blacklist user-name test
```

```
Are you sure to delete the specified user in blacklist? [Y/N]:
```

reset password-control history-record

Syntax

```
reset password-control history-record [ user-name name | super [ level level/ ] ]
```

View

User view

Default level

3: Manage level

Parameters

user-name name: Specifies the username of the user whose password records are to be deleted. The *name* argument is a case-sensitive string of 1 to 80 characters.

super: Deletes the history records of the super password specified by the **level level/** combination or the history records of all super passwords.

level level/: Specifies a user level, in the range of 1 to 3.

Description

Use **reset password-control history-record** to delete history password records.

With no arguments or keywords specified, this command deletes the history password records of all local users.

With the **super** keyword specified but the *level* argument not specified, this command deletes the history records of all super passwords.

Examples

Clear the history password records of all local users (enter **Y** to confirm).

```
<Sysname> reset password-control history-record
```

```
Are you sure to delete all local user's history records? [Y/N]:
```

HABP configuration commands

display habp

Syntax

display habp [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display habp** to display HABP configuration information.

If the HABP function is not enabled on the device, this command does not display the HABP configuration but only the running status of the HABP function.

Examples

Display HABP configuration information.

```
<Sysname> display habp
```

```
Global HABP information:
```

```
  HABP Mode: Server
```

```
  Sending HABP request packets every 20 seconds
```

```
  Bypass VLAN: 2
```

Table 23 Command output

Field	Description
HABP Mode	HABP mode of the current device, server or client.
Sending HABP request packets every 20 seconds	The HABP server sends HABP request packets at an interval of 20 seconds.
Bypass VLAN	ID of the VLAN in which HABP packets are transmitted.

display habp table

Syntax

display habp table [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display habp table** to display HABP MAC address table entries.

This command is applicable only on an HABP server to display the MAC address entries collected by the HABP server.

Examples

On the HABP server, display HABP MAC address table entries.

```
<Sysname> display habp table
MAC                Holdtime  Receive Port
001f-3c00-0030    53          GigabitEthernet1/0/1
```

Table 24 Command output

Field	Description
MAC	MAC address.
Holdtime	Lifetime of an entry in seconds. The initial value is three times the interval to send HABP request packets. An entry will age out if it is not updated during the period.
Receive Port	Port that learned the MAC address.

display habp traffic

Syntax

display habp traffic [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display habp traffic** to display HABP packet statistics.

Examples

```
# Display HABP packet statistics.
<Sysname> display habp traffic
HABP counters :
    Packets output: 48, Input: 36
    ID error: 0, Type error: 0, Version error: 0
    Sent failed: 0
```

Table 25 Command output

Field	Description
Packets output	Number of HABP packets sent
Input	Number of HABP packets received
ID error	Number of packets with an incorrect ID
Type error	Number of packets with an incorrect type
Version error	Number of packets with an incorrect version number
Sent failed	Number of packets that failed to be sent

habp client vlan

Syntax

habp client vlan *vlan-id*

undo habp client

View

System view

Default level

2: System level

Parameters

vlan-id: Specifies the ID of the VLAN in which HABP packets are to be transmitted, in the range of 1 to 4094.

Description

Use **habp client vlan** to specify the VLAN to which the HABP client belongs. HABP packets are to be transmitted in this VLAN.

Use **undo habp client** to restore the default.

By default, an HABP client belongs to VLAN 1.

Examples

Specify the HABP client to belong to VLAN 2.

```
<Sysname> system-view  
[Sysname] habp client vlan 2
```

habp enable

Syntax

habp enable

undo habp enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **habp enable** to enable HABP.

Use **undo habp enable** to disable HABP.

By default, HABP is enabled.

Examples

Enable HABP.

```
<Sysname> system-view  
[Sysname] habp enable
```

habp server vlan

Syntax

habp server vlan *vlan-id*

undo habp server

View

System view

Default level

2: System level

Parameters

vlan-id: Specifies the ID of the VLAN in which HABP packets are to be transmitted, in the range of 1 to 4094.

Description

Use **habp server vlan** to configure HABP to operate in server mode and specify the VLAN in which HABP packets are to be transmitted.

Use **undo habp server** to configure HABP to operate in the default mode.

By default, HABP operates in client mode.

In a cluster, if a member switch with 802.1X authentication or MAC authentication enabled is attached with some other member switches of the cluster, you also need to configure HABP server on this device. Otherwise, the cluster management device will not be able to manage the devices attached to this member switch. For information about the cluster function, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure HABP to operate in server mode and specify the VLAN for HABP packets as VLAN 2.

```
<Sysname> system-view
```

```
[Sysname] habp server vlan 2
```

habp timer

Syntax

habp timer *interval*

undo habp timer

View

System view

Default level

2: System level

Parameters

interval: Specifies the interval (in seconds) at which the switch sends HABP request packets, in the range of 5 to 600.

Description

Use **habp timer** to set the interval at which the switch sends HABP request packets.

Use **undo habp timer** to restore the default.

The default interval is 20 seconds.

This command is required only on the HABP server.

Examples

Set the interval at which the switch sends HABP request packets to 50 seconds.

```
<Sysname> system-view
```

```
[Sysname] habp timer 50
```

Public key configuration commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

display public-key local public

Syntax

```
display public-key local { dsa | rsa } public [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

dsa: Specifies a DSA key pair.

rsa: Specifies an RSA key pair.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display public-key local public** to display the public key information of the local asymmetric key pairs.

Related commands: **public-key local create**.

Examples

```
# Display the public key information of the local RSA key pairs.
```

```
<Sysname> display public-key local rsa public
```

```
=====
```

```
Time of Key pair created: 19:59:16 2012/03/07
```

```
Key name: HOST_KEY
```

```
Key type: RSA Encryption Key
```

```
=====
```

```
Key code:
```

```
30819F300D06092A864886F70D010101050003818D0030818902818100BC4C392A97734A633BA0F1DB01F  
84EB51228EC86ADE1DBA597E0D9066FDC4F04776CEA3610D2578341F5D049143656F1287502C06D39D39F
```

```
28F0F5CBA630DA8CD1C16ECE8A7A65282F2407E8757E7937DCCDB5DB620CD1F471401B711713970234844
4A2D8900497A87B8D5F13D61C4DEFA3D14A7DC07624791FC1D226F62DF30203010001
```

```
=====
```

```
Time of Key pair created: 19:59:17 2012/03/07
```

```
Key name: SERVER_KEY
```

```
Key type: RSA Encryption Key
```

```
=====
```

```
Key code:
```

```
307C300D06092A864886F70D0101010500036B003068026100C51AF7CA926962284A4654B2AACC7B2AE12
B2B1EABFAC1CDA97E42C3C10D7A70D1012BF23ADE5AC4E7AAB132CFB6453B27E054BFAA0A85E113FBDE75
1EE0ECECF659529E857CF8C211E2A03FD8F10C5BEC162B2989ABB5D299D1E4E27A13C7DD10203010001
```

```
# Display the public key information of the local DSA key pair.
```

```
<Sysname> display public-key local dsa public
```

```
=====
```

```
Time of Key pair created: 20:00:16 2012/03/07
```

```
Key name: HOST_KEY
```

```
Key type: DSA Encryption Key
```

```
=====
```

```
Key code:
```

```
308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD96E5F061C4F
0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1EDBD13EC8B274DA9F75BA26
CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941DDD77FE6B12893DA76EEBC1D128D97F067
8D7722B5341C8506F358214B16A2FAC4B368950387811C7DA33021500C773218C737EC8EE993B4F2DED30
F48EDACE915F0281810082269009E14EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF931
33E84B47093C52B20CD35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC
717B612391C76C1FB2E88317C1BD8171D41ECB83E210C3CC9B32E810561C21621C73D6DAAC028F4B1585
DA7F42519718CC9B09EEF0381850002818100CCF1F78E0860BE937FD3CA07D2F2A1B66E74E5D1E16693EB
374D677A7A6124EBABD59FE48796C56F3FF919F999AEB97D1F2B83D9B98AC09BC1F72E80DBE337CB29989
A23378EB21C38EE083F11ED6DC8D4DBE001BA85450CEA071C2A471C83761E4CF32C174B418612CDD597B4
41F0CAA05DC01CB93A0ABB247C06FBA4C79054
```

Table 26 Command output

Field	Description
Time of Key pair created	Date and time when the local asymmetric key pair was created.
Key name	<p>Key name:</p> <ul style="list-style-type: none"> HOST_KEY—Host public key. SERVER_KEY—Server public key. This value is available only for RSA key pairs.
Key type	<p>Key type:</p> <ul style="list-style-type: none"> RSA Encryption Key—RSA key pair. DSA Encryption Key—DSA key pair.
Key code	Public key data.

display public-key peer

Syntax

```
display public-key peer [ brief | name publickey-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

brief: Displays brief information about all peer public keys saved on the local device.

name *publickey-name*: Displays information about a peer public key saved on the local device. The *publickey-name* argument represents a public key by its name, a case-sensitive string of 1 to 64 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display public-key peer** to display information about the specified or all peer public keys on the local device.

With neither the **brief** keyword nor the **name** *publickey-name* option specified, the command displays detailed information about all locally saved peer public keys.

You can use the **public-key peer** command or the **public-key peer import sshkey** command to get a local copy of a peer public key.

Related commands: **public-key peer** and **public-key peer import sshkey**.

Examples

Display detailed information about the peer host public key named **idrsa** saved on the local device.

```
<Sysname> display public-key peer name idrsa
```

```
=====
```

```
Key Name   : idrsa
```

```
Key Type   : RSA
```

```
Key Module: 1024
```

```
=====
```

```
Key Code:
```

```
30819D300D06092A864886F70D010101050003818B00308187028181009C46A8710216CEC0C01C7CE136B
A76C79AA6040E79F9E305E453998C7ADE8276069410803D5974F708496947AB39B3F39C5CE56C95B6AB74
42D56393BF241F99A639DD02D9E29B1F5C1FD05CC1C44FBD6CFFB58BE6F035FAA2C596B27D1231D159846
B7CB9A7757C5800FADA9FD72F65672F4A549EE99F63095E11BD37789955020123
```


Table 27 Command output

Field	Description
Key Name	Name of the public key.
Key Type	Key type, which can be RSA or DSA.
Key Module	Key modulus length in bits.
Key Code	Public key data.

Display brief information about all locally saved peer public keys.

```
<Sysname> display public-key peer brief
```

```
Type  Module  Name
```

```
-----
```

```
RSA    1024    idrsa
```

```
DSA    1024    10.1.1.1
```

Table 28 Command output

Field	Description
Type	Key type, RSA or DSA.
Module	Key modulus length in bits
Name	Name of the public key

peer-public-key end

Syntax

peer-public-key end

View

Public key view

Default level

2: System level

Parameters

None

Description

Use **peer-public-key end** to return from public key view to system view.

Related commands: **public-key peer**.

Examples

Exit public key view.

```
<Sysname> system-view
```

```
[Sysname] public-key peer key1
```

```
[Sysname-pkey-public-key] peer-public-key end
```

```
[Sysname]
```

public-key-code begin

Syntax

public-key-code begin

View

Public key view

Default level

2: System level

Parameters

None

Description

Use **public-key-code begin** to enter public key code view. Then input the key data in the correct format to specify the peer public key. Spaces and carriage returns are allowed between characters, but are not saved.

If the peer device is an HP device, input the key data displayed by the **display public-key local public** command so that the key is format compliant.

Related commands: **public-key peer** and **public-key-code end**.

Examples

Enter public key code view and input the key.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] public-key-code begin
[Sysname-pkey-key-code]30819F300D06092A864886F70D010101050003818D0030818902818100C0EC
8014F82515F6335A0A
[Sysname-pkey-key-code]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719D164
3135877E13B1C531B4
[Sysname-pkey-key-code]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B952ADF6
B80EB5F52698FCF3D6
[Sysname-pkey-key-code]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4A9B1
DDE675AC30CB020301
[Sysname-pkey-key-code]0001
```

public-key-code end

Syntax

public-key-code end

View

Public key code view

Default level

2: System level

Parameters

None

Description

Use **public-key-code end** to return from public key code view to public key view and to save the configured public key.

The system verifies the key before saving it. If the key is not in the correct format, the system discards the key and displays an error message. If the key is valid, the system saves the key.

Related commands: **public-key peer** and **public-key-code begin**.

Examples

Exit public key code view and save the configured public key.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] public-key-code begin
[Sysname-pkey-key-code] 30819F300D06092A864886F70D010101050003818D0030818902818100C0EC
8014F82515F6335A0A
[Sysname-pkey-key-code] EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719D164
3135877E13B1C531B4
[Sysname-pkey-key-code] FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B952ADF6
B80EB5F52698FCF3D6
[Sysname-pkey-key-code] 1F0C2EAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4A9B1
DDE675AC30CB020301
[Sysname-pkey-key-code] 0001
[Sysname-pkey-key-code] public-key-code end
[Sysname-pkey-public-key]
```

public-key local create

Syntax

public-key local create { dsa | rsa }

View

System view

Default level

2: System level

Parameters

dsa: Specifies a DSA key pair.

rsa: Specifies an RSA key pair.

Description

Use **public-key local create** to create local asymmetric key pairs. The created local key pairs are saved automatically, and can survive a reboot.

By default, no asymmetric key pair is created.

When using this command to create DSA or RSA key pairs, you are asked to provide the length of the key modulus. In non-FIPS mode, the DSA or RSA modulus length is in the range of 512 to 2048 bits, and defaults to 1024 bits. In FIPS mode, the DSA modulus length is in the range of 1024 to 2048 bits and defaults to 1024 bits, and the RSA modulus length must be 2048 bits. If the type of key pair already exists, the system asks you whether you want to overwrite it.

Related commands: **public-key local destroy** and **display public-key local public**.

Examples

[illegible]

public-key local destroy

Syntax

public-key local destroy { dsa | rsa }

View

System view

Default level

2: System level

Parameters

dsa: DSA key pair.

rsa: RSA key pair.

Description

Use **public-key local destroy** to destroy the local asymmetric key pairs.

Related commands: **public-key local create**.

Examples

```
# Destroy the local RSA key pairs.
<Sysname> system-view
[Sysname] public-key local destroy rsa
Warning: Confirm to destroy these keys? [Y/N]:y

# Destroy the local DSA key pair.
<Sysname> system-view
[Sysname] public-key local destroy dsa
Warning: Confirm to destroy these keys? [Y/N] :y
```

public-key local export dsa

Syntax

```
public-key local export dsa { openssh | ssh2 } [ filename ]
```

View

System view

Default level

2: System level

Parameters

openssh: Uses the format of OpenSSH.

ssh2: Uses the format of SSH2.0.

filename: Specifies the name of the file for storing the local public key. For more information about file name, see *Fundamentals Configuration Guide*.

Description

Use **public-key local export dsa** without the *filename* argument to display the host public key of the local DSA key pair in the specified format.

Use **public-key local export dsa** with the *filename* argument to export the host public key of the local DSA key pair to the specified file.

SSH2.0 and OpenSSH are two different public key formats. Choose the proper format that is supported on the device where you import the host public key.

Related commands: **public-key local create** and **public-key local destroy**.

Examples

```
# Export the local DSA host public key in OpenSSH format to a file named key.pub.
<Sysname> system-view
[Sysname] public-key local export dsa openssh key.pub

# Display the local DSA host public key in SSH2.0 format.
<Sysname> system-view
[Sysname] public-key local export dsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-20120307"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHGRx9ozAAAAFQDHcyGMC37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YU
```

```
XrZWUGeZn/OrpbsTV75MTPoS0cJPFKyDNNdAkkroVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBANVcLNEKdDt6xcatp
RjxsSrHXFVIdRjxw59qZnKh187GsbgP4ccUp3KmcRzuqgz1qNtfgoZOLzHnG1YGxPp7Q2k/uRuuHN0bJfBkOL
o2/RyGqDJIqB4FQwmrkWJuauYGqQy+mgE6dmHn0VG4gAkx9MQxDIBjzbZRX0bvXMdNKR22
---- END SSH2 PUBLIC KEY ----
```

Display the local DSA host public key in OpenSSH format.

```
<Sysname> system-view
```

```
[Sysname] public-key local export dsa openssh
```

```
ssh-dss
```

```
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3
B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuORChYLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbz
WCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGmc37I7pk7Ty3tMPSO2s6RXwAAAEAgiaQCeFOxHS68pMuadOx8YU
XrZWUGeZn/OrpbsTV75MTPoS0cJPFKyDNNdAkkroVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBANVcLNEKdDt6xcatp
RjxsSrHXFVIdRjxw59qZnKh187GsbgP4ccUp3KmcRzuqgz1qNtfgoZOLzHnG1YGxPp7Q2k/uRuuHN0bJfBkOL
o2/RyGqDJIqB4FQwmrkWJuauYGqQy+mgE6dmHn0VG4gAkx9MQxDIBjzbZRX0bvXMdNKR22 dsa-key
```

public-key local export rsa

Syntax

In non-FIPS mode:

```
public-key local export rsa { openssh | ssh1 | ssh2 } [ filename ]
```

In FIPS mode:

```
public-key local export rsa { openssh | ssh2 } [ filename ]
```

View

System view

Default level

2: System level

Parameters

openssh: Uses the format of OpenSSH.

ssh1: Uses the format of SSH1.5.

ssh2: Uses the format of SSH2.0.

filename: Specifies the name of the file for storing the host public key. For more information about file name, see *Fundamentals Configuration Guide*.

Description

Use **public-key local export rsa** without the *filename* argument to display the host public key of the local RSA key pairs in the specified key format.

Use **public-key local export rsa** with the *filename* argument to export the host public key of the local RSA key pairs to the specified file.

SSH1, SSH2.0 and OpenSSH are three different public key formats for different requirements.

Related commands: **public-key local create** and **public-key local destroy**.

Examples

```
# Export the host public key of the local RSA key pairs in OpenSSH format to the file named key.pub.
```

```

<Sysname> system-view
[Sysname] public-key local export rsa openssh key.pub

# Display the host public key of the local RSA key pairs in SSH2.0 format.
<Sysname> system-view
[Sysname] public-key local export rsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20120307"
AAAAB3NzaClyc2EAAAADAQABAAQDAQAo0dVYR1S5f30eLKGNKuqb5HU3M0TTSaG1ER2GmcRI2sgSegbolx6u
t5NIc5+jJxuRCU4+gMc76iS8d+2d50FqIweEkHHkSG/ddgXt/iAZ6cY81bdu/CKxGiQlkUpbw4vSv+X5KeE7j
+o0MpOpzh3W768/+ulriz+1LcwVTs5lQ==
---- END SSH2 PUBLIC KEY ----

# Display the host public key of the local RSA key pairs in OpenSSH format.
<Sysname> system-view
[Sysname] public-key local export rsa openssh
ssh-rsa
AAAAB3NzaClyc2EAAAADAQABAAQDAQAo0dVYR1S5f30eLKGNKuqb5HU3M0TTSaG1ER2GmcRI2sgSegbolx6u
t5NIc5+jJxuRCU4+gMc76iS8d+2d50FqIweEkHHkSG/ddgXt/iAZ6cY81bdu/CKxGiQlkUpbw4vSv+X5KeE7j
+o0MpOpzh3W768/+ulriz+1LcwVTs5lQ== rsa-key

```

public-key peer

Syntax

```

public-key peer keyname
undo public-key peer keyname

```

View

System view

Default level

2: System level

Parameters

keyname: Specifies a name for the peer public key on the local device, a case-sensitive string of 1 to 64 characters.

Description

Use **public-key peer** to specify a name for the peer public key and enter public key view.

Use **undo public-key peer** to remove the public key.

To manually configure the peer public key on the local device, obtain the public key in hexadecimal from the peer device beforehand, and perform the following configurations on the local device:

1. Execute the **public-key peer** command, and then the **public-key-code begin** command to enter public key code view.
2. Type the peer public key.
3. Execute the **public-key-code end** command to save the public key and return to public key view.
4. Execute the **peer-public-key end** command to return to system view.

Related commands: **public-key-code begin**, **public-key-code end**, **peer-public-key end**, and **display public-key peer**.

Examples

```
# Specify the name for the per public key as key1 and enter public key view.  
<Sysname> system-view  
[Sysname] public-key peer key1  
[Sysname-pkey-public-key]
```

public-key peer import sshkey

Syntax

```
public-key peer keyname import sshkey filename  
undo public-key peer keyname
```

View

System view

Default level

2: System level

Parameters

keyname: Specifies a public key name, a case-sensitive string of 1 to 64 characters.

filename: Specifies the name of the file that saves the peer host public key. For more information about file name, see *Fundamentals Configuration Guide*.

Description

Use **public-key peer import sshkey** to import a peer host public key from the public key file.

Use **undo public-key peer** to remove the specified peer host public key.

After execution of this command, the system automatically transforms the peer host public key to the PKCS format, and imports the key. This operation requires that you get a copy of the public key file from the peer device through FTP or TFTP in binary mode in advance.

The device supports importing public keys in the format of SSH1.5, SSH2.0, and OpenSSH.

Related commands: **display public-key peer**.

Examples

```
# Import the peer host public key named key2 from the public key file key.pub.  
<Sysname> system-view  
[Sysname] public-key peer key2 import sshkey key.pub
```

PKI configuration commands

attribute

Syntax

```
attribute id { alt-subject-name { fqdn | ip } | { issuer-name | subject-name } { dn | fqdn | ip } } { ctn | equ | nctn | nequ } attribute-value  
undo attribute { id | all }
```

View

Certificate attribute group view

Default level

2: System level

Parameters

id: Sequence number of the certificate attribute rule, in the range of 1 to 16.

alt-subject-name: Specifies the name of the alternative certificate subject.

fqdn: Specifies the FQDN of the entity.

ip: Specifies the IP address of the entity.

issuer-name: Specifies the name of the certificate issuer.

subject-name: Specifies the name of the certificate subject.

dn: Specifies the distinguished name of the entity.

ctn: Specifies the contain operation.

equ: Specifies the equal operation.

nctn: Specifies the not-contain operation.

nequ: Specifies the not-equal operation.

attribute-value: Value of the certificate attribute, a case-insensitive string of 1 to 128 characters.

all: Specifies all certificate attributes.

Description

Use **attribute** to configure the attribute rules of the certificate issuer name, certificate subject name and alternative certificate subject name.

Use **undo attribute** to delete the attribute rules of certificates.

By default, no restriction exists on the issuer name, subject name, and alternative subject name of a certificate.

The attribute of the alternative certificate subject name does not appear as a distinguished name, and therefore the **dn** keyword is not available for the attribute.

Examples

Create a certificate attribute rule, specifying that the DN in the subject name includes the string of **abc**.

```

<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup] attribute 1 subject-name dn ctn abc

# Create a certificate attribute rule, specifying that the FQDN in the issuer name cannot be the string of
abc.
[Sysname-pki-cert-attribute-group-mygroup] attribute 2 issuer-name fqdn nequ abc

# Create a certificate attribute rule, specifying that the IP address in the alternative subject name cannot
be 10.0.0.1.
[Sysname-pki-cert-attribute-group-mygroup] attribute 3 alt-subject-name ip nequ 10.0.0.1

```

ca identifier

Syntax

```

ca identifier name
undo ca identifier

```

View

PKI domain view

Default level

2: System level

Parameters

name: Name of the trusted CA, a case-insensitive string of 1 to 63 characters.

Description

Use **ca identifier** to specify the trusted CA and bind the switch with the CA.

Use **undo ca identifier** to remove the configuration.

By default, no trusted CA is specified for a PKI domain.

Certificate request, retrieval, revocation, and query all depend on the trusted CA.

Examples

```

# Specify the trusted CA as new-ca.
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] ca identifier new-ca

```

certificate request entity

Syntax

```

certificate request entity entity-name
undo certificate request entity

```

View

PKI domain view

Default level

2: System level

Parameters

entity-name: Name of the entity for certificate request, a case-insensitive string of 1 to 15 characters.

Description

Use **certificate request entity** to specify the entity for certificate request.

Use **undo certificate request entity** to remove the configuration.

By default, no entity is specified for certificate request.

Related commands: **pki entity**.

Examples

```
# Specify the entity for certificate request as entity1.
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request entity entity1
```

certificate request from

Syntax

certificate request from { ca | ra }

undo certificate request from

View

PKI domain view

Default level

2: System level

Parameters

ca: Indicates that the entity requests a certificate from a CA.

ra: Indicates that the entity requests a certificate from an RA.

Description

Use **certificate request from** to specify the authority for certificate request.

Use **undo certificate request from** to remove the configuration.

By default, no authority is specified for certificate request.

Examples

```
# Specify that the entity requests a certificate from the CA.
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request from ca
```

certificate request mode

Syntax

certificate request mode { auto [key-length key-length | password { cipher | simple } password] * | manual }

undo certificate request mode

View

PKI domain view

Default level

2: System level

Parameters

auto: Requests certificates in auto mode.

key-length: Length of the RSA keys in bits, in the range of 512 to 2048. It is 1024 bits by default.

cipher: Sets a ciphertext password for certificate revocation.

simple: Sets a plaintext password for certificate revocation.

password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 31 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 73 characters.

manual: Requests certificates in manual mode.

Description

Use **certificate request mode** to set the certificate request mode.

Use **undo certificate request mode** to restore the default.

By default, manual mode is used.

In auto mode, an entity automatically requests a certificate from an RA or CA when it has no certificate. However, if the certificate will expire or has expired, the entity does not initiate a re-request automatically. To have a new local certificate, you need to request one manually. In manual mode, all operations associated with certificate request are carried out manually. The plaintext password or ciphertext password is saved in cipher text in the configuration file.

Related commands: **pki request-certificate**.

Examples

```
# Specify to request a certificate in auto mode.
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request mode auto
```

certificate request polling

Syntax

certificate request polling { count *count* | interval *minutes* }

undo certificate request polling { count | interval }

View

PKI domain view

Default level

2: System level

Parameters

count *count*: Specifies the maximum number of attempts to poll the status of the certificate request, in the range of 1 to 100.

interval *minutes*: Specifies the polling interval in minutes, in the range of 5 to 168.

Description

Use **certificate request polling** to specify the certificate request polling interval and attempt limit.

Use **undo certificate request polling** to restore the defaults.

By default, the polling is executed every 20 minutes for up to 50 times.

After an applicant makes a certificate request, the CA might need a long period of time if it verifies the certificate request manually. During this period, the applicant needs to query the status of the request periodically to get the certificate as soon as possible after the certificate is signed.

Related commands: **display pki certificate**.

Examples

Specify the polling interval as 15 minutes and the maximum number of attempts as 40.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request polling interval 15
[Sysname-pki-domain-1] certificate request polling count 40
```

certificate request url

Syntax

certificate request url *url-string*

undo certificate request url

View

PKI domain view

Default level

2: System level

Parameters

url-string: URL for certificate request, a case-insensitive string of 1 to 127 characters. It comprises the location of the server and the location of CGI command interface script in the format `http://server_location/ca_script_location`, where *server_location* must be an IP address and does not support domain name resolution.

Description

Use **certificate request url** to specify the URL for certificate request through SCEP.

Use **undo certificate request url** to remove the configuration.

By default, no certificate request URL is specified for a PKI domain.

Examples

Specify the certificate request URL.

```
<Sysname> system-view
[Sysname] pki domain 1
```

```
[Sysname-pki-domain-1] certificate request url  
http://169.254.0.100/certsrv/mscep/mscep.dll
```

common-name

Syntax

common-name *name*

undo common-name

View

PKI entity view

Default level

2: System level

Parameters

name: Common name of an entity, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use **common-name** to configure the common name of an entity, which can be, for example, the user name.

Use **undo common-name** to remove the configuration.

By default, no common name is specified.

Examples

Configure the common name of an entity as **test**.

```
<Sysname> system-view
```

```
[Sysname] pki entity 1
```

```
[Sysname-pki-entity-1] common-name test
```

country

Syntax

country *country-code-str*

undo country

View

PKI entity view

Default level

2: System level

Parameters

country-code-str: Country code for the entity, a 2-character case-insensitive string.

Description

Use **country** to specify the code of the country to which an entity belongs. It is a standard 2-character code, for example, CN for China.

Use **undo country** to remove the configuration.

By default, no country code is specified.

Examples

```
# Set the country code of an entity to CN.
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] country CN
```

crl check

Syntax

```
crl check { disable | enable }
```

View

PKI domain view

Default level

2: System level

Parameters

disable: Disables CRL checking.

enable: Enables CRL checking.

Description

Use **crl check** to enable or disable CRL checking.

By default, CRL checking is enabled.

CRLs are files issued by the CA to publish all certificates that have been revoked. Revocation of a certificate might occur before the certificate expires. CRL checking is intended for checking whether a certificate has been revoked. A revoked certificate is no longer trusted.

Examples

```
# Disable CRL checking.
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl check disable
```

crl update-period

Syntax

```
crl update-period hours
```

```
undo crl update-period
```

View

PKI domain view

Default level

2: System level

Parameters

hours: CRL update period in hours, in the range of 1 to 720.

Description

Use **crl update-period** to set the CRL update period, the interval at which a PKI entity with a certificate downloads the latest CRL from the LDAP server.

Use **undo crl update-period** to restore the default.

By default, the CRL update period depends on the next update field in the CRL file.

Examples

```
# Set the CRL update period to 20 hours.
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl update-period 20
```

crl url

Syntax

crl url *url-string*

undo crl url

View

PKI domain view

Default level

2: System level

Parameters

url-string: URL of the CRL distribution point, a case-insensitive string of 1 to 127 characters in the format `ldap://server_location` or `http://server_location`, where *server_location* must be an IP address and does not support domain name resolution.

Description

Use **crl url** to specify the URL of the CRL distribution point.

Use **undo crl url** to remove the configuration.

By default, no CRL distribution point URL is specified.

When the URL of the CRL distribution point is not set, you should acquire the CA certificate and a local certificate, and then acquire a CRL through SCEP.

Examples

```
# Specify the URL of the CRL distribution point.
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl url ldap://169.254.0.30
```

display pki certificate

Syntax

display pki certificate { { **ca** | **local** } **domain** *domain-name* | **request-status** } [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ca: Displays the CA certificate.

local: Displays the local certificate.

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

request-status: Displays the status of a certificate request.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display pki certificate** to display the contents or request status of a certificate.

Related commands: **certificate request polling**, **pki domain**, and **pki retrieval-certificate**.

Examples

Display the local certificate.

```
<Sysname> display pki certificate local domain 1
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

10B7D4E3 00010000 0086

Signature Algorithm: md5WithRSAEncryption

Issuer:

emailAddress=myca@aabbcc.net

C=CN

ST=Country A

L=City X

O=abc

OU=bjs

CN=new-ca

Validity

Not Before: Jan 13 08:57:21 2012 GMT

Not After : Jan 20 09:07:21 2012 GMT

Subject:

C=CN

ST=Country B

L=City Y

```

      CN=pki test
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (512 bit)
    Modulus (512 bit):
      00D41D1F ...
    Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Subject Alternative Name:
    DNS: hyf.xxyyzz.net
  X509v3 CRL Distribution Points:
    URI:http://1.1.1.1:447/myca.crl
    ...
Signature Algorithm: md5WithRSAEncryption
A3A5A447 4D08387D ...

```

Table 29 Command output

Field	Description
Version	Version of the certificate
Serial Number	Serial number of the certificate
Signature Algorithm	Signature algorithm
Issuer	Issuer of the certificate
Validity	Validity period of the certificate
Subject	Entity holding the certificate
Subject Public Key Info	Public key information of the entity
X509v3 extensions	Extensions of the X.509 (version 3) certificate
X509v3 CRL Distribution Points	Distribution points of X.509 (version 3) CRLs

display pki certificate access-control-policy

Syntax

```
display pki certificate access-control-policy { policy-name | all } [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

policy-name: Name of the certificate attribute-based access control policy, a string of 1 to 16 characters.

all: Specifies all certificate attribute-based access control policies.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display pki certificate access-control-policy** to display information about certificate attribute-based access control policies.

Examples

Display information about the certificate attribute-based access control policy named **mypolicy**.

```
<Sysname> display pki certificate access-control-policy mypolicy
access-control-policy name: mypolicy
    rule 1 deny    mygroup1
    rule 2 permit  mygroup2
```

Table 30 Command output

Field	Description
access-control-policy	Name of the certificate attribute-based access control policy
rule number	Number of the access control rule

display pki certificate attribute-group

Syntax

```
display pki certificate attribute-group { group-name | all } [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

group-name: Name of a certificate attribute group, a string of 1 to 16 characters.

all: Specifies all certificate attribute groups.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display pki certificate attribute-group** to display information about certificate attribute groups.

Examples

```
# Display information about certificate attribute group mygroup.
<Sysname> display pki certificate attribute-group mygroup
attribute group name: mygroup
      attribute 1 subject-name      dn      ctn      abc
      attribute 2 issuer-name      fqdn     nctn     app
```

Table 31 Command output

Field	Description
attribute group name	Name of the certificate attribute group
attribute <i>number</i>	Number of the attribute rule
subject-name	Name of the certificate subject
dn	DN of the entity
ctn	Indicates the contain operations
abc	Value of attribute 1
issuer-name	Name of the certificate issuer
fqdn	FQDN of the entity
nctn	Indicates the not-contain operations
app	Value of attribute 2

display pki crt domain

Syntax

```
display pki crt domain domain-name [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display pki crt domain** to display the locally saved CRLs.

Related commands: **pki domain** and **pki retrieval-crl**.

Examples

Display the locally saved CRLs.

```
<Sysname> display pki crl domain 1
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer:
    C=CN
    O=abc
    OU=soft
    CN=A Test Root
  Last Update: Jan  5 08:44:19 2012 GMT
  Next Update: Jan  5 21:42:13 2012 GMT
  CRL extensions:
    X509v3 Authority Key Identifier:
      keyid:0F71448E E075CAB8 ADDB3A12 0B747387 45D612EC
    Revoked Certificates:
      Serial Number: 05a234448E...
      Revocation Date: Feb 6 12:33:22 2012 GMT
      CRL entry extensions:...
      Serial Number: 05a278445E...
      Revocation Date: Feb 7 12:33:22 2012 GMT
      CRL entry extensions:...
```

Table 32 Command output

Field	Description
Version	Version of the CRL.
Signature Algorithm	Signature algorithm used by the CRLs.
Issuer	CA issuing the CRLs.
Last Update	Last update time.
Next Update	Next update time.
CRL extensions	Extensions of CRL.
X509v3 Authority Key Identifier	CA issuing the CRLs. The certificate version is X.509 v3.
keyid	ID of the public key. A CA might have multiple key pairs. This field indicates the key pair used by the CRL's signature.
Revoked Certificates	Revoked certificates.
Serial Number	Serial number of the revoked certificate.
Revocation Date	Revocation date of the certificate.

undo fqdn

View

PKI entity view

Default level

2: System level

Parameters

name-str: Fully qualified domain name (FQDN) of an entity, a case-insensitive string of 1 to 127 characters.

Description

Use **fqdn** to configure the FQDN of an entity.

Use **undo fqdn** to remove the configuration.

By default, no FQDN is specified for an entity.

An FQDN is the unique identifier of an entity on a network. It consists of a host name and a domain name and can be resolved into an IP address.

Examples

Configure the FQDN of an entity as **pki.domain-name.com**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] fqdn pki.domain-name.com
```

ip (PKI entity view)

Syntax

ip *ip-address*

undo ip

View

PKI entity view

Default level

2: System level

Parameters

ip-address: IP address for an entity.

Description

Use **ip** to configure the IP address of an entity.

Use **undo ip** to remove the configuration.

By default, no IP address is specified for an entity.

Examples

Configure the IP address of an entity as 11.0.0.1.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] ip 11.0.0.1
```

ldap-server

Syntax

```
ldap-server ip ip-address [ port port-number ] [ version version-number ]  
undo ldap-server
```

View

PKI domain view

Default level

2: System level

Parameters

ip-address: IP address of the LDAP server, in dotted decimal format.

port-number: Port number of the LDAP server, in the range of 1 to 65535. The default is 389.

version-number: LDAP version number, either 2 or 3. By default, it is 2.

Description

Use **ldap-server** to specify an LDAP server for a PKI domain.

Use **undo ldap-server** to remove the configuration.

By default, no LDP server is specified for a PKI domain.

Examples

```
# Specify an LDAP server for PKI domain 1.  
<Sysname> system-view  
[Sysname] pki domain 1  
[Sysname-pki-domain-1] ldap-server ip 169.254.0.30
```

locality

Syntax

```
locality locality-name  
undo locality
```

View

PKI entity view

Default level

2: System level

Parameters

locality-name: Name for the geographical locality, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use **locality** to configure the geographical locality of an entity, which can be, for example, a city name.

Use **undo locality** to remove the configuration.

By default, no geographical locality is specified for an entity.

Examples

```
# Configure the locality of an entity as city.
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] locality city
```

organization

Syntax

```
organization org-name
undo organization
```

View

PKI entity view

Default level

2: System level

Parameters

org-name: Organization name, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use **organization** to configure the name of the organization to which the entity belongs.

Use **undo organization** to remove the configuration.

By default, no organization name is specified for an entity.

Examples

```
# Configure the name of the organization to which an entity belongs as test-lab.
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] organization test-lab
```

organization-unit

Syntax

```
organization-unit org-unit-name
undo organization-unit
```

View

PKI entity view

Default level

2: System level

Parameters

org-unit-name: Organization unit name for distinguishing different units in an organization, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use **organization-unit** to specify the name of the organization unit to which this entity belongs.

Use **undo organization-unit** to remove the configuration.

By default, no organization unit name is specified for an entity.

Examples

Configure the name of the organization unit to which an entity belongs as **group1**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] organization-unit group1
```

pki certificate access-control-policy

Syntax

pki certificate access-control-policy *policy-name*

undo pki certificate access-control-policy { *policy-name* | **all** }

View

System view

Default level

2: System level

Parameters

policy-name: Name of the certificate attribute-based access control policy, a case-insensitive string of 1 to 16 characters. It cannot be a, al, or all.

all: Specifies all certificate attribute-based access control policies.

Description

Use **pki certificate access-control-policy** to create a certificate attribute-based access control policy and enter its view.

Use **undo pki certificate access-control-policy** to remove certificate attribute-based access control policies.

No access control policy exists by default.

Examples

Configure an access control policy named **mypolicy** and enter its view.

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy]
```

pki certificate attribute-group

Syntax

pki certificate attribute-group *group-name*

undo pki certificate attribute-group { *group-name* | **all** }

View

System view

Default level

2: System level

Parameters

group-name: Name for the certificate attribute group, a case-insensitive string of 1 to 16 characters. It cannot be *a*, *al*, or *all*.

all: Specifies all certificate attribute groups.

Description

Use **pki certificate attribute-group** to create a certificate attribute group and enter its view.

Use **undo pki certificate attribute-group** to delete certificate attribute groups.

By default, no certificate attribute group exists.

Examples

```
# Create a certificate attribute group named mygroup and enter its view.
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup]
```

pki delete-certificate

Syntax

pki delete-certificate { **ca** | **local** } **domain** *domain-name*

View

System view

Default level

2: System level

Parameters

ca: Deletes the locally stored CA certificate.

local: Deletes the locally stored local certificate.

domain-name: Name of the PKI domain whose certificates are to be deleted, a string of 1 to 15 characters.

Description

Use **pki delete-certificate** to delete the certificate locally stored for a PKI domain.

Examples

```
# Delete the local certificate for PKI domain cer.
<Sysname> system-view
[Sysname] pki delete-certificate local domain cer
```

pki domain

Syntax

pki domain *domain-name*

undo pki domain *domain-name*

View

System view

Default level

2: System level

Parameters

domain-name: PKI domain name, a case-insensitive string of 1 to 15 characters.

Description

Use **pki domain** to create a PKI domain and enter PKI domain view.

Use **undo pki domain** to remove a PKI domain.

By default, no PKI domain exists.

Examples

Create a PKI domain and enter its view.

```
<Sysname> system-view
```

```
[Sysname] pki domain 1
```

```
[Sysname-pki-domain-1]
```

pki entity

Syntax

pki entity *entity-name*

undo pki entity *entity-name*

View

System view

Default level

2: System level

Parameters

entity-name: Name for the entity, a case-insensitive string of 1 to 15 characters.

Description

Use **pki entity** to create a PKI entity and enter its view.

Use **undo pki entity** to remove a PKI entity.

By default, no entity exists.

You can configure a variety of attributes for an entity in PKI entity view. An entity is intended only for convenience of reference by other commands.

Examples

```
# Create a PKI entity named en and enter its view.  
<Sysname> system-view  
[Sysname] pki entity en  
[Sysname-pki-entity-en]
```

pki import-certificate

Syntax

```
pki import-certificate { ca | local } domain domain-name { der | p12 | pem } [ filename filename ]
```

View

System view

Default level

2: System level

Parameters

ca: Specifies the CA certificate.

local: Specifies the local certificate.

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

der: Specifies the certificate format of DER.

p12: Specifies the certificate format of P12.

pem: Specifies the certificate format of PEM.

filename filename: Specifies the name of the certificate file, a case-insensitive string of 1 to 127 characters. If no file name is specified, the system uses the default file name that is used when the certificate is retrieved, that is, *domain-name_ca.cer* or *domain-name_local.cer*.

Description

Use **pki import-certificate** to import a CA certificate or local certificate from a file and save it locally.

Related commands: **pki domain**.

Examples

```
# Import the CA certificate for PKI domain cer in the PEM format.  
<Sysname> system-view  
[Sysname] pki import-certificate ca domain cer pem
```

pki request-certificate domain

Syntax

```
pki request-certificate domain domain-name [ password ] [ pkcs10 [ filename filename ] ]
```

View

System view

Default level

2: System level

Parameters

domain-name: Name of the PKI domain name, a string of 1 to 15 characters.

password: Password for certificate revocation, a case-sensitive string of 1 to 31 characters.

pkcs10: Displays the BASE64-encoded PKCS#10 certificate request information, which can be used to request a certification by an out-of-band means, like phone, disk, or email.

filename filename: Specifies the name of the local file for saving the PKCS#10 certificate request, a case-insensitive string of 1 to 127 characters.

Description

Use **pki request-certificate domain** to request a local certificate from a CA through SCEP. If SCEP fails, you can use the **pkcs10** keyword to print the request information in BASE64 format, or use the **pkcs10 filename filename** option to save the request information to a local file and send the file to the CA by an out-of-band means.

This operation will not be saved in the configuration file.

Related commands: **pki domain**.

Examples

Display the PKCS#10 certificate request information.

```
<Sysname> system-view
[Sysname] pki request-certificate domain 1 pkcs10
-----BEGIN CERTIFICATE REQUEST-----
MIIBTDCBtgIBADANMQswCQYDVQQDEwJqaJCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAw5Drj8ofs9THA4ezkDcQPB8pvH1kumampPsJmx8sGG52NftbrDTnTT5
ALx3LJijB3d/ndKpCHT/DfbJVDCn5gdw32tBZyCkEwMHZN3ol2z7Nvdu5TED6iN8
4m+hfp1QWoV6lty3o9pxAXuQl8peUDcfN6WV3LBXYy1lWctkLkECAwEAAaAAMA0G
CSqGSIb3DQEBBAAUAA4GBAA8E7BaIdmT6NVCZgv/I/ltqZH3TS4e4H9Qo5NiCKiEw
R8owVmA0XVtGMbyqBNcDTG0f5NbHrXZQT5+MbFJOnm5K/mn1ro5TJKMTKV46PlCZ
JUjsugaY02GBY0BVcylpC9iIXLuXNIqjh1MBIqVsa1lQOHS7YMvnop6hXAQlkM4c
-----END CERTIFICATE REQUEST-----
```

pki retrieval-certificate

Syntax

pki retrieval-certificate { ca | local } domain domain-name

View

System view

Default level

2: System level

Parameters

ca: Retrieves the CA certificate.

local: Retrieves the local certificate.

domain-name: Name of the PKI domain used for certificate request, a string of 1 to 15 characters.

Description

Use **pki retrieval-certificate** to retrieve a certificate from the server for certificate distribution.

The retrieved certificates are stored in the root directory of the switch, with the file name as *domain-name_ca.cer* or *domain-name_local.cer* according to the certificate type.

Related commands: **pki domain**.

Examples

Retrieve the CA certificate from the certificate issuing server.

```
<Sysname> system-view
```

```
[Sysname] pki retrieval-certificate ca domain 1
```

pki retrieval-crl domain

Syntax

pki retrieval-crl domain *domain-name*

View

System view

Default level

2: System level

Parameters

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

Description

Use **pki retrieval-crl domain** to retrieve the latest CRLs from the server for CRL distribution.

CRLs help examine the validity of certificates.

Related commands: **pki domain**.

Examples

Retrieve CRLs.

```
<Sysname> system-view
```

```
[Sysname] pki retrieval-crl domain 1
```

pki validate-certificate

Syntax

pki validate-certificate { ca | local } domain *domain-name*

View

System view

Default level

2: System level

Parameters

ca: Verifies the CA certificate.

local: Verifies the local certificate.

domain-name: Name of the PKI domain to which the certificate to be verified belongs, a string of 1 to 15 characters.

Description

Use **pki validate-certificate** to examine the validity of a certificate.

Certificate validity verification examines whether the certificate is signed by the CA and that the certificate has neither expired nor been revoked.

Related commands: **pki domain**.

Examples

```
# Verify the validity of the local certificate.
<Sysname> system-view
[Sysname] pki validate-certificate local domain 1
```

root-certificate fingerprint

Syntax

```
root-certificate fingerprint { md5 | sha1 } string
undo root-certificate fingerprint
```

View

PKI domain view

Default level

2: System level

Parameters

md5: Uses an MD5 fingerprint.

sha1: Uses a SHA1 fingerprint.

string: Fingerprint to be used. An MD5 fingerprint must be a string of 32 characters in hexadecimal. A SHA1 fingerprint must be a string of 40 characters in hexadecimal.

Description

Use **root-certificate fingerprint** to configure the fingerprint to be used for verifying the validity of the CA root certificate.

Use **undo root-certificate fingerprint** to remove the configuration.

By default, no fingerprint is configured for verifying the validity of the CA root certificate.

Examples

```
# Configure an MD5 fingerprint for verifying the validity of the CA root certificate.
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] root-certificate fingerprint md5
12EF53FA355CD23E12EF53FA355CD23E

# Configure a SHA1 fingerprint for verifying the validity of the CA root certificate.
[Sysname-pki-domain-1] root-certificate fingerprint sha1
D1526110AAD7527FB093ED7FC037B0B3CDDAD93
```

rule (PKI CERT ACP view)

Syntax

```
rule [ id ] { deny | permit } group-name  
undo rule { id | all }
```

View

PKI certificate access control policy view

Default level

2: System level

Parameters

id: Number of the certificate attribute access control rule, in the range of 1 to 16. The default is the smallest unused number in this range.

deny: Indicates that a certificate whose attributes match an attribute rule in the specified attribute group is considered invalid and denied.

permit: Indicates that a certificate whose attributes match an attribute rule in the specified attribute group is considered valid and permitted.

group-name: Name of the certificate attribute group to be associated with the rule, a case-insensitive string of 1 to 16 characters. It cannot be a, al, or all.

all: Specifies all access control rules.

Description

Use **rule** to create a certificate attribute access control rule.

Use **undo rule** to delete access control rules.

By default, no access control rule exists.

A certificate attribute group must exist to be associated with a rule.

Examples

```
# Create an access control rule, specifying that a certificate is considered valid when it matches an  
attribute rule in certificate attribute group mygroup.
```

```
<Sysname> system-view
```

```
[Sysname] pki certificate access-control-policy mypolicy
```

```
[Sysname-pki-cert-acp-mypolicy] rule 1 permit mygroup
```

state

Syntax

```
state state-name  
undo state
```

View

PKI entity view

Default level

2: System level

Parameters

state-name: State or province name, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use **state** to specify the name of the state or province where an entity resides.

Use **undo state** to remove the configuration.

By default, no state or province is specified.

Examples

Specify the state where an entity resides.

```
<Sysname> system-view
```

```
[Sysname] pki entity 1
```

```
[Sysname-pki-entity-1] state country
```

IPsec configuration commands

IPsec configuration commands are available only for the switches in FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

ah authentication-algorithm

Syntax

```
ah authentication-algorithm sha1  
undo ah authentication-algorithm
```

View

IPsec proposal view

Default level

2: System level

Parameters

sha1: Uses SHA1.

Description

Use the **ah authentication-algorithm** command to specify an authentication algorithm for the authentication header (AH) protocol.

Use the **undo ah authentication-algorithm** command to restore the default.

By default, SHA-1 is used.

Before specifying the authentication algorithm for AH, be sure to use the **transform** command to specify the security protocol as AH or both AH and ESP.

Related commands: **ipsec proposal** and **transform**.

Examples

```
# Configure IPsec proposal prop1 to use AH and SHA1.  
<Sysname> system-view  
[Sysname] ipsec proposal prop1  
[Sysname-ipsec-proposal-prop1] transform ah  
[Sysname-ipsec-proposal-prop1] ah authentication-algorithm sha1
```

connection-name

Syntax

```
connection-name name  
undo connection-name
```

View

IPsec policy view

Default level

2: System level

Parameters

name: IPsec connection name, a case-insensitive string of 1 to 32 characters.

Description

Use the **connection-name** command to configure an IPsec connection name. This name functions only as a description of the IPsec policy.

Use the **undo connection-name** command to restore the default.

By default, no IPsec connection name is configured.

Example

```
# Set IPsec connection name to aaa.  
<Sysname> system-view  
[Sysname] ipsec policy policy1 1 isakmp  
[Sysname-ipsec-policy-isakmp-policy1-1] connection-name aaa
```

display ipsec policy

Syntax

display ipsec policy [**brief** | **name** *policy-name* [*seq-number*]] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

brief: Displays brief information about all IPsec policies.

name: Displays detailed information about a specified IPsec policy or IPsec policy group.

policy-name: Name of the IPsec policy, a string of 1 to 15 characters.

seq-number: Sequence number of the IPsec policy, in the range 1 to 65535.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use the **display ipsec policy** command to display information about IPsec policies.

If you do not specify any parameters, the command displays detailed information about all IPsec policies.

If you specify the **name** *policy-name* option but leave the *seq-number* argument, the command displays detailed information about the specified IPsec policy group.

Related commands: **ipsec policy (system view)**.

Examples

Display brief information about all IPsec policies.

```
<Sysname> display ipsec policy brief
```

IPsec-Policy-Name	Mode	acl	ike-peer name	Mapped Template

aaa-100	manual			
policy1-1	isakmp			

IPsec-Policy-Name	Mode	acl	Local-Address	Remote-Address

aaa-100	manual			

Table 33 Output description

Field	Description
IPsec-Policy-Name	Name and sequence number of the IPsec policy separated by hyphen
Mode	Negotiation mode of the IPsec policy: <ul style="list-style-type: none">• manual—Manual mode• isakmp—IKE negotiation mode
acl	Access control list (ACL) referenced by the IPsec policy
ike-peer name	IKE peer name
Local-Address	IP address of the local end
Remote-Address	IP address of the remote end

Display detailed information about all IPsec policies.

```
<Sysname> display ipsec policy
```

```
=====
IPsec Policy Group: "aaa"
Interface:
=====
```

```
-----
IPsec policy name: "aaa"
sequence number: 100
mode: manual
-----
```

```
security data flow :
tunnel local address:
tunnel remote address:
proposal name:
inbound AH setting:
    AH spi:
```

```

    AH string-key:
    AH authentication hex key:
inbound ESP setting:
    ESP spi:
    ESP string-key:
    ESP encryption hex key:
    ESP authentication hex key:
outbound AH setting:
    AH spi:
    AH string-key:
    AH authentication hex key:
outbound ESP setting:
    ESP spi:
    ESP string-key:
    ESP encryption hex key:
    ESP authentication hex key:

=====
IPsec Policy Group: "policy1"
Interface:
=====

-----
IPsec policy name: "policy1"
sequence number: 1
mode: isakmp
-----

security data flow :
selector mode: standard
tunnel remote address:
perfect forward secrecy:
proposal name:
IPsec sa local duration(time based): 3600 seconds
IPsec sa local duration(traffic based): 1843200 kilobytes
policy enable: True

```

Table 34 Output description

Field	Description
security data flow	ACL referenced by the IPsec policy.
Interface	Interface to which the IPsec policy is applied.
sequence number	Sequence number of the IPsec policy.
mode	Negotiation mode of the IPsec policy, which can be: <ul style="list-style-type: none"> • manual—Manual mode • isakmp—IKE negotiation mode
selector mode	Data flow protection mode of the IPsec policy.
ike-peer name	IKE peer referenced by the IPsec policy.

Field	Description
tunnel local address	Local IP address of the tunnel.
tunnel remote address	Remote IP address of the tunnel.
perfect forward secrecy	Whether PFS is enabled.
proposal name	Proposal referenced by the IPsec policy.
policy enable	Whether the IPsec policy is enabled or not.
inbound/outbound AH/ESP setting	AH/ESP settings in the inbound/outbound direction, including the SPI and keys.

display ipsec proposal

Syntax

display ipsec proposal [*proposal-name*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

proposal-name: Name of a proposal, a string of 1 to 32 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use the **display ipsec proposal** command to display information about IPsec proposals.

If you do not specify any parameters, the command displays information about all IPsec proposals.

Related commands: **ipsec proposal**.

Examples

Display information about all IPsec proposals.

```
<Sysname> display ipsec proposal
```

```
IPsec proposal name: aaa
encapsulation mode: tunnel
transform: ah-new
AH protocol: authentication sha1-hmac-96
```

Table 35 Output description

Field	Description
IPsec proposal name	Name of the IPsec proposal
encapsulation mode	Encapsulation mode used by the IPsec proposal, transport or tunnel
transform	Security protocol(s) used by the IPsec proposal: AH, ESP, or both. If both protocols are configured, IPsec uses ESP before AH.
AH protocol	Authentication algorithm used by AH
ESP protocol	Authentication algorithm and encryption algorithm used by ESP

display ipsec sa

Syntax

display ipsec sa [**brief** | **policy** *policy-name* [*seq-number*] | **remote** *ip-address*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

brief: Displays brief information about all IPsec SAs.

policy: Displays detailed information about IPsec SAs created by using a specified IPsec policy.

policy-name: Name of the IPsec policy, a string 1 to 15 characters.

seq-number: Sequence number of the IPsec policy, in the range 1 to 65535.

remote *ip-address*: Displays detailed information about the IPsec SA with a specified remote address.

| : Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use the **display ipsec sa** command to display information about IPsec SAs.

If you do not specify any parameters, the command displays information about all IPsec SAs.

Related commands: **reset ipsec sa** and **ipsec sa global-duration**.

Examples

Display brief information about all IPsec SAs.

```
<Sysname> display ipsec sa brief
```

```
Src Address  Dst Address  SPI      Protocol  Algorithm
```

```

-----
10.1.1.1      10.1.1.2      300    ESP      E:AES-192;
                                     A:HMAC-SHA1-96
10.1.1.2      10.1.1.1      400    ESP      E:AES-192;
                                     A:HMAC-SHA1-96

```

Table 36 Output description

Field	Description
Src Address	Local IP address
Dst Address	Remote IP address
SPI	Security parameter index
Protocol	Security protocol used by IPsec
Algorithm	Authentication algorithm and encryption algorithm used by the security protocol, where E indicates the encryption algorithm and A indicates the authentication algorithm. A value of NULL means that type of algorithm is not specified.

Display detailed information about all IPsec SAs.

```

<Sysname> display ipsec sa
=====
Interface: Vlan-interface 1
    path MTU: 1500
=====

-----
IPsec policy name: "r2"
sequence number: 1
mode: isakmp
-----

    connection id: 3
    encapsulation mode: tunnel
    perfect forward secrecy:
    tunnel:
        local  address: 2.2.2.2
        remote address: 1.1.1.2
    flow:
        sour addr: 192.168.2.0/255.255.255.0  port: 0  protocol: IP
        dest addr: 192.168.1.0/255.255.255.0  port: 0  protocol: IP

[inbound ESP SAs]
    spi: 3564837569 (0xd47blac1)
    proposal: ESP-ENCRYPT-AES-CBC-192 ESP-AUTH-SHA1
    sa duration (kilobytes/sec): 4294967295/604800
    sa remaining duration (kilobytes/sec): 1843200/2686
    max received sequence-number: 5
    anti-replay check enable: Y
    anti-replay window size: 32
    udp encapsulation used for nat traversal: N

```



```

[outbound ESP SAs]
  spi: 801701189 (0x2fc8fd45)
  proposal: ESP-ENCRYPT-AES-CBC-192 ESP-AUTH-SHA1
  sa duration (kilobytes/sec): 4294967295/604800
  sa remaining duration (kilobytes/sec): 1843200/2686
  max sent sequence-number: 6
  udp encapsulation used for nat traversal: N

```

Table 37 Output description

Field	Description
Interface	Interface referencing the IPsec policy.
path MTU	Maximum IP packet length supported by the interface.
Protocol	Name of the protocol to which the IPsec policy is applied.
IPsec policy name	Name of IPsec policy used.
sequence number	Sequence number of the IPsec policy.
mode	IPsec negotiation mode.
connection id	IPsec tunnel identifier.
encapsulation mode	Encapsulation mode, transport or tunnel.
perfect forward secrecy	Whether the perfect forward secrecy feature is enabled.
tunnel	IPsec tunnel.
local address	Local IP address of the IPsec tunnel.
remote address	Remote IP address of the IPsec tunnel.
flow	Data flow.
sour addr	Source IP address of the data flow.
dest addr	Destination IP address of the data flow.
port	Port number.
protocol	Protocol type.
inbound	Information of the inbound SA.
spi	Security parameter index.
proposal	Security protocol and algorithms used by the IPsec proposal.
sa duration	Lifetime of the IPsec SA.
sa remaining key duration	Remaining lifetime of the SA.
max received sequence-number	Maximum sequence number of the received packets (relevant to the anti-replay function provided by the security protocol).
udp encapsulation used for nat traversal	Whether NAT traversal is enabled for the SA.
outbound	Information of the outbound SA.
max sent sequence-number	Maximum sequence number of the sent packets (relevant to the anti-replay function provided by the security protocol).

Field	Description
anti-replay check enable	Whether IPsec anti-replay checking is enabled.
anti-replay window size	Size of the anti-replay window.

display ipsec session

Syntax

display ipsec session [**tunnel-id** *integer*] [[{ **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

integer: ID of the IPsec tunnel, in the range 1 to 2000000000.

[: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use the **display ipsec session** command to display information about IPsec sessions.

If you do not specify any parameters, the command displays information about all IPsec sessions.

IPsec can find matched tunnels directly by session, reducing the intermediate matching procedures and improving the forwarding efficiency. A session is identified by the quintuplet of protocol, source IP address, source port, destination IP address, and destination port.

Related commands: **reset ipsec session**.

Examples

Display information about all IPsec sessions.

```
<Sysname> display ipsec session

-----
total sessions : 2
-----

tunnel-id : 3
session idle time/total duration (sec) : 36/300

session flow :      (8 times matched)
    Sour Addr : 15.15.15.1      Sour Port:    0  Protocol : 1
    Dest Addr : 15.15.15.2      Dest Port:    0  Protocol : 1
```

```

-----
tunnel-id : 4
session idle duration/total duration (sec) : 7/300

session flow :      (3 times matched)
    Sour Addr : 12.12.12.1          Sour Port:    0  Protocol : 1
    Dest Addr : 13.13.13.1          Dest Port:    0  Protocol : 1

# Display information about the session with an IPsec tunnel ID of 5.
<Sysname> display ipsec session tunnel-id 5
-----
total sessions : 1
-----

tunnel-id : 5
session idle time/total duration (sec) : 30/300

session flow :      (4 times matched)
    Sour Addr : 12.12.12.2          Sour Port:    0  Protocol : 1
    Dest Addr : 13.13.13.2          Dest Port:    0  Protocol : 1

```

Table 38 Output description

Field	Description
total sessions	Total number of IPsec sessions
tunnel-id	IPsec tunnel ID, same as the connection-id of the IPsec SA
session idle time	Idle duration of the IPsec session in seconds
total duration	Lifetime of the IPsec session in seconds, defaulted to 300 seconds
session flow	Flow information of the IPsec session
times matched	Total number of packets matching the IPsec session
Sour Addr	Source IP address of the IPsec session
Dest Addr	Destination IP address of the IPsec session
Sour Port	Source port number of the IPsec session
Dest Port	Destination port number of the IPsec session
Protocol	Protocol number of the IPsec protected data flow, for example, 1 for ICMP

display ipsec statistics

Syntax

```
display ipsec statistics [ tunnel-id integer ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

tunnel-id *integer*: Specifies an IPsec tunnel by its ID, which is in the range 1 to 2000000000.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use the **display ipsec statistics** command to display IPsec packet statistics.

If you do not specify any parameters, the command displays the statistics for all IPsec packets.

Related commands: **reset ipsec statistics**.

Examples

Display statistics on all IPsec packets.

```
<Sysname> display ipsec statistics
the security packet statistics:
  input/output security packets: 47/62
  input/output security bytes: 3948/5208
  input/output dropped security packets: 0/45
  dropped security packet detail:
    not enough memory: 0
    can't find SA: 45
    queue is full: 0
    authentication has failed: 0
    wrong length: 0
    replay packet: 0
    packet too long: 0
    wrong SA: 0
```

Table 39 Output description

Field	Description
Connection ID	ID of the tunnel
input/output security packets	Counts of inbound and outbound IPsec protected packets
input/output security bytes	Counts of inbound and outbound IPsec protected bytes
input/output dropped security packets	Counts of inbound and outbound IPsec protected packets that are discarded by the device
dropped security packet detail	Detailed information about inbound/outbound packets that get dropped
not enough memory	Number of packets dropped due to lack of memory
can't find SA	Number of packets dropped due to finding no security association
queue is full	Number of packets dropped due to full queues

Field	Description
authentication has failed	Number of packets dropped due to authentication failure
wrong length	Number of packets dropped due to wrong packet length
replay packet	Number of packets replayed
packet too long	Number of packets dropped due to excessive packet length
wrong SA	Number of packets dropped due to improper SA

display ipsec tunnel

Syntax

display ipsec tunnel [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use the **display ipsec tunnel** command to display information about IPsec tunnels.

Examples

Display information about IPsec tunnels.

```
<Sysname> display ipsec tunnel
total tunnel : 2
-----
connection id: 3
perfect forward secrecy:
SA's SPI:
    inbound:  187199087 (0xb286e6f) [ESP]
    outbound: 3562274487 (0xd453feb7) [ESP]
tunnel:
    local  address:  44.44.44.44
    remote address : 44.44.44.55
flow:
    sour addr : 44.44.44.0/255.255.255.0  port: 0  protocol : IP
    dest addr : 44.44.44.0/255.255.255.0  port: 0  protocol : IP
current Encrypt-card: None
```

```

-----
connection id: 5
perfect forward secrecy:
SA's SPI:
    inbound: 12345 (0x3039) [ESP]
    outbound: 12345 (0x3039) [ESP]
tunnel:
flow:
current Encrypt-card:

```

Table 40 Output description

Field	Description
connection id	Connection ID, used to uniquely identify an IPsec Tunnel
perfect forward secrecy	Perfect forward secrecy, indicating which DH group is to be used for fast negotiation mode in IKE phase 2
SA's SPI	SPIs of the inbound and outbound SAs
tunnel	Local and remote addresses of the tunnel
flow	Data flow protected by the IPsec tunnel, including source IP address, destination IP address, source port, destination port and protocol
as defined in acl 3001	The IPsec tunnel protects all data flows defined by ACL 3001
current Encrypt-card	Encryption card interface used by the current tunnel

encapsulation-mode

Syntax

```

encapsulation-mode { transport | tunnel }
undo encapsulation-mode

```

View

IPsec proposal view

Default level

2: System level

Parameters

transport: Uses transport mode.

tunnel: Uses tunnel mode.

Description

Use the **encapsulation-mode** command to set the encapsulation mode that the security protocol uses to encapsulate IP packets.

Use the **undo encapsulation-mode** command to restore the default.

By default, a security protocol encapsulates IP packets in tunnel mode.

Related commands: **ipsec proposal**.

Examples

```
# Configure IPsec proposal prop2 to encapsulate IP packets in transport mode.
<Sysname> system-view
[Sysname] ipsec proposal prop2
[Sysname-ipsec-proposal-prop2] encapsulation-mode transport
```

esp authentication-algorithm

Syntax

```
esp authentication-algorithm sha1
undo esp authentication-algorithm
```

View

IPsec proposal view

Default level

2: System level

Parameters

sha1: Uses the SHA1 algorithm, which uses a 160-bit key.

Description

Use the **esp authentication-algorithm** command to specify an authentication algorithm for ESP.

Use the **undo esp authentication-algorithm** command to configure ESP not to perform authentication on packets.

By default, SHA-1 is used.

You must use both ESP authentication and encryption.

For ESP, you must specify an encryption algorithm, an authentication algorithm, or both. The **undo esp authentication-algorithm** command takes effect only if one encryption algorithm is specified for ESP.

Related commands: **ipsec proposal**, **esp encryption-algorithm**, **proposal**, and **transform**.

Examples

```
# Configure IPsec proposal prop1 to use ESP and specify SHA1 as the authentication algorithm for ESP.
<Sysname> system-view
[Sysname] ipsec proposal prop1
[Sysname-ipsec-proposal-prop1] transform esp
[Sysname-ipsec-proposal-prop1] esp authentication-algorithm sha1
```

esp encryption-algorithm

Syntax

```
esp encryption-algorithm aes [ key-length ]
undo esp encryption-algorithm
```

View

IPsec proposal view

Default level

2: System level

Parameters

aes: Uses the Advanced Encryption Standard (AES) in CBC mode as the encryption algorithm. The AES algorithm uses a 128-bit, 192-bit, or 256-bit key for encryption.

key-length: Key length for the AES algorithm, which can be 128, 192, and 256 and defaults to 128. This argument is for AES only.

Description

Use the **esp encryption-algorithm** command to specify an encryption algorithm for ESP.

Use the **undo esp encryption-algorithm** command to configure ESP not to encrypt packets.

By default, AES-128 is used.

You must use both ESP authentication and encryption.

For ESP, you must specify an encryption algorithm, an authentication algorithm, or both. The **undo esp encryption-algorithm** command takes effect only if one authentication algorithm is specified for ESP.

Related commands: **ipsec proposal**, **esp authentication-algorithm**, **proposal**, and **transform**.

Examples

Configure IPsec proposal prop1 to use ESP and specify AES as the encryption algorithm for ESP.

```
<Sysname> system-view
[Sysname] ipsec proposal prop1
[Sysname-ipsec-proposal-prop1] transform esp
[Sysname-ipsec-proposal-prop1] esp encryption-algorithm aes
```

ike-peer (IPsec policy view)

Syntax

ike-peer *peer-name*

undo ike-peer *peer-name*

View

IPsec policy view

Default level

2: System level

Parameters

peer-name: IKE peer name, a string of 1 to 32 characters.

Description

Use the **ike-peer** command to reference an IKE peer in an IPsec policy configured through IKE negotiation.

Use the **undo ike peer** command to remove the reference.

This command applies to only IKE negotiation mode.

Related commands: **ipsec policy**.

Examples

```
# Configure a reference to an IKE peer in an IPsec policy.
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] ike-peer peer1
```

ipsec anti-replay check

Syntax

```
ipsec anti-replay check
undo ipsec anti-replay check
```

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ipsec anti-replay check** command to enable IPsec anti-replay checking.

Use the **undo ipsec anti-replay check** command to disable IPsec anti-replay checking.

By default, IPsec anti-replay checking is enabled.

Examples

```
# Enable IPsec anti-replay checking.
<Sysname> system-view
[Sysname] ipsec anti-replay check
```

ipsec anti-replay window

Syntax

```
ipsec anti-replay window width
undo ipsec anti-replay window
```

View

System view

Default level

2: System level

Parameters

width: Size of the anti-replay window. It can be 32, 64, 128, 256, 512, or 1024.

Description

Use the **ipsec anti-replay window** command to set the size of the anti-replay window.

Use the **undo ipsec anti-replay window** command to restore the default.

By default, the size of the anti-replay window is 32.
Your configuration affects only IPsec SAs negotiated later.

Examples

```
# Set the size of the anti-replay window to 64.  
<Sysname> system-view  
[Sysname] ipsec anti-replay window 64
```

ipsec decrypt check

Syntax

```
ipsec decrypt check  
undo ipsec decrypt check
```

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ipsec decrypt check** command to enable ACL checking of de-encapsulated IPsec packets.
Use the **undo ipsec decrypt check** command to disable ACL checking of de-encapsulated IPsec packets.
By default, ACL checking of de-encapsulated IPsec packets is enabled.

Examples

```
# Enable ACL checking of de-encapsulated IPsec packets.  
<Sysname> system-view  
[Sysname] ipsec decrypt check
```

ipsec policy (interface view)

Syntax

```
ipsec policy policy-name  
undo ipsec policy [ policy-name ]
```

View

Interface view

Default level

2: System level

Parameters

policy-name: Name of the existing IPsec policy group to be applied to the interface, a string of 1 to 15 characters.

Description

Use the **ipsec policy** command to apply an IPsec policy group to an interface.

Use the **undo ipsec policy** command to remove the application.

IPsec policies can be applied only to VLAN interfaces on the switch.

Only one IPsec policy group can be applied to an interface. To apply another IPsec policy group to the interface, remove the original application first. An IPsec policy can be applied to only one interface.

With an IPsec policy group applied to an interface, the system uses each IPsec policy in the group to protect certain data flows.

For each packet to be sent out an IPsec protected interface, the system checks the IPsec policies of the IPsec policy group in the ascending order of sequence numbers. If it finds an IPsec policy whose ACL matches the packet, it uses the IPsec policy to protect the packet. If it finds no ACL of the IPsec policies matches the packet, it does not provide IPsec protection for the packet and sends the packet out directly.

Related commands: **ipsec policy (system view)**.

Examples

```
# Apply IPsec policy group pg1 to interface VLAN-interface 1.
```

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 1
```

```
[Sysname-Vlan-interface1] ipsec policy pg1
```

ipsec policy (system view)

Syntax

ipsec policy *policy-name* *seq-number* [**isakmp** | **manual**]

undo ipsec policy *policy-name* [*seq-number*]

View

System view

Default level

2: System level

Parameters

policy-name: Name for the IPsec policy, a case-insensitive string of 1 to 15 characters, including letters and digits. No minus sign (-) can be included.

seq-number: Sequence number for the IPsec policy, in the range of 1 to 65535.

isakmp: Sets up SAs through IKE negotiation.

manual: Sets up SAs manually.

Description

Use the **ipsec policy** command to create an IPsec policy and enter its view.

Use the **undo ipsec policy** command to delete the specified IPsec policies.

By default, no IPsec policy exists.

When creating an IPsec policy, you must specify the generation mode.

You cannot change the generation mode of an existing IPsec policy; you can only delete the policy and then re-create it with the new mode.

IPsec policies with the same name constitute an IPsec policy group. An IPsec policy is identified uniquely by its name and sequence number. In an IPsec policy group, an IPsec policy with a smaller sequence number has a higher priority.

The **undo ipsec policy** command without the *seq-number* argument deletes an IPsec policy group.

Related commands: **ipsec policy (interface view)** and **display ipsec policy**.

Examples

Create an IPsec policy with the name **policy1** and sequence number **100**, and specify to set up SAs through IKE negotiation.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100]
```

Create an IPsec policy with the name **policy1** and specify the manual mode for it.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 101 manual
[Sysname-ipsec-policy-manual-policy1-101]
```

ipsec proposal

Syntax

ipsec proposal *proposal-name*

undo ipsec proposal *proposal-name*

View

System view

Default level

2: System level

Parameters

proposal-name: Name for the proposal, a case-insensitive string of 1 to 32 characters .

Description

Use the **ipsec proposal** command to create an IPsec proposal and enter its view.

Use the **undo ipsec proposal** command to delete an IPsec proposal.

By default, no IPsec proposal exists.

IPsec proposal created by using the **ipsec proposal** command takes the security protocol of ESP, the encryption algorithm of AES-128, and the authentication algorithm of SHA1 by default.

Related commands: **display ipsec proposal**.

Examples

Create an IPsec proposal named **newprop1**.

```
<Sysname> system-view
[Sysname] ipsec proposal newprop1
```

ipsec sa global-duration

Syntax

```
ipsec sa global-duration { time-based seconds | traffic-based kilobytes }  
undo ipsec sa global-duration { time-based | traffic-based }
```

View

System view

Default level

2: System level

Parameters

seconds: Time-based global SA lifetime in seconds, in the range 180 to 604800.

kilobytes: Traffic-based global SA lifetime in kilobytes, in the range 2560 to 4294967295.

Description

Use the **ipsec sa global-duration** command to configure the global SA lifetime.

Use the **undo ipsec sa global-duration** command to restore the default.

By default, the time-based global SA lifetime is 3600 seconds, and the traffic-based global SA lifetime is 1843200 kilobytes.

When negotiating to set up an SA, IKE prefers the lifetime of the IPsec policy that it uses. If the IPsec policy is not configured with its own lifetime, IKE uses the global SA lifetime.

When negotiating to set up an SA, IKE prefers the shorter one of the local lifetime and that proposed by the remote.

You can configure both a time-based lifetime and a traffic-based lifetime. An SA expires when either lifetime expires.

The SA lifetime applies to only IKE negotiated SAs. It is not effective for manually configured SAs.

If IPsec uses IKE automatic negotiation, when IPsec SAs reach the traffic-based lifetime, IPsec notifies IKE to re-perform phase 1 and phase 2 negotiations.

Related commands: **sa duration**.

Examples

Set the time-based global SA lifetime to 7200 seconds (2 hours).

```
<Sysname> system-view
```

```
[Sysname] ipsec sa global-duration time-based 7200
```

Set the traffic-based global SA lifetime to 10240 kilobytes (10 Mbytes).

```
[Sysname] ipsec sa global-duration traffic-based 10240
```

ipsec session idle-time

Syntax

```
ipsec session idle-time seconds  
undo ipsec session idle-time
```

View

System view

Default level

2: System level

Parameters

Seconds: IPsec session idle timeout in seconds, in the range of 60 to 3,600.

Description

Use the **ipsec session idle-time** command to set the idle timeout for IPsec sessions.

Use the **undo ipsec session idle-time** command to restore the default.

By default, the IPsec session idle timeout is 300 seconds.

Examples

Set the IPsec session idle timeout to 600 seconds.

```
<Sysname> system-view
```

```
[Sysname] ipsec session idle-time 600
```

pfs

Syntax

pfs { dh-group2 | dh-group5 | dh-group14 }

undo pfs

View

IPsec policy view

Default level

2: System level

Parameters

dh-group2: Uses 1024-bit Diffie-Hellman group.

dh-group5: Uses 1536-bit Diffie-Hellman group.

dh-group14: Uses 2048-bit Diffie-Hellman group.

Description

Use the **pfs** command to enable and configure the perfect forward secrecy (PFS) feature so that the system uses the feature when employing the IPsec policy to initiate a negotiation.

Use the **undo pfs** command to remove the configuration.

By default, the PFS feature is not used for negotiation.

In terms of security and necessary calculation time, the following four groups are in the descending order: 2048-bit Diffie-Hellman group (**dh-group14**), 1536-bit Diffie-Hellman group (**dh-group5**), and 1024-bit Diffie-Hellman group (**dh-group2**).

This command allows IPsec to perform an additional key exchange process during the negotiation phase 2, providing an additional level of security.

The local Diffie-Hellman group must be the same as that of the peer.

Related commands: **ipsec policy (system view)**.

Examples

```
# Enable and configure PFS for IPsec policy policy1.
<Sysname> system-view
[Sysname] ipsec policy policy1 200 isakmp
[Sysname-ipsec-policy-isakmp-policy1-200] pfs dh-group2
```

policy enable

Syntax

policy enable
undo policy enable

View

IPsec policy view

Default level

2: System level

Parameters

None

Description

Used the **policy enable** command to enable the IPsec policy.

Use the **undo policy enable** command to disable the IPsec policy.

By default, the IPsec policy is enabled.

If the IPsec policy is not enabled for the IKE peer, the peer cannot take part in the IKE negotiation.

Related commands: **ipsec policy (system view)**.

Examples

```
# Enable the IPsec policy with the name policy1 and sequence number 100.
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] policy enable
```

proposal (IPsec policy view)

Syntax

proposal *proposal-name*&<1-6>
undo proposal [*proposal-name*]

View

IPsec policy view

Default level

2: System level

Parameters

proposal-name&<1-6>: Name of the IPsec proposal, a string of 1 to 32 characters. &<1-6> means that you can specify the *proposal-name* argument for up to six times.

Description

Use the **proposal** command to specify an IPsec proposal for the IPsec policy to reference.

Use the **undo proposal** command to remove an IPsec proposal reference by the IPsec policy .

By default, an IPsec policy references no IPsec proposal.

The IPsec proposals must already exist.

A manual IPsec policy can reference only one IPsec proposal. To replace a referenced IPsec proposal, use the **undo proposal** command to remove the original proposal binding and then use the **proposal** command to reconfigure one.

An IKE negotiated IPsec policy can reference up to six IPsec proposals. The IKE negotiation process will search for and use the exactly matched proposal.

Related commands: **ipsec proposal**, **ipsec policy (system view)**.

Examples

```
# Configure IPsec policy policy1 to reference IPsec proposal prop1.
<Sysname> system-view
[Sysname] ipsec proposal prop1
[Sysname-ipsec-proposal-prop1] quit
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] proposal prop1
```

qos pre-classify

Syntax

qos pre-classify

undo qos pre-classify

View

IPsec policy view

Default level

2: System level

Parameters

None

Description

Use the **qos pre-classify** command to enable packet information pre-extraction.

Use the **undo qos pre-classify** command to restore the default.

By default, packet information pre-extraction is disabled.

With the packet information pre-extraction feature enabled, QoS classifies a packet based on the header of the original IP packet—the header of the IP packet that has not been encapsulated by IPsec.

Related commands: **ipsec policy (system view)**.

Examples

```
# Enable packet information pre-extraction.
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] qos pre-classify
```

reset ipsec sa

Syntax

reset ipsec sa [**parameters** *dest-address protocol spi* | **policy** *policy-name* [*seq-number*] | **remote** *ip-address*]

View

User view

Default level

2: System level

Parameters

parameters: Specifies IPsec SAs that use the specified destination IP address, security protocol, and SPI.

dest-address: Destination address, in dotted decimal notation.

protocol: Security protocol, which can be keyword **ah** or **esp**, case insensitive.

spi: Security parameter index in the range 256 to 4294967295.

policy: Specifies IPsec SAs that use an IPsec policy.

policy-name: Name of the IPsec policy, a case-insensitive string of 1 to 15 characters, including letters and digits.

seq-number: Sequence number of the IPsec policy, in the range 1 to 65535. If no *seq-number* is specified, all the policies in the IPsec policy group named *policy-name* are specified.

remote: Specifies SAs to or from a remote address, in dotted decimal notation.

Description

Use the **reset ipsec sa** command to clear IPsec SAs.

Immediately after a manually set up SA is cleared, the system automatically sets up a new SA based on the parameters of the IPsec policy. After IKE negotiated SAs are cleared, the system sets up new SAs only when IKE negotiation is triggered by interesting packets.

IPsec SAs appear in pairs. If you specify the **parameters** keyword to clear an IPsec SA, the IPsec SA in the other direction is also automatically cleared.

If you do not specify any parameter, the command clears all IPsec SAs.

Related commands: **display ipsec sa**.

Examples

```
# Clear all IPsec SAs.
<Sysname> reset ipsec sa

# Clear the IPsec SA with a remote IP address of 10.1.1.2.
<Sysname> reset ipsec sa remote 10.1.1.2

# Clear the IPsec SA of the IPsec policy with the name of policy1 and sequence number of 10.
<Sysname> reset ipsec sa policy policy1 10

# Clear the IPsec SA with a remote IP address of 10.1.1.2, security protocol of AH, and SPI of 10000.
<Sysname> reset ipsec sa parameters 10.1.1.2 ah 10000
```

reset ipsec session

Syntax

```
reset ipsec session [ tunnel-id integer ]
```

View

User view

Default level

2: System level

Parameters

integer: ID of the IPsec tunnel, in the range 1 to 20000000000.

Description

Use the **reset ipsec session** command to clear the sessions of a specified IPsec tunnel or all IPsec tunnels.

Related commands: **display ipsec session**.

Examples

```
# Clear all IPsec sessions.
<Sysname> reset ipsec session

# Clear the sessions of IPsec tunnel 5.
<Sysname> reset ipsec session tunnel-id 5
```

reset ipsec statistics

Syntax

```
reset ipsec statistics
```

View

User view

Default level

2: System level

Parameters

None

Description

Use the **reset ipsec statistics** command to clear IPsec packet statistics.

Related commands: **display ipsec statistics**.

Examples

```
# Clear IPsec packet statistics.  
<Sysname> reset ipsec statistics
```

sa authentication-hex

Syntax

```
sa authentication-hex { inbound | outbound } { ah | esp } [ cipher | simple ] hex-key  
undo sa authentication-hex { inbound | outbound } { ah | esp }
```

View

IPsec policy view

Default level

2: System level

Parameters

inbound: Specifies the inbound SA through which IPsec processes the received packets.

outbound: Specifies the outbound SA through which IPsec processes the packets to be sent.

ah: Uses AH.

esp: Uses ESP.

cipher: Sets a ciphertext authentication key.

simple: Sets a plaintext authentication key.

hex-key: Authentication key for the SA. The *hex-key* argument is a case-sensitive ciphertext string of 8 to 85 characters when the **cipher** keyword is specified, or a case-insensitive plaintext hexadecimal string when the **simple** keyword is specified. The plaintext string must be a 20-byte hexadecimal string for SHA1. If neither **cipher** nor **simple** is specified, you set a plaintext authentication key string.

Description

Use the **sa authentication-hex** command to configure an authentication key for an SA.

Use the **undo sa authentication-hex** command to remove the configuration.

When configuring a manual IPsec policy, you must set the parameters of both the inbound and outbound SAs.

The authentication key for the inbound SA at the local end must be the same as that for the outbound SA at the remote end, and the authentication key for the outbound SA at the local end must be the same as that for the inbound SA at the remote end.

At both ends of an IPsec tunnel, the keys for the inbound and outbound SAs must be in the same format.

Related commands: **ipsec policy (system view)**.

Examples

```
# Configure the authentication keys of the inbound and outbound SAs that use AH as  
0x112233445566778899aabbccddeeff00 and 0xaabbccddeeff001100aabbccddeeff00, respectively.
```

```

<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa authentication-hex inbound ah
112233445566778899aabbccddeeff00
[Sysname-ipsec-policy-manual-policy1-100] sa authentication-hex outbound ah
aabbccddeeff001100aabbccddeeff00

```

sa duration

Syntax

```

sa duration { time-based seconds | traffic-based kilobytes }
undo sa duration { time-based | traffic-based }

```

View

IPsec policy view

Default level

2: System level

Parameters

seconds: Time-based SA lifetime in seconds, in the range 180 to 604800.

kilobytes: Traffic-based SA lifetime in kilobytes, in the range 2560 to 4294967295.

Description

Use the **sa duration** command to set an SA lifetime for the IPsec policy.

Use the **undo sa duration** command to restore the default.

By default, the SA lifetime of an IPsec policy equals the current global SA lifetime.

By default, the time-based global SA lifetime is 3600 seconds, and traffic-based SA lifetime is 1843200 kilobytes.

When negotiating to set up an SA, IKE prefers the lifetime settings of the IPsec policy that it uses. If the IPsec policy or IPsec proposal is not configured with its own lifetime settings, IKE uses the global SA lifetime settings, which are configured with the **ipsec sa global-duration** command.

When negotiating to set up an SA, IKE prefers the shorter ones of the local lifetime settings and those proposed by the remote.

The SA lifetime applies to only IKE negotiated SAs. It is not effective for manually configured SAs.

If IPsec uses IKE automatic negotiation, when IPsec SAs reach the traffic-based lifetime, the system notifies IKE to re-perform phase 1 and phase 2 negotiations.

Related commands: **ipsec sa global-duration**, **ipsec policy (system view)**.

Examples

Set the SA lifetime for IPsec **policy1** to 7200 seconds (two hours).

```

<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] sa duration time-based 7200

```

Set the SA lifetime for IPsec policy **policy1** to 20480 kilobytes (20 Mbytes).

```

<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp

```

[Sysname-ipsec-policy-isakmp-policy1-100] sa duration traffic-based 20480

sa encryption-hex

Syntax

sa encryption-hex { **inbound** | **outbound** } **esp** [**cipher** | **simple**] *hex-key*

undo sa encryption-hex { **inbound** | **outbound** } **esp**

View

IPsec policy view

Default level

2: System level

Parameters

inbound: Specifies the inbound SA through which IPsec processes the received packets.

outbound: Specifies the outbound SA through which IPsec processes the packets to be sent.

esp: Uses ESP.

cipher *string-key*: Sets a ciphertext encryption key.

simple *hex-key*: Sets a plaintext encryption key.

hex-key: Encryption key for the SA. The *hex-key* argument is a case-sensitive ciphertext string of 8 to 117 characters when the **cipher** keyword is specified, or a case-insensitive plaintext hexadecimal string when the **simple** keyword is specified. The plaintext string must be a 16-byte hexadecimal string for AES128-CBC, a 24-byte hexadecimal string for AES192-CBC, or a 32-byte hexadecimal string for AES256-CBC. If neither **cipher** nor **simple** is specified, you set a plaintext encryption key string.

Description

Use the **sa encryption-hex** command to configure an encryption key for an SA.

Use the **undo sa encryption-hex** command to remove the configuration.

When configuring a manual IPsec policy, you must set the parameters of both the inbound and outbound SAs.

The encryption key for the inbound SA at the local end must be the same as that for the outbound SA at the remote end, and the encryption key for the outbound SA at the local end must be the same as that for the inbound SA at the remote end.

At both ends of an IPsec tunnel, the keys for the inbound and outbound SAs must be in the same format.

Related commands: **ipsec policy (system view)**.

Examples

Configure the encryption keys for the inbound and outbound SAs that use ESP as 0x1234567890abcdef and 0xabcdefabcdef1234, respectively.

```
<Sysname> system-view
```

```
[Sysname] ipsec policy policy1 100 manual
```

```
[Sysname-ipsec-policy-manual-policy1-100] sa encryption-hex inbound esp 1234567890abcdef
```

```
[Sysname-ipsec-policy-manual-policy1-100] sa encryption-hex outbound esp  
abcdefabcdef1234
```

sa spi

Syntax

sa spi { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*

undo sa spi { **inbound** | **outbound** } { **ah** | **esp** }

View

IPsec policy view

Default level

2: System level

Parameters

inbound: Specifies the inbound SA through which IPsec processes the received packets.

outbound: Specifies the outbound SA through which IPsec processes the packets to be sent.

ah: Uses AH.

esp: Uses ESP.

spi-number: Security parameters index (SPI) in the SA triplet, in the range 256 to 4294967295.

Description

Use the **sa spi** command to configure an SPI for an SA.

Use the **undo sa spi** command to remove the configuration.

When configuring a manual IPsec policy, you must configure parameters for both inbound and outbound SAs, and make sure that you specify different SPIs for different SAs.

The local inbound SA must use the same SPI and keys as the remote outbound SA. The same is true of the local outbound SA and remote inbound SA.

Related commands: **ipsec policy (system view)**.

Examples

Set the SPI for the inbound SA to 10000 and that for the outbound SA to 20000 in a manual IPsec policy.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa spi inbound ah 10000
[Sysname-ipsec-policy-manual-policy1-100] sa spi outbound ah 20000
```

security acl

Syntax

security acl *acl-number*

undo security acl

View

IPsec policy view

Default level

2: System level

Parameters

acl-number: Number of the ACL for the IPsec policy to reference, in the range 3000 to 3999.

Description

Use the **security acl** command to specify the ACL for the IPsec policy to reference.

Use the **undo security acl** command to remove the configuration.

By default, an IPsec policy references no ACL.

With an IKE-dependent IPsec policy configured, data flows can be protected in standard mode. In standard mode, one tunnel protects one data flow. The data flow permitted by each ACL rule is protected by one tunnel that is established separately for it.

When you specify an ACL for an IPsec policy, note these guidelines:

- You must create a mirror image ACL rule at the remote end for each ACL rule created at the local end. Otherwise, IPsec may protect traffic in only one direction.
- The ACL cannot be deployed to an aggregate interface or a tunnel interface.
- You cannot specify multiple ACLs for one IPsec policy or one ACL for multiple IPsec policies. To configure ACL rules you want to deploy for an IPsec policy, you must configure all of them in one ACL and specify the ACL for the IPsec policy.
- You can specify only one ACL for an IPsec policy. To deploy multiple ACL rules, configure the ACL rules in one ACL, and then reference the ACL in an IPsec policy.
- ACLs referenced by IPsec cannot be used by other services.

Related commands: **ipsec policy (system view)**.

Examples

Configure IPsec policy policy1 to reference ACL 3001.

```
<Sysname> system-view
[Sysname] acl number 3001
[Sysname-acl-adv-3001] rule permit tcp source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[Sysname-acl-adv-3001] quit
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] security acl 3001
```

transform

Syntax

transform { ah | ah-esp | esp }

undo transform

View

IPsec proposal view

Default level

2: System level

Parameters

ah: Uses the AH protocol.

ah-esp: Uses ESP first and then AH.

esp: Uses the ESP protocol.

Description

Use the **transform** command to specify a security protocol for an IPsec proposal.

Use the **undo transform** command to restore the default.

By default, the ESP protocol is used.

- If AH is used, the default authentication algorithm is SHA1.
- If ESP is used, the default encryption and authentication algorithms are AES-128 and SHA1, respectively.
- If both AH and ESP are used, AH uses the SHA1 authentication algorithm by default, and ESP uses the AES-128 encryption algorithm and the SHA1 authentication algorithm by default.

The IPsec proposals at the two ends of an IPsec tunnel must use the same security protocol.

Related commands: **ipsec proposal**.

Examples

```
# Configure IPsec proposal prop1 to use AH.  
<Sysname> system-view  
[Sysname] ipsec proposal prop1  
[Sysname-ipsec-proposal-prop1] transform ah
```

tunnel local

Syntax

tunnel local *ip-address*

undo tunnel local

View

IPsec policy view

Default level

2: System level

Parameters

ip-address: Local address for the IPsec tunnel.

Description

Use the **tunnel local** command to configure the local address of an IPsec tunnel.

Use the **undo tunnel local** command to remove the configuration.

By default, no local address is configured for an IPsec tunnel.

The local address, if not configured, will be the address of the interface to which the IPsec policy is applied.

Related commands: **ipsec policy (system view)**.

Examples

```
# Set the local address of the IPsec tunnel to the address of Loopback 0, 10.0.0.1.
```



```

<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-LoopBack0] ip address 10.0.0.1 32
[Sysname-LoopBack0] quit
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] tunnel local 10.0.0.1

```

tunnel remote

Syntax

```

tunnel remote ip-address
undo tunnel remote [ ip-address ]

```

View

IPsec policy view

Default level

2: System level

Parameters

ip-address: Remote address for the IPsec tunnel.

Description

Use the **tunnel remote** command to configure the remote address of an IPsec tunnel.

Use the **undo tunnel remote** command to remove the configuration.

By default, no remote address is configured for the IPsec tunnel.

If you configure the remote address repeatedly, the last one takes effect.

An IPsec tunnel is established between the local and remote ends. The remote IP address of the local end must be the same as that of the local IP address of the remote end.

Related commands: **ipsec policy (system view)**.

Examples

```

# Set the remote address of the IPsec tunnel to 10.1.1.2.
<Sysname> system-view
[Sysname] ipsec policy policy1 10 manual
[Sysname-ipsec-policy-policy1-10] tunnel remote 10.1.1.2

```

IKE configuration commands

IKE configuration commands are available only for the switches in FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

authentication-algorithm

Syntax

```
authentication-algorithm sha  
undo authentication-algorithm
```

View

IKE proposal view

Default level

2: System level

Parameters

sha: Uses HMAC-SHA1.

Description

Use the **authentication-algorithm** command to specify an authentication algorithm for an IKE proposal.

Use the **undo authentication-algorithm** command to restore the default.

By default, an IKE proposal uses the SHA1 authentication algorithm.

Related commands: **ike proposal** and **display ike proposal**.

Examples

```
# Set SHA1 as the authentication algorithm for IKE proposal 10.  
<Sysname> system-view  
[Sysname] ike proposal 10  
[Sysname-ike-proposal-10] authentication-algorithm sha
```

authentication-method

Syntax

```
authentication-method { pre-share | rsa-signature }  
undo authentication-method
```

View

IKE proposal view

Default level

2: System level

Parameters

pre-share: Uses the pre-shared key method.

rsa-signature: Uses the RSA digital signature method.

Description

Use the **authentication-method** command to specify an authentication method for an IKE proposal.

Use the **undo authentication-method** command to restore the default.

By default, an IKE proposal uses the pre-shared key authentication method.

Related commands: **ike proposal** and **display ike proposal**.

Examples

Specify that IKE proposal 10 uses the pre-shared key authentication method.

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] authentication-method pre-share
```

certificate domain

Syntax

certificate domain *domain-name*

undo certificate domain

View

IKE peer view

Default level

2: System level

Parameters

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

Description

Use the **certificate domain** command to configure the PKI domain of the certificate when IKE uses digital signature as the authentication mode.

Use the **undo certificate domain** command to remove the configuration.

Related commands: **authentication-method** and **pki domain**.

Examples

Configure the PKI domain as **abcde** for IKE negotiation.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] certificate domain abcde
```

dh

Syntax

dh { group2 | group5 | group14 }

undo dh

View

IKE proposal view

Default level

2: System level

Parameters

group2: Uses the 1024-bit Diffie-Hellman group for key negotiation in phase 1.

group5: Uses the 1536-bit Diffie-Hellman group for key negotiation in phase 1.

group14: Uses the 2048-bit Diffie-Hellman group for key negotiation in phase 1.

Description

Use the **dh** command to specify the DH group to be used in key negotiation phase 1 for an IKE proposal.

Use the **undo dh** command to restore the default.

By default, group2, the 1024-bit Diffie-Hellman group, is used.

Related commands: **ike proposal** and **display ike proposal**.

Examples

Specify 1536-bit Diffie-Hellman for IKE proposal 10.

```
<Sysname> system-view
```

```
[Sysname] ike proposal 10
```

```
[Sysname-ike-proposal-10] dh group5
```

display ike dpd

Syntax

```
display ike dpd [ dpd-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

dpd-name: DPD name, a string of 1 to 32 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use the **display ike dpd** command to display information about Dead Peer Detection (DPD) detectors.

If you do not specify any parameters, the command displays information about all DPD detectors.

Related commands: **ike dpd**.

Examples

Display information about all DPD detectors.

```
<Sysname> display ike dpd
```

```
-----  
IKE dpd: dpd1  
  references: 1  
  interval-time: 10  
  time_out: 5  
-----
```

Table 41 Output description

Field	Description
references	Number of IKE peers that use the DPD detector
Interval-time	DPD query triggering interval in seconds
time_out	DPD packet retransmission interval in seconds

display ike peer

Syntax

```
display ike peer [ peer-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

peer-name: Name of the IKE peer, a string of 1 to 32 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use the **display ike peer** command to display information about IKE peers.

If you do not specify any parameters, the command displays information about all IKE peers.

Related commands: **ike peer**.

Examples

Display information about all IKE peers.

```
<Sysname> display ike peer
```

```
-----  
IKE Peer: aaa  
  exchange mode: main on phase 1  
  peer id type: ip  
  peer ip address: 0.0.0.0 ~ 255.255.255.255  
  local ip address:  
  peer name:  
  nat traversal: disable  
  dpd:  
-----
```

Table 42 Output description

Field	Description
exchange mode	IKE negotiation mode in phase 1
pre-shared-key	Pre-shared key used in phase 1
peer id type	ID type used in phase 1
peer ip address	IP address of the remote security gateway
local ip address	IP address of the local security gateway
peer name	Name of the remote security gateway
nat traversal	Whether NAT traversal is enabled
dpd	Name of the peer DPD detector

display ike proposal

Syntax

```
display ike proposal [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use the **display ike proposal** command to view the settings of all IKE proposals.

This command displays the configuration information of all IKE proposals in the descending order of proposal priorities.

Related commands: **authentication-method**, **ike proposal**, **encryption-algorithm**, **authentication-algorithm**, **dh**, and **sa duration**.

Examples

Display the settings of all IKE proposals.

```
<Sysname> display ike proposal
priority authentication authentication encryption Diffie-Hellman duration
                method      algorithm    algorithm    group        (seconds)
-----
  11      PRE_SHARED    SHA        AES_CBC_128  MODP_1024    86400
 default PRE_SHARED    SHA        AES_CBC_128  MODP_1024    86400
```

Table 43 Output description

Field	Description
priority	Priority of the IKE proposal
authentication method	Authentication method used by the IKE proposal
authentication algorithm	Authentication algorithm used by the IKE proposal
encryption algorithm	Encryption algorithm used by the IKE proposal
Diffie-Hellman group	DH group used in IKE negotiation phase 1
duration (seconds)	ISAKMP SA lifetime of the IKE proposal in seconds

display ike sa

Syntax

```
display ike sa [ verbose [ connection-id connection-id | remote-address remote-address ] ] [ | { begin
| exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

verbose: Displays detailed information.

connection-id connection-id: Displays detailed information about IKE SAs by connection ID, in the range 1 to 2000000000.

remote: Displays detailed information about IKE SAs with a specified remote address.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use the **display ike sa** command to display information about the current IKE SAs.

If you do not specify any parameters or keywords, the command displays brief information about the current IKE SAs.

Related commands: **ike proposal** and **ike peer**.

Examples

Display brief information about the current IKE SAs.

```
<Sysname> display ike sa
  total phase-1 SAs: 1
  connection-id  peer          flag          phase   doi
  -----
    1            202.38.0.2      RD|ST         1       IPSEC
    2            202.38.0.2      RD|ST         2       IPSEC
```

flag meaning

RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT

Table 44 Output description

Field	Description
total phase-1 SAs	Total number of SAs for phase 1
connection-id	Identifier of the ISAKMP SA
peer	Remote IP address of the SA
flag	Status of the SA: <ul style="list-style-type: none">RD (READY): The SA has been established.ST (STAYALIVE): This end is the initiator of the tunnel negotiation.RL (REPLACED): The tunnel has been replaced by a new one and will be deleted later.FD (FADING): The soft lifetime is over but the tunnel is still in use. The tunnel will be deleted when the hard lifetime is over.TO (TIMEOUT): The SA has received no keepalive packets after the last keepalive timeout. If no keepalive packets are received before the next keepalive timeout, the SA will be deleted.
phase	The phase the SA belongs to: <ul style="list-style-type: none">Phase 1: The phase for establishing the ISAKMP SA.Phase 2: The phase for negotiating the security service. IPsec SAs are established in this phase.
doi	Interpretation domain the SA belongs to

Display detailed information about the current IKE SAs.

```
<Sysname> display ike sa verbose
-----
  connection id: 2
transmitting entity: initiator
-----
  local ip: 4.4.4.4
```



```

local id type: IPV4_ADDR
local id: 4.4.4.4

remote ip: 4.4.4.5
remote id type: IPV4_ADDR
remote id: 4.4.4.5

authentication-method: PRE-SHARED-KEY
authentication-algorithm: HASH-SHA1
encryption-algorithm: AES-CBC

life duration(sec): 86400
remaining key duration(sec): 86379
exchange-mode: MAIN
diffie-hellman group: GROUP1
nat traversal: NO

```

Display detailed information about the IKE SA with the connection ID of 2.

```

<Sysname> display ike sa verbose connection-id 2
-----
connection id: 2
transmitting entity: initiator
-----
local ip: 4.4.4.4
local id type: IPV4_ADDR
local id: 4.4.4.4

remote ip: 4.4.4.5
remote id type: IPV4_ADDR
remote id: 4.4.4.5

authentication-method: PRE-SHARED-KEY
authentication-algorithm: HASH-SHA1
encryption-algorithm: AES-CBC

life duration(sec): 86400
remaining key duration(sec): 82480
exchange-mode: MAIN
diffie-hellman group: GROUP14
nat traversal: NO

```

Display detailed information about the IKE SA with the remote address of 4.4.4.5.

```

<Sysname> display ike sa verbose remote-address 4.4.4.5
-----
connection id: 2
transmitting entity: initiator
-----
local ip: 4.4.4.4
local id type: IPV4_ADDR
local id: 4.4.4.4

```

```

remote ip: 4.4.4.5
remote id type: IPV4_ADDR
remote id: 4.4.4.5

authentication-method: PRE-SHARED-KEY
authentication-algorithm: HASH-SHA1
encryption-algorithm: AES-CBC

life duration(sec): 86400
remaining key duration(sec): 82236
exchange-mode: MAIN
diffie-hellman group: GROUP1
nat traversal: NO

```

Table 45 Output description

Field	Description
connection id	Identifier of the ISAKMP SA
transmitting entity	Entity in the IKE negotiation
local ip	IP address of the local gateway
local id type	Identifier type of the local gateway
local id	Identifier of the local gateway
remote ip	IP address of the remote gateway
remote id type	Identifier type of the remote gateway
remote id	Identifier of the remote security gateway
authentication-method	Authentication method used by the IKE proposal
authentication-algorithm	Authentication algorithm used by the IKE proposal
encryption-algorithm	Encryption algorithm used by the IKE proposal
life duration(sec)	Lifetime of the ISAKMP SA in seconds
remaining key duration(sec)	Remaining lifetime of the ISAKMP SA in seconds
exchange-mode	IKE negotiation mode in phase 1
diffie-hellman group	DH group used for key negotiation in IKE phase 1
nat traversal	Whether NAT traversal is enabled

dpd Syntax

dpd *dpd-name*

undo dpd

View

IKE peer view

Default level

2: System level

Parameters

dpd-name: DPD detector name, a string of 1 to 32 characters.

Description

Use the **dpd** command to apply a DPD detector to an IKE peer.

Use the **undo dpd** command to remove the application.

By default, no DPD detector is applied to an IKE peer.

Examples

```
# Apply dpd1 to IKE peer peer1.  
<Sysname> system-view  
[Sysname] ike peer peer1  
[Sysname-ike-peer-peer1] dpd dpd1
```

encryption-algorithm

Syntax

encryption-algorithm aes-cbc [*key-length*]

undo encryption-algorithm

View

IKE proposal view

Default level

2: System level

Parameters

aes-cbc: Uses the AES algorithm in CBC mode as the encryption algorithm. The AES algorithm uses 128-bit, 192-bit, or 256-bit keys for encryption.

key-length: Key length for the AES algorithm, which can be 128, 192 or 256 bits and is defaulted to 128 bits.

Description

Use the **encryption-algorithm** command to specify an encryption algorithm for an IKE proposal.

Use the **undo encryption-algorithm** command to restore the default.

The default encryption algorithm for an IKE proposal is AES-128.

Related commands: **ike proposal** and **display ike proposal**.

Examples

```
# Use 128-bit AES in CBC mode as the encryption algorithm for IKE proposal 10.  
<Sysname> system-view  
[Sysname] ike proposal 10  
[Sysname-ike-proposal-10] encryption-algorithm aes 128
```

exchange-mode

Syntax

```
exchange-mode main
undo exchange-mode
```

View

IKE peer view

Default level

2: System level

Parameters

main: Main mode.

Description

Use the **exchange-mode** command to select an IKE negotiation mode.

Use the **undo exchange-mode** command to restore the default.

By default, main mode is used.

Related commands: **id-type**.

Examples

```
# Specify that IKE negotiation works in main mode.
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] exchange-mode main
```

id-type

Syntax

```
id-type { ip | name | user-fqdn }
undo id-type
```

View

IKE peer view

Default level

2: System level

Parameters

ip: Uses an IP address as the ID during IKE negotiation.

name: Uses a FQDN name as the ID during IKE negotiation.

user-fqdn: Uses a user FQDN name as the ID during IKE negotiation.

Description

Use the **id-type** command to select the type of the ID for IKE negotiation.

Use the **undo id-type** command to restore the default.

By default, the ID type is IP address.

In main mode, only the ID type of IP address can be used in IKE negotiation and SA creation.

Related commands: **local-name**, **ike local-name**, **remote-name**, **remote-address**, **local-address**, and **exchange-mode**.

Examples

Use the ID type of name during IKE negotiation.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] id-type name
```

ike dpd

Syntax

```
ike dpd dpd-name
undo ike dpd dpd-name
```

View

System view

Default level

2: System level

Parameters

dpd-name: Name for the dead peer detection (DPD) detector, a string of 1 to 32 characters.

Description

Use the **ike dpd** command to create a DPD detector and enter IKE DPD view.

Use the **undo ike dpd** command to remove a DPD detector.

Related commands: **display ike dpd**, **interval-time**, and **time-out**.

Examples

```
# Create a DPD detector named dpd2.
<Sysname> system-view
[Sysname] ike dpd dpd2
```

ike local-name

Syntax

```
ike local-name name
undo ike local-name
```

View

System view

Default level

2: System level

Parameters

name: Name of the local security gateway for IKE negotiation, a case-sensitive string of 1 to 32 characters.

Description

Use the **ike local-name** command to configure a name for the local security gateway.

Use the **undo ike local-name** command to restore the default.

By default, the device name is used as the name of the local security gateway.

If you configure the **id-type name** or **id-type user-fqdn** command on the initiator, the IKE negotiation peer uses the security gateway name as its ID to initiate IKE negotiation, and you must configure the **ike local-name** command in system view or the **local-name** command in IKE peer view on the local device. If you configure both the **ike local-name** command and the **local-name** command, the name configured by the **local-name** command is used.

The IKE negotiation initiator sends its security gateway name as its ID to the peer, and the peer uses the security gateway name configured with the **remote-name** command to authenticate the initiator. Make sure the local gateway name matches the remote gateway name configured on the peer.

Related commands: **remote-name** and **id-type**.

Examples

Configure the local security gateway name as **app**.

```
<Sysname> system-view  
[Sysname] ike local-name app
```

ike next-payload check disabled

Syntax

ike next-payload check disabled

undo ike next-payload check disabled

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ike next-payload check disabled** command to disable the checking of the Next payload field in the last payload of an IKE message during IKE negotiation, gaining interoperability with products assigning the field a value other than zero.

Use the **undo ike next-payload check disabled** command to restore the default.

By default, the Next payload field is checked.

Examples

Disable Next payload field checking for the last payload of an IKE message.

```
<Sysname> system-view
```

```
[Sysname] ike next-payload check disabled
```

ike peer (system view)

Syntax

```
ike peer peer-name  
undo ike peer peer-name
```

View

System view

Default level

2: System level

Parameters

peer-name: IKE peer name, a string of 1 to 32 characters.

Description

Use the **ike peer** command to create an IKE peer and enter IKE peer view.

Use the **undo ike peer** command to delete an IKE peer.

Examples

```
# Create an IKE peer named peer1 and enter IKE peer view.  
<Sysname> system-view  
[Sysname] ike peer peer1  
[Sysname-ike-peer-peer1]
```

ike proposal

Syntax

```
ike proposal proposal-number  
undo ike proposal proposal-number
```

View

System view

Default level

2: System level

Parameters

proposal-number: IKE proposal number, in the range 1 to 65535. The lower the number, the higher the priority of the IKE proposal. During IKE negotiation, a high priority IKE proposal is matched before a low priority IKE proposal.

Description

Use the **ike proposal** command to create an IKE proposal and enter IKE proposal view.

Use the **undo ike proposal** command to delete an IKE proposal.

The system provides a default IKE proposal, which has the lowest priority and uses these settings:

- Encryption algorithm AES-128

- Authentication algorithm HMAC-SHA1
- Authentication method Pre-shared key
- DH group MODP_1024
- SA lifetime 86400 seconds

Related commands: **display ike proposal**.

Examples

Create IKE proposal 10 and enter IKE proposal view.

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10]
```

ike sa keepalive-timer interval

Syntax

ike sa keepalive-timer interval *seconds*

undo ike sa keepalive-timer interval

View

System view

Default level

2: System level

Parameters

seconds: Transmission interval of ISAKMP SA keepalives in seconds, in the range 20 to 28,800.

Description

Use the **ike sa keepalive-timer interval** command to set the ISAKMP SA keepalive interval.

Use the **undo ike sa keepalive-timer interval** command to disable the ISAKMP SA keepalive transmission function.

By default, no keepalive packet is sent.

The keepalive interval configured at the local end must be shorter than the keepalive timeout configured at the remote end.

Related commands: **ike sa keepalive-timer timeout**.

Examples

Set the keepalive interval to 200 seconds.

```
<Sysname> system-view
[Sysname] ike sa keepalive-timer interval 200
```

ike sa keepalive-timer timeout

Syntax

ike sa keepalive-timer timeout *seconds*

undo ike sa keepalive-timer timeout

View

System view

Default level

2: System level

Parameters

seconds: ISAKMP SA keepalive timeout in seconds, in the range 20 to 28800.

Description

Use the **ike sa keepalive-timer timeout** command to set the ISAKMP SA keepalive timeout.

Use the **undo ike sa keepalive-timer timeout** command to disable the function.

By default, no keepalive packet is sent.

The keepalive timeout configured at the local end must be longer than the keepalive interval configured at the remote end. Since it seldom occurs that more than three consecutive packets are lost on a network, the keepalive timeout can be configured to be three times of the keepalive interval.

Related commands: **ike sa keepalive-timer interval**.

Examples

```
# Set the keepalive timeout to 20 seconds.
```

```
<Sysname> system-view
```

```
[Sysname] ike sa keepalive-timer timeout 20
```

ike sa nat-keepalive-timer interval

Syntax

ike sa nat-keepalive-timer interval *seconds*

undo ike sa nat-keepalive-timer interval

View

System view

Default level

2: System level

Parameters

seconds: NAT keepalive interval in seconds, in the range 5 to 300.

Description

Use the **ike sa nat-keepalive-timer interval** command to set the NAT keepalive interval.

Use the **undo ike sa nat-keepalive-timer interval** command to disable the function.

By default, the NAT keepalive interval is 20 seconds.

Examples

```
# Set the NAT keepalive interval to 5 seconds.
```

```
<Sysname> system-view
```

```
[Sysname] ike sa nat-keepalive-timer interval 5
```

interval-time

Syntax

interval-time *interval-time*

undo interval-time

View

IKE DPD view

Default level

2: System level

Parameters

interval-time: Sets DPD interval in seconds, in the range of 1 to 300 seconds. When the local end sends an IPsec packet, it checks the time the last IPsec packet was received from the peer. If the time interval exceeds the DPD interval, it sends a DPD hello to the peer.

Description

Use the **interval-time** command to set the DPD query triggering interval for a DPD detector.

Use the **undo interval-time** command to restore the default.

The default DPD interval is 10 seconds.

Examples

```
# Set the DPD interval to 1 second for dpd2.  
<Sysname> system-view  
[Sysname] ike dpd dpd2  
[Sysname-ike-dpd-dpd2] interval-time 1
```

local-address

Syntax

local-address *ip-address*

undo local-address

View

IKE peer view

Default level

2: System level

Parameters

ip-address: IP address of the local security gateway to be used in IKE negotiation.

Description

Use the **local-address** command to configure the IP address of the local security gateway in IKE negotiation.

Use the **undo local-address** command to remove the configuration.

By default, the primary address of the interface referencing the IPsec policy is used as the local security gateway IP address for IKE negotiation. Use this command if you want to specify a different address for the local security gateway.

Examples

```
# Set the IP address of the local security gateway to 1.1.1.1.
<Sysname> system-view
[Sysname] ike peer xhy
[Sysname-ike-peer-xhy] local-address 1.1.1.1
```

local-name

Syntax

local-name *name*
undo local-name

View

IKE peer view

Default level

2: System level

Parameters

name: Name for the local security gateway to be used in IKE negotiation, a case-sensitive string of 1 to 32 characters.

Description

Use the **local-name** command to configure a name for the local security gateway to be used in IKE negotiation.

Use the **undo local-name** to restore the default.

By default, the device name is used as the name of the local security gateway view.

If you configure the **id-type name** or **id-type user-fqdn** command on the initiator, the IKE negotiation peer uses the security gateway name as its ID to initiate IKE negotiation, and you must configure the **ike local-name** command in system view or the **local-name** command in IKE peer view on the local device. If you configure both the **ike local-name** command and the **local-name** command, the name configured by the **local-name** command is used.

The IKE negotiation initiator sends its security gateway name as its ID to the peer, and the peer uses the security gateway name configured with the **remote-name** command to authenticate the initiator. Make sure the local gateway name matches the remote gateway name configured on the peer.

Relate commands: **remote-name**, **id-type**.

Examples

```
# Set the name of the local security gateway to localgw in IKE peer view of peer1.
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] local-name localgw
```

nat traversal

Syntax

nat traversal
undo nat traversal

View

IKE peer view

Default level

2: System level

Parameters

None

Description

Use the **nat traversal** command to enable the NAT traversal function of IKE/IPsec.

Use the **undo nat traversal** command to disable the NAT traversal function of IKE/IPsec.

By default, the NAT traversal function is disabled.

Examples

```
# Enable the NAT traversal function for IKE peer peer1.  
<Sysname> system-view  
[Sysname] ike peer peer1  
[Sysname-ike-peer-peer1] nat traversal
```

peer

Syntax

peer { multi-subnet | single-subnet }
undo peer

View

IKE peer view

Default level

2: System level

Parameters

multi-subnet: Sets the subnet type to multiple.

single-subnet: Sets the subnet type to single.

Description

Use the **peer** command to set the subnet type of the peer security gateway for IKE negotiation.

Use the **undo peer** command to restore the default.

By default, the subnet is a single one.

Use this command to enable interoperability with a NetScreen device.

Examples

```
# Set the subnet type of the peer security gateway to multiple.
<Sysname> system-view
[Sysname] ike peer xhy
[Sysname-ike-peer-xhy] peer multi-subnet
```

pre-shared-key

Syntax

```
pre-shared-key [ cipher | simple ] key
undo pre-shared-key
```

View

IKE peer view

Default level

2: System level

Parameters

key: Plaintext pre-shared key to be displayed in cipher text, a case-sensitive string of 8 to 128 characters.

cipher *key*: Specifies the ciphertext pre-shared key to be displayed in cipher text, a case-sensitive string of 8 to 201 characters.

simple *key*: Specifies the plaintext pre-shared key to be displayed in plain text, a case-sensitive string of 8 to 128 characters, which must contain digits, upper-case letters, lower-case letters, and special characters.

Description

Use the **pre-shared-key** command to configure the pre-shared key to be used in IKE negotiation.

Use the **undo pre-shared-key** command to remove the configuration.

Related commands: **authentication-method**.

Examples

```
# Set the pre-shared key used in IKE negotiation to AAbbcc1234%.
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] pre-shared-key AAbbcc1234%
```

proposal (IKE peer view)

Syntax

```
proposal proposal-number&<1-6>
undo proposal [ proposal-number ]
```

View

IKE peer view

Default level

2: System level

Parameters

proposal-number&<1-6>: Sequence number of the IKE proposal for the IKE peer to reference, in the range 1 to 65535. &<1-6> means that you can specify the *proposal-number* argument for up to six times. An IKE proposal with a smaller sequence number has a higher priority.

Description

Use the **proposal** command to specify the IKE proposals for the IKE peer to reference.

Use the **undo proposal** command to remove one or all IKE proposals referenced by the IKE peer.

By default, an IKE peer references no IKE proposals and, when initiating IKE negotiation, it uses the IKE proposals configured in system view.

In the IKE negotiation phase 1, the local peer uses the IKE proposals specified for it, if any.

An IKE peer can reference up to six IKE proposals.

The responder uses the IKE proposals configured in system view for negotiation.

Related commands: **ike proposal** and **ike peer (system view)**.

Examples

Configure IKE peer **peer1** to reference IKE proposal **10**.

```
<Sysname> system-view
```

```
[Sysname] ike peer peer1
```

```
[Sysname-ike-peer-peer1] proposal 10
```

remote-address

Syntax

remote-address { *hostname* [**dynamic**] | *low-ip-address* [*high-ip-address*] }

undo remote-address

View

IKE peer view

Default level

2: System level

Parameters

hostname: Host name of the IPsec remote security gateway, a case-insensitive string of 1 to 255 characters. The host name uniquely identifies the remote IPsec peer and can be resolved to an IP address by the DNS server.

dynamic: Specifies to use dynamic address resolution for the IPsec remote peer name. If you do not provide this keyword, the local peer has the remote host name resolved only once after you configure the remote host name.

low-ip-address: IP address of the IPsec remote security gateway. It is the lowest address in the address range if you want to specify a range of addresses.

high-ip-address: Highest address in the address range if you want to specify a range of addresses.

Description

Use the **remote-address** command to configure the IP address of the IPsec remote security gateway.

Use the **undo remote-address** command to remove the configuration.

The IP address configured with the **remote-address** command must match the local security gateway IP address that the remote security gateway uses for IKE negotiation, which is the IP address configured with the **local-address** command or, if the **local-address** command is not configured, the primary IP address of the interface to which the policy is applied.

The local peer can be the initiator of IKE negotiation if the remote address is a host IP address or a host name. The local end can only be the responder of IKE negotiation if the remote address is an address range that the local peer can respond to.

If the IP address of the remote address changes frequently, configure the host name of the remote gateway with the **dynamic** keyword so that the local peer can use the up-to-date remote IP address to initiate IKE negotiation.

Related commands: **id-type ip** and **local-address**.

Examples

Configure the IP address of the remote security gateway as 10.0.0.1.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] remote-address 10.0.0.1
```

Configure the host name of the remote gateway as **test.com**, and specify the local peer to dynamically update the remote IP address.

```
<Sysname> system-view
[Sysname] ike peer peer2
[Sysname-ike-peer-peer2] remote-address test.com dynamic
```

remote-name

Syntax

remote-name *name*

undo remote-name

View

IKE peer view

Default level

2: System level

Parameters

name: Name of the peer security gateway for IKE negotiation, a string of 1 to 32 characters.

Description

Use the **remote-name** command to configure the name of the remote gateway.

Use the **undo remote-name** command to remove the configuration.

If you configure the **id-type name** or **id-type user-fqdn** command on the initiator, the IKE negotiation initiator sends its security gateway name as its ID for IKE negotiation, and the peer uses the security gateway name configured with the **remote-name** command to authenticate the initiator. Make sure the local gateway name matches the remote gateway name configured on the peer.

Related commands: **id-type**, **local-name**, and **ike local-name**.

Examples

Configure the remote security gateway name as **apple** for IKE peer peer1.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] remote-name apple
```

reset ike sa

Syntax

reset ike sa [*connection-id*]

View

User view

Default level

2: System level

Parameters

connection-id: Connection ID of the IKE SA to be cleared, in the range 1 to 2000000000.

Description

Use the **reset ike sa** command to clear IKE SAs.

If you do not specify a connection ID, the command clears all ISAKMP SAs.

When you clear a local IPsec SA, its ISAKMP SA can transmit the Delete message to notify the remote end to delete the paired IPsec SA. If the ISAKMP SA has been cleared, the local end cannot notify the remote end to clear the paired IPsec SA, and you must manually clear the remote IPsec SA.

Related commands: **display ike sa**.

Examples

Clear an IPsec tunnel to 202.38.0.2.

```
<Sysname> display ike sa
  total phase-1 SAs:  1
  connection-id  peer          flag          phase   doi
  -----
    1            202.38.0.2    RD|ST         1       IPSEC
    2            202.38.0.2    RD|ST         2       IPSEC
flag meaning
RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
<Sysname> reset ike sa 2
<Sysname> display ike sa
  total phase-1 SAs:  1
  connection-id  peer          flag          phase   doi
  -----
    1            202.38.0.2    RD|ST         1       IPSEC
flag meaning
RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
```


sa duration

Syntax

sa duration *seconds*

undo sa duration

View

IKE proposal view

Default level

2: System level

Parameters

Seconds: Specifies the ISAKMP SA lifetime in seconds, in the range 60 to 604800.

Description

Use the **sa duration** command to set the ISAKMP SA lifetime for an IKE proposal.

Use the **undo sa duration** command to restore the default.

By default, the ISAKMP SA lifetime is 86400 seconds.

Before an SA expires, IKE negotiates a new SA. The new SA takes effect immediately after being set up, and the old one will be cleared automatically when it expires.

Related commands: **ike proposal** and **display ike proposal**.

Examples

```
# Specify the ISAKMP SA lifetime for IKE proposal 10 as 600 seconds (10 minutes).
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] sa duration 600
```

time-out

Syntax

time-out *time-out*

undo time-out

View

IKE DPD view

Default level

2: System level

Parameters

time-out: DPD packet retransmission interval in seconds, in the range 1 to 60.

Description

Use the **time-out** command to set the DPD packet retransmission interval for a DPD detector.

Use the **undo time-out** command to restore the default.

The default DPD packet retransmission interval is 5 seconds.

Examples

Set the DPD packet retransmission interval to 1 second for dpd2.

```
<Sysname> system-view
```

```
[Sysname] ike dpd dpd2
```

```
[Sysname-ike-dpd-dpd2] time-out 1
```

SSH2.0 configuration commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

SSH2.0 server configuration commands

display ssh server

Syntax

```
display ssh server { session | status } [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

session: Displays the session information of the SSH server.

status: Displays the status information of the SSH server.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ssh server** on an SSH server to display SSH server status information or session information.

Related commands: **ssh server authentication-retries**, **ssh server authentication-timeout**, **ssh server compatible-ssh1x enable**, **ssh server enable**, and **ssh server rekey-interval**.

Examples

```
# Display SSH server status information.
<Sysname> display ssh server status
SSH Server: Disable
SSH version : 1.99
SSH authentication-timeout : 60 second(s)
SSH server key generating interval : 0 hour(s)
SSH Authentication retries : 3 time(s)
SFTP Server: Disable
SFTP Server Idle-Timeout: 10 minute(s)
```

Table 46 Command output

Field	Description
SSH Server	Whether the SSH server function is enabled.
SSH version	SSH protocol version. When the SSH supports SSH1, the protocol version is 1.99. Otherwise, the protocol version is 2.0.
SSH authentication-timeout	Authentication timeout period.
SSH server key generating interval	SSH server key pair update interval.
SSH Authentication retries	Maximum number of authentication attempts for SSH users.
SFTP Server	Whether the SFTP server function is enabled.
SFTP Server Idle-Timeout	SFTP connection idle timeout period.

Display the SSH server session information.

```
<Sysname> display ssh server session
Conn  Ver  Encry  State      Retry  SerType  Username
VTY 0   2.0   DES     Established  0      SFTP     client001
```

Table 47 Command output

Field	Description
Conn	Connected VTY channel.
Ver	SSH server protocol version.
Encry	Encryption algorithm.
State	Status of the session: <ul style="list-style-type: none"> • Init—Initialization. • Ver-exchange—Version negotiation. • Keys-exchange—Keys exchange. • Auth-request—Authentication request. • Serv-request—Session service request. • Established—The session is established. • Disconnected—The session is disconnected.
Retry	Number of authentication attempts.
SerType	Service type (SCP, SFTP, and Stelnet).
Username	Name of a user for login.

display ssh user-information

Syntax

display ssh user-information [*username*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

username: Specifies an SSH username, a string of 1 to 80 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ssh user-information** on an SSH server to display information about SSH users.

This command displays only information about SSH users configured through the **ssh user** command on the SSH server.

Without the *username* argument, the command displays information about all SSH users.

Related commands: **ssh user**.

Examples

Display information about all SSH users.

```
<Sysname> display ssh user-information
```

```
Total ssh users : 2
```

Username	Authentication-type	User-public-key-name	Service-type
yemx	password	null	all
test	publickey	pubkey	sftp

Table 48 Command output

Field	Description
Username	Name of the user.
Authentication-type	Authentication method. If this field has a value of password , the next field has a value of null .
User-public-key-name	Public key of the user.
Service-type	Service type, including SFTP, Stelnet, SCP, and all, where all indicates all authentication methods are supported.

ssh server authentication-retries

Syntax

ssh server authentication-retries *times*

undo ssh server authentication-retries

View

System view

Default level

3: Manage level

Parameters

times: Specifies the maximum number of authentication attempts for SSH users, in the range of 1 to 5.

Description

Use **ssh server authentication-retries** to set the maximum number of authentication attempts for SSH users.

Use **undo ssh server authentication-retries** to restore the default.

By default, the maximum number of authentication attempts for SSH users is 3.

You can set this limit to prevent malicious hacking of usernames and passwords.

This configuration takes effect only for the users at next login.

Authentication fails if the total number of authentication attempts (including both publickey and password authentication) exceeds the upper limit configured by the **ssh server authentication-retries** command.

If the authentication method of SSH users is **password-publickey**, the server first uses publickey authentication, and then uses password authentication to authenticate SSH users. The process is regarded as one authentication attempt.

Related commands: **display ssh server**.

Examples

```
# Set the maximum number of authentication attempts for SSH users to 4.
<Sysname> system-view
[Sysname] ssh server authentication-retries 4
```

ssh server authentication-timeout

Syntax

ssh server authentication-timeout *time-out-value*

undo ssh server authentication-timeout

View

System view

Default level

3: Manage level

Parameters

time-out-value: Specifies an authentication timeout period in seconds, in the range of 1 to 120.

Description

Use **ssh server authentication-timeout** to set the SSH user authentication timeout period on the SSH server. If a user does not finish the authentication when the timer expires, the connection is down.

Use **undo ssh server authentication-timeout** to restore the default.

By default, the authentication timeout period is 60 seconds.

You can set a small value for this timer to prevent malicious occupation of TCP connections.

Related commands: **display ssh server**.

Examples

```
# Set the SSH user authentication timeout period to 10 seconds.
<Sysname> system-view
[Sysname] ssh server authentication-timeout 10
```

ssh server compatible-ssh1x

Syntax

```
ssh server compatible-ssh1x [ enable ]
undo ssh server compatible-ssh1x
```

View

System view

Default level

3: Manage level

Parameters

enable: Enables the SSH server to support SSH1 clients. This keyword is not necessary. Even if it is not specified, the command can also enable the SSH server to support SSH1 clients.

Description

Use **ssh server compatible-ssh1x** to enable the SSH server to support SSH1 clients.

Use **undo ssh server compatible-ssh1x** to disable the SSH server from supporting SSH1 clients.

By default, the SSH server supports SSH1 clients.

The configuration takes effect only for clients that log in after the configuration.

This command is not available in FIPS mode.

Related commands: **display ssh server**.

Examples

```
# Enable the SSH server to support SSH1 clients.
<Sysname> system-view
[Sysname] ssh server compatible-ssh1x enable
```

ssh server dscp

Syntax

```
ssh server dscp dscp-value
undo ssh server dscp
```

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in the IPv4 packets sent by the SSH server, which ranges from 0 to 63.

Description

Use **ssh server dscp** to set the DSCP value for IPv4 packets sent by the SSH server.

Use **undo ssh server dscp** to restore the default.

By default, the DSCP value in IPv4 packets sent by the SSH server is 16.

Examples

Set the DSCP value to 30 for IPv4 packets sent by the SSH server.

```
<Sysname> system-view  
[Sysname] ssh server dscp 30
```

ssh server enable

Syntax

ssh server enable

undo ssh server enable

View

System view

Default level

3: Manage level

Parameters

None

Description

Use **ssh server enable** to enable the SSH server function so that the SSH clients can communicate with the server through SSH.

Use **undo ssh server enable** to disable the SSH server function.

By default, SSH server is disabled.

Related commands: **display ssh server**.

Examples

Enable SSH server.

```
<Sysname> system-view  
[Sysname] ssh server enable
```

ssh server ipv6 dscp

Syntax

ssh server ipv6 dscp *dscp-value*

undo ssh server ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in the IPv6 packets sent by the SSH server, which ranges from 0 to 63.

Description

Use **ssh server ipv6 dscp** to set the DSCP value for IPv6 packets sent by the SSH server.

Use **undo ssh server ipv6 dscp** to restore the default.

By default, the DSCP value in IPv6 packets sent by the SSH server is 0.

Examples

Set the DSCP value to 30 for IPv6 packets sent by the SSH server.

```
<Sysname> system-view
```

```
[Sysname] ssh server ipv6 dscp 30
```

ssh server rekey-interval

Syntax

ssh server rekey-interval *hours*

undo ssh server rekey-interval

View

System view

Default level

3: Manage level

Parameters

hours: Specifies an interval (in hours) for updating the server key pair, in the range of 1 to 24.

Description

Use **ssh server rekey-interval** to set the interval for updating the RSA server key.

Use **undo ssh server rekey-interval** to restore the default.

By default, the update interval of the RSA server key is 0, and the RSA server key is not updated.

Periodically updating the RSA server key can prevent malicious hacking of the key and enhance security of the SSH connections.

This command is not available in FIPS mode.

This command is only available to SSH users using SSH1 client software.

The system does not update any DSA key pair periodically.

Related commands: **display ssh server**.

Examples

```
# Set the RSA server key pair update interval to 3 hours.
<Sysname> system-view
[Sysname] ssh server rekey-interval 3
```

ssh user

Syntax

In non-FIPS mode:

```
ssh user username service-type stelnet authentication-type { password | { any | password-publickey | publickey } assign publickey keyname }
```

```
ssh user username service-type { all | scp | sftp } authentication-type { password | { any | password-publickey | publickey } assign publickey keyname work-directory directory-name }
```

```
undo ssh user username
```

In FIPS mode:

```
ssh user username service-type stelnet authentication-type { password | password-publickey assign publickey keyname }
```

```
ssh user username service-type { all | scp | sftp } authentication-type { password | password-publickey assign publickey keyname work-directory directory-name }
```

```
undo ssh user username
```

View

System view

Default level

3: Manage level

Parameters

username: Specifies an SSH username, a case-sensitive string of 1 to 80 characters.

service-type: Specifies the service type of an SSH user, which can be one of the following:

- **all**: Specifies Stelnet, SFTP, and SCP.
- **scp**: Specifies the service type as secure copy.
- **sftp**: Specifies the service type as secure FTP.
- **stelnet**: Specifies the service type of secure Telnet.

authentication-type: Specifies the authentication method of an SSH user, which can be one of the following:

- **password**: Specifies password authentication. This authentication method features easy and fast encryption, but it is vulnerable. It can work with AAA to implement user authentication, authorization, and accounting.
- **any**: Specifies either password authentication or publickey authentication.
- **password-publickey**: Specifies both password authentication and publickey authentication (featuring higher security) if the client runs SSH2, and performs either type of authentication if the client runs SSH1.

- **publickey**: Specifies publickey authentication. This authentication method has the downside of complicated and slow encryption, but it provides strong authentication that can defend against brute-force attacks. This authentication method is easy to use. Once it is configured, the authentication process completes automatically without the need of remembering or entering any password.

assign publickey *keyname*: Assigns an existing public key to an SSH user. The *keyname* argument indicates the name of the client public key and is a string of 1 to 64 characters.

work-directory *directory-name*: Specifies the working directory for an SFTP or SCP user. The *directory-name* argument indicates the name of the working directory and is a string of 1 to 135 characters.

Description

Use **ssh user** to create an SSH user and specify the service type and authentication method.

Use **undo ssh user** to delete an SSH user.

For a publickey authentication user, you must configure the username and the public key on the switch. For a password authentication user, you can configure the account information on either the switch or the remote authentication server, such as a RADIUS server.

If you use the **ssh user** command to configure a public key for a user who has already had a public key, the new one overwrites the old one.

You can change the authentication method and public key of an SSH user when the user is communicating with the SSH server. However, your changes take effect for the clients at next login.

If an SCP or SFTP user has been assigned a public key, it is necessary to set a working folder for the user.

The working folder of an SCP or SFTP user depends on the user authentication method. For a user using only password authentication, the working folder is the AAA authorized one. For a user using only publickey authentication or using both publickey authentication and password authentication, the working folder is the one set by using the **ssh user** command.

Related commands: **display ssh user-information**.

Examples

Create an SSH user named **user1**, set the service type as **sftp**, the authentication method as **publickey**, assign a public key named **key1** to the user, and specify the working directory of the SFTP server as **flash:/**.

```
<Sysname> system-view
[Sysname] ssh user user1 service-type sftp authentication-type publickey assign publickey
key1 work-directory flash:/
```

SSH2.0 client configuration commands

display ssh client source

Syntax

display ssh client source [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ssh client source** to display the source IP address or source interface information on an SSH client.

If neither source IP address nor source interface is specified for the SSH client, the system displays the message "Neither source IP address nor source interface was specified for the Stelnet client."

Related commands: **ssh client source**.

Examples

Display the source IP address or source interface of the SSH client.

```
<Sysname> display ssh client source
```

```
The source IP address you specified is 192.168.0.1
```

display ssh server-info

Syntax

```
display ssh server-info [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ssh server-info** on a client to display mappings between SSH servers and their host public keys on an SSH client.

When an SSH client needs to authenticate the SSH server, it uses the locally saved public key of the server for the authentication. If the authentication fails, you can use this command to check the public key of the server saved on the client.

This command is also available on an SFTP client.

Related commands: **ssh client authentication server**.

Examples

Display the mappings between host public keys and SSH servers saved on the client.

```
<Sysname> display ssh server-info
```

Server Name(IP)	Server public key name
-----------------	------------------------

192.168.0.1	abc_key01
-------------	-----------

192.168.0.2	abc_key02
-------------	-----------

Table 49 Command output

Field	Description
Server Name(IP)	Name or IP address of the server
Server public key name	Name of the host public key of the server

ssh client authentication server

Syntax

ssh client authentication server *server* **assign publickey** *keyname*

undo ssh client authentication server *server* **assign publickey**

View

System view

Default level

2: System level

Parameters

server: Specifies an IP address or name of the server, a string of 1 to 80 characters.

assign publickey *keyname*: Specifies the name of the host public key of the server, a string of 1 to 64 characters.

Description

Use **ssh client authentication server** on a client to configure the host public key of a server so that the client can determine whether the server is trustworthy.

Use **undo ssh client authentication server** to remove the configuration.

By default, the host public key of the server is not configured, and when logging into the server, the client uses the IP address or host name used for login as the public key name.

A client that does not support first-time authentication rejects unauthenticated servers. To enable the client to use the correct public key of a server to authenticate the server, you must configure the public keys of the servers and specify the mappings between public keys and servers on the client.

The specified host public key of the server must already exist.

Related commands: **ssh client first-time enable**.

Examples

```
# Configure the public key of the server with the IP address of 192.168.0.1 to be key1.
<Sysname> system-view
[Sysname] ssh client authentication server 192.168.0.1 assign publickey key1
```

ssh client dscp

Syntax

```
ssh client dscp dscp-value
undo ssh client dscp
```

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in the IPv4 packets sent by the SSH client, which ranges from 0 to 63.

Description

Use **ssh client dscp** to set the DSCP value for IPv4 packets sent by the SSH client.

Use **undo ssh client dscp** to restore the default.

By default, the DSCP value in IPv4 packets sent by the SSH client is 16.

Examples

```
# Set the DSCP value to 30 for IPv4 packets sent by the SSH client.
<Sysname> system-view
[Sysname] ssh client dscp 30
```

ssh client first-time

Syntax

```
ssh client first-time [ enable ]
undo ssh client first-time
```

View

System view

Default level

2: System level

Parameters

enable: Enables the first-time authentication of the SSH client to the SSH server. This keyword is not necessary. Even if it is not specified, the command can also enable the first-time authentication function.

Description

Use **ssh client first-time** to enable the first-time authentication function.

Use **undo ssh client first-time** to disable the function.

By default, the function is enabled.

With first-time authentication, when an SSH client not configured with the server host public key accesses the server for the first time, the user can continue accessing the server, and save the host public key on the client. When accessing the server again, the client uses the saved server host public key to authenticate the server.

Without first-time authentication, a client that is not configured with the server host public key refuses to access the server. To access the server, a user must configure in advance the server host public key locally and specify the public key name for authentication.

Because the server might update its key pairs periodically, clients must obtain the most recent public keys of the server for successful authentication of the server.

Examples

```
# Enable the first-time authentication function.
```

```
<Sysname> system-view
```

```
[Sysname] ssh client first-time enable
```

ssh client ipv6 dscp

Syntax

ssh client ipv6 dscp *dscp-value*

undo ssh client ipv6 dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in the IPv6 packets sent by the SSH client, which ranges from 0 to 63.

Description

Use **ssh client ipv6 dscp** to set the DSCP value for IPv6 packets sent by the SSH client.

Use **undo ssh client ipv6 dscp** to restore the default.

By default, the DSCP value in IPv6 protocol packets sent by the SSH client is 0.

Examples

```
# Set the DSCP value to 30 for IPv6 protocol packets sent by the SSH client.
```

```
<Sysname> system-view
```

```
[Sysname] ssh client ipv6 dscp 30
```

ssh client ipv6 source

Syntax

```
ssh client ipv6 source { ipv6 ipv6-address | interface interface-type interface-number }  
undo ssh client ipv6 source
```

View

System view

Default level

3: Manage level

Parameters

ipv6 *ipv6-address*: Specifies a source IPv6 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description

Use **ssh client ipv6 source** to specify the source IPv6 address or source interface for the SSH client.

Use **undo ssh client ipv6 source** to remove the configuration.

By default, an SSH client uses the IPv6 address of the interface specified by the route of the device to access the SSH server.

To make sure the SSH client and the SSH server can communicate with each other, and to improve the manageability of SSH clients in the authentication service, HP recommends you specify a loopback interface as the source interface.

Related commands: **display ssh client source**.

Examples

```
# Specify the source IPv6 address as 2:2::2:2 for the SSH client.
```

```
<Sysname> system-view
```

```
[Sysname] ssh client ipv6 source ipv6 2:2::2:2
```

ssh client source

Syntax

```
ssh client source { ip ip-address | interface interface-type interface-number }  
undo ssh client source
```

View

System view

Default level

3: Manage level

Parameters

ip *ip-address*: Specifies a source IPv4 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description

Use **ssh client source** to specify the source IPv4 address or source interface of the SSH client.

Use **undo ssh client source** to remove the configuration.

By default, an SSH client uses the IP address of the interface specified by the route of the device to access the SSH server.

To make sure the SSH client and the SSH server can communicate with each other, and to improve the manageability of SSH clients in the authentication service, HP recommends you specify a loopback interface as the source interface.

Related commands: **display ssh client source**.

Examples

```
# Specify the source IPv4 address of the SSH client as 192.168.0.1.
```

```
<Sysname> system-view
```

```
[Sysname] ssh client source ip 192.168.0.1
```

ssh2

Syntax

In non-FIPS mode:

```
ssh2 server [ port-number ] [ identity-key { dsa | rsa } | prefer-ctos-cipher { 3des | aes128 | des } |  
prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1  
| dh-group14 } | prefer-stoc-cipher { 3des | aes128 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1  
| sha1-96 } ] *
```

In FIPS mode:

```
ssh2 server [ port-number ] [ identity-key rsa | prefer-ctos-cipher { aes128 | aes256 } |  
prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher { aes128 | aes256 }  
| prefer-stoc-hmac { sha1 | sha1-96 } ] *
```

View

User view

Default level

0: Visit level

Parameters

server: Specifies an IPv4 address or host name of the server, a case-insensitive string of 1 to 20 characters.

port-number: Specifies the port number of the server, in the range of 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

prefer-ctos-cipher: Specifies the preferred encryption algorithm from client to server. The default is **aes128**.

- **3des**: Specifies the encryption algorithm **3des-cbc**.
- **aes128**: Specifies the encryption algorithm **aes128-cbc**.
- **aes256**: Specifies the encryption algorithm **aes256-cbc**.
- **des**: Specifies the encryption algorithm **des-cbc**.

prefer-ctos-hmac: Specifies the preferred HMAC algorithm from client to server. The default is **sha1-96**.

- **md5:** Specifies the HMAC algorithm **hmac-md5**.
- **md5-96:** Specifies the HMAC algorithm **hmac-md5-96**.
- **sha1:** Specifies the HMAC algorithm **hmac-sha1**.
- **sha1-96:** Specifies the HMAC algorithm **hmac-sha1-96**.

prefer-kex: Specifies the preferred key exchange algorithm. The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.

- **dh-group-exchange:** Specifies the key exchange algorithm **diffie-hellman-group-exchange-sha1**.
- **dh-group1:** Specifies the key exchange algorithm **diffie-hellman-group1-sha1**.
- **dh-group14:** Specifies the key exchange algorithm **diffie-hellman-group14-sha1**.

prefer-stoc-cipher: Specifies the preferred encryption algorithm from server to client. The default is **aes128**.

prefer-stoc-hmac: Specifies the preferred HMAC algorithm from server to client. The default is **sha1-96**.

Description

Use **ssh2** to establish a connection to an IPv4 SSH server and specify the publickey algorithm, the preferred key exchange algorithm, and the preferred encryption algorithms and preferred HMAC algorithms between the client and server.

When the server adopts publickey authentication to authenticate a client, the client needs to get the local private key for digital signature. As the publickey authentication uses either RSA or DSA algorithm, you must specify an algorithm for the client (by using the **identity-key** keyword) in order to get the correct data for the local private key.

Examples

Log in to remote SSH2.0 server 10.214.50.51, using the following connection scheme:

- Preferred key exchange algorithm: **DH-group1**.
- Preferred encryption algorithm from server to client: **aes128**.
- Preferred HMAC algorithm from client to server: **md5**.
- Preferred HMAC algorithm from server to client: **sha1-96**.

```
<Sysname> ssh2 10.214.50.51 prefer-kex dh-group1 prefer-stoc-cipher aes128  
prefer-ctos-hmac md5 prefer-stoc-hmac sha1-96
```

ssh2 ipv6

Syntax

In non-FIPS mode:

```
ssh2 ipv6 server [ port-number ] [ identity-key { dsa | rsa } | prefer-ctos-cipher { 3des | aes128 | des }  
| prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1  
| dh-group14 } | prefer-stoc-cipher { 3des | aes128 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1  
| sha1-96 } ] *
```

In FIPS mode:

```
ssh2 ipv6 server [ port-number ] [ identity-key rsa | prefer-ctos-cipher { aes128 | aes256 } |  
prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher { aes128 | aes256 }  
| prefer-stoc-hmac { sha1 | sha1-96 } ] *
```

View

User view

Default level

0: Visit level

Parameters

server: Specifies an IPv6 address or host name of the server, a case-insensitive string of 1 to 46 characters.

port-number: Specifies the port number of the server, in the range of 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

prefer-ctos-cipher: Specifies the preferred encryption algorithm from client to server. The default is **aes128**.

- **3des:** Specifies the encryption algorithm **3des-cbc**.
- **aes128:** Specifies the encryption algorithm **aes128-cbc**.
- **aes256:** Specifies the encryption algorithm **aes256-cbc**.
- **des:** Specifies the encryption algorithm **des-cbc**.

prefer-ctos-hmac: Specifies the preferred HMAC algorithm from client to server. The default is **sha1-96**.

- **md5:** Specifies the HMAC algorithm **hmac-md5**.
- **md5-96:** Specifies the HMAC algorithm **hmac-md5-96**.
- **sha1:** Specifies the HMAC algorithm **hmac-sha1**.
- **sha1-96:** Specifies the HMAC algorithm **hmac-sha1-96**.

prefer-kex: Specifies the preferred key exchange algorithm. The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.

- **dh-group-exchange:** Specifies the key exchange algorithm **diffie-hellman-group-exchange-sha1**.
- **dh-group1:** Specifies the key exchange algorithm **diffie-hellman-group1-sha1**.
- **dh-group14:** Specifies the key exchange algorithm **diffie-hellman-group14-sha1**.

prefer-stoc-cipher: Specifies the preferred encryption algorithm from server to client. The default is **aes128**.

prefer-stoc-hmac: Specifies the preferred HMAC algorithm from server to client. The default is **sha1-96**.

Description

Use **ssh2 ipv6** to establish a connection to an IPv6 SSH server and specify publickey algorithm, the preferred key exchange algorithm, and the preferred encryption algorithms and preferred HMAC algorithms between the client and server.

When the server adopts publickey authentication to authenticate a client, the client needs to get the local private key for digital signature. As the publickey authentication uses either RSA or DSA algorithm, you must specify an algorithm for the client (by using the **identity-key** keyword) in order to get the correct data for the local private key.

Examples

Log in to remote SSH2.0 server 2000::1, using the following connection scheme:

- Preferred key exchange algorithm: **dh-group1**.
- Preferred encryption algorithm from server to client: **aes128**.

- Preferred HMAC algorithm from client to server: **md5**.
- Preferred HMAC algorithm from server to client: **sha1-96**.

```
<Sysname> ssh2 ipv6 2000::1 prefer-kex dh-group1 prefer-stoc-cipher aes128  
prefer-ctos-hmac md5 prefer-stoc-hmac sha1-96
```

SFTP configuration commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

SFTP server configuration commands

sftp server enable

Syntax

```
sftp server enable  
undo sftp server enable
```

View

System view

Default level

3: Manage level

Parameters

None

Description

Use **sftp server enable** to enable the SFTP server function.

Use **undo sftp server enable** to disable the SFTP server function.

By default, the SFTP server function is disabled.

Related commands: **display ssh server**.

Examples

```
# Enable the SFTP server function.  
<Sysname> system-view  
[Sysname] sftp server enable
```

sftp server idle-timeout

Syntax

```
sftp server idle-timeout time-out-value  
undo sftp server idle-timeout
```

View

System view

Default level

3: Manage level

Parameters

time-out-value: Specifies the timeout period in minutes, in the range of 1 to 35791.

Description

Use **sftp server idle-timeout** to set the idle timeout period for SFTP user connections.

Use **undo sftp server idle-timeout** to restore the default.

By default, the idle timeout period is 10 minutes.

If an SFTP connection is idle when the idle timeout timer expires, the system automatically terminates the connection. If there are many SFTP connections, you can set a smaller value so that the connection resources can be properly released.

Related commands: **display ssh server**.

Examples

```
# Set the idle timeout period for SFTP user connections to 500 minutes.
<Sysname> system-view
[Sysname] sftp server idle-timeout 500
```

SFTP client configuration commands

bye

Syntax

bye

View

SFTP client view

Default level

3: Manage level

Parameters

None

Description

Use **bye** to terminate the connection with a remote SFTP server and return to user view.

This command functions as the **exit** and **quit** commands.

Examples

```
# Terminate the connection with the remote SFTP server.
sftp-client> bye
Bye
Connection closed.
<Sysname>
```

cd

Syntax

cd [*remote-path*]

View

SFTP client view

Default level

3: Manage level

Parameters

remote-path: Specifies the name of a path on the server.

Description

Use **cd** to change the working path on a remote SFTP server. With the argument not specified, the command displays the current working path.

You can use the **cd ..** command to return to the upper-level directory.

You can use the **cd /** command to return to the root directory of the system.

Examples

Change the working path to **new1**.

```
sftp-client> cd new1
Current Directory is:
/new1
```

cdup

Syntax

cdup

View

SFTP client view

Default level

3: Manage level

Parameters

None

Description

Use **cdup** to return to the upper-level directory.

Examples

From the current working directory **/new1**, return to the upper-level directory.

```
sftp-client> cdup
Current Directory is:
/
```

delete

Syntax

delete *remote-file*&<1-10>

View

SFTP client view

Default level

3: Manage level

Parameters

remote-file&<1-10>: Specifies the names of files on the server. &<1-10> means that you can provide up to 10 filenames, which are separated by space.

Description

Use **delete** to delete files from a server.

This command functions as the **remove** command.

Examples

```
# Delete file temp.c from the server.
sftp-client> delete temp.c
The following files will be deleted:
/temp.c
Are you sure to delete it? [Y/N]:y
This operation might take a long time. Please wait...

File successfully Removed
```

dir

Syntax

dir [**-a** | **-l**] [*remote-path*]

View

SFTP client view

Default level

3: Manage level

Parameters

-a: Displays the names of the files and sub-directories under the specified directory.

-l: Displays the detailed information of the files and sub-directories under the specified directory in the form of a list.

remote-path: Specifies the name of the directory to be queried.

Description

Use **dir** to display information about the files and sub-directories under a directory.

With the **-a** and **-l** keyword not specified, the command displays detailed information of the files and sub-directories under the specified directory in the form of a list.

With the *remote-path* not specified, the command displays information about the files and sub-directories of the current working directory.

This command functions as the **ls** command.

Examples

Display detailed information about the files and sub-directories under the current working directory in the form of a list.

```
sftp-client> dir
-rwxrwxrwx  1 noone  nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup        283 Aug 24 07:39 pubkey1
-rwxrwxrwx  1 noone  nogroup        225 Sep 28 08:28 pub1
drwxrwxrwx  1 noone  nogroup         0 Sep 28 08:24 new1
drwxrwxrwx  1 noone  nogroup         0 Sep 28 08:18 new2
-rwxrwxrwx  1 noone  nogroup        225 Sep 28 08:30 pub2
```

display sftp client source

Syntax

```
display sftp client source [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display sftp client source** to display the source IP address or source interface set for the SFTP client.

If neither source IP address nor source interface is specified for the SFTP client, the system displays the message "Neither source IP address nor source interface was specified for the SFTP client."

Related commands: **sftp client source**.

Examples

Display the source IP address of the SFTP client.

```
<Sysname> display sftp client source
```

```
The source IP address you specified is 192.168.0.1
```

exit

Syntax

exit

View

SFTP client view

Default level

3: Manage level

Parameters

None

Description

Use **exit** to terminate the connection with a remote SFTP server and return to user view.

This command functions as the **bye** and **quit** commands.

Examples

```
# Terminate the connection with the remote SFTP server.
sftp-client> exit
Bye
Connection closed.
<Sysname>
```

get

Syntax

get *remote-file* [*local-file*]

View

SFTP client view

Default level

3: Manage level

Parameters

remote-file: Name of a file on the remote SFTP server.

local-file: Name for the local file.

Description

Use **get** to download a file from a remote SFTP server and save it locally.

If you do not specify the *local-file* argument, the file will be saved locally with the same name as that on the remote SFTP server.

Examples

```
# Download the file templ.c from an SFTP server and save it as temp.c locally.
sftp-client> get templ.c temp.c
Remote file:/templ.c ---> Local file: temp.c
Downloading file successfully ended
```

help

Syntax

help [**all** | *command-name*]

View

SFTP client view

Default level

3: Manage level

Parameters

all: Displays a list of all commands.

command-name: Specifies the name of a command.

Description

Use **help** to display a list of all commands or the help information of an SFTP client command.

With neither the argument nor the keyword specified, the command displays a list of all commands.

Examples

Display the help information of the **get** command.

```
sftp-client> help get
```

```
get remote-path [local-path]  Download file.Default local-path is the same
                               as remote-path
```

ls

Syntax

ls [**-a** | **-l**] [*remote-path*]

View

SFTP client view

Default level

3: Manage level

Parameters

-a: Displays the filenames and the folder names of the specified directory.

-l: Displays in a list form detailed information of the files and folders of the specified directory.

remote-path: Name of the directory to be queried.

Description

Use **ls** to display file and folder information under a directory.

With the **-a** and **-l** keyword not specified, the command displays detailed information of files and folders under the specified directory in a list form.

With the *remote-path* not specified, the command displays the file and folder information of the current working directory.

This command functions as the **dir** command.

Examples

Display in a list form detailed file and folder information under the current working directory.

```
sftp-client> ls
-rwxrwxrwx  1 noone  nogroup      1759 Aug  23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup        225 Aug  24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup        283 Aug  24 07:39 pubkey1
-rwxrwxrwx  1 noone  nogroup        225 Sep  28 08:28 publ
drwxrwxrwx  1 noone  nogroup         0 Sep  28 08:24 new1
drwxrwxrwx  1 noone  nogroup         0 Sep  28 08:18 new2
-rwxrwxrwx  1 noone  nogroup        225 Sep  28 08:30 pub2
```

mkdir

Syntax

mkdir *remote-path*

View

SFTP client view

Default level

3: Manage level

Parameters

remote-path: Specifies the name for the directory on a remote SFTP server.

Description

Use **mkdir** to create a directory on a remote SFTP server.

Examples

Create a directory named **test** on the remote SFTP server.

```
sftp-client> mkdir test
New directory created
```

put

Syntax

put *local-file* [*remote-file*]

View

SFTP client view

Default level

3: Manage level

Parameters

local-file: Specifies the name of a local file.

remote-file: Specifies the name for the file on a remote SFTP server.

Description

Use **put** to upload a local file to a remote SFTP server.

If the *remote-file* argument is not specified, the file will be saved remotely with the same name as the local one.

Examples

```
# Upload local file temp.c to the remote SFTP server and save it as templ.c.
sftp-client> put temp.c templ.c
Local file:temp.c ---> Remote file: /templ.c
Uploading file successfully ended
```

pwd

Syntax

pwd

View

SFTP client view

Default level

3: Manage level

Parameters

None

Description

Use **pwd** to display the current working directory of a remote SFTP server.

Examples

```
# Display the current working directory of the remote SFTP server.
sftp-client> pwd
/
```

quit

Syntax

quit

View

SFTP client view

Default level

3: Manage level

Parameters

None

Description

Use **quit** to terminate the connection with a remote SFTP server and return to user view.

This command functions as the **bye** and **exit** commands.

Examples

```
# Terminate the connection with the remote SFTP server.
```

```
sftp-client> quit
Bye
Connection closed.
<Sysname>
```

remove

Syntax

remove *remote-file*&<1-10>

View

SFTP client view

Default level

3: Manage level

Parameters

remote-file&<1-10>: Specifies names of files on an SFTP server. &<1-10> means that you can provide up to 10 filenames, which are separated by space.

Description

Use **remove** to delete files from a remote server.

This command functions as the **delete** command.

Examples

```
# Delete file temp.c from the server.
sftp-client> remove temp.c
The following files will be deleted:
/temp.c
Are you sure to delete it? [Y/N]:y
This operation might take a long time.Please wait...

File successfully Removed
```

rename

Syntax

rename *oldname newname*

View

SFTP client view

Default level

3: Manage level

Parameters

oldname: Specifies the name of an existing file or directory.

newname: Specifies the new name for the file or directory.

Description

Use **rename** to change the name of a file or directory on an SFTP server.

Examples

Change the name of a file on the SFTP server from **temp1.c** to **temp2.c**.

```
sftp-client> rename temp1.c temp2.c
File successfully renamed
```

rmdir

Syntax

rmdir *remote-path*&<1-10>

View

SFTP client view

Default level

3: Manage level

Parameters

remote-path&<1-10>: Specifies the names of directories on the remote SFTP server. &<1-10> means that you can provide up to 10 directory names that are separated by space.

Description

Use **rmdir** to delete the specified directories from an SFTP server.

Examples

On the SFTP server, delete directory **temp1** in the current directory.

```
sftp-client> rmdir temp1
Directory successfully removed
```

sftp

Syntax

In non-FIPS mode:

```
sftp server [ port-number ] [ identity-key { dsa | rsa } | prefer-ctos-cipher { 3des | aes128 | des } |
prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1
| dh-group14 } | prefer-stoc-cipher { 3des | aes128 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1
| sha1-96 } ] *
```

In FIPS mode:

```
sftp server [ port-number ] [ identity-key rsa | prefer-ctos-cipher { aes128 | aes256 } | prefer-ctos-hmac
{ sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher { aes128 | aes256 } | prefer-stoc-hmac
{ sha1 | sha1-96 } ] *
```

View

User view

Default level

3: Manage level

Parameters

server: IPv4 address or host name of the server, a case-insensitive string of 1 to 20 characters.

port-number: Port number of the server, in the range of 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

prefer-ctos-cipher: Specifies the preferred encryption algorithm from client to server. The default is **aes128**.

- **3des:** Specifies the encryption algorithm **3des-cbc**.
- **aes128:** Specifies the encryption algorithm **aes128-cbc**.
- **aes256:** Specifies the encryption algorithm **aes256-cbc**.
- **des:** Specifies the encryption algorithm **des-cbc**.

prefer-ctos-hmac: Specifies the preferred HMAC algorithm from client to server. The default is **sha1-96**.

- **md5:** Specifies the HMAC algorithm **hmac-md5**.
- **md5-96:** Specifies the HMAC algorithm **hmac-md5-96**.
- **sha1:** Specifies the HMAC algorithm **hmac-sha1**.
- **sha1-96:** Specifies the HMAC algorithm **hmac-sha1-96**.

prefer-kex: Specifies the preferred key exchange algorithm. The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.

- **dh-group-exchange:** Specifies the key exchange algorithm **diffie-hellman-group-exchange-sha1**.
- **dh-group1:** Specifies the key exchange algorithm **diffie-hellman-group1-sha1**.
- **dh-group14:** Specifies the key exchange algorithm **diffie-hellman-group14-sha1**.

prefer-stoc-cipher: Specifies the preferred encryption algorithm from server to client. The default is **aes128**.

prefer-stoc-hmac: Specifies the preferred HMAC algorithm from server to client. The default is **sha1-96**.

Description

Use **sftp** to establish a connection to a remote IPv4 SFTP server and enter SFTP client view.

When the server adopts publickey authentication to authenticate a client, the client needs to get the local private key for digital signature. As the publickey authentication uses either RSA or DSA algorithm, you must specify an algorithm for the client (by using the **identity-key** keyword) in order to get the correct data for the local private key.

Examples

Connect to SFTP server 10.1.1.2, using the following connection scheme:

- Preferred key exchange algorithm: **dh-group1**.
- Preferred encryption algorithm from server to client: **aes128**.
- Preferred HMAC algorithm from client to server: **md5**.
- Preferred HMAC algorithm from server to client: **sha1-96**.

```
<Sysname> sftp 10.1.1.2 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac  
md5 prefer-stoc-hmac sha1-96
```

```
Input Username:
```


sftp client dscp

Syntax

```
sftp client dscp dscp-value  
undo sftp client dscp
```

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in the IPv4 packets sent by the SFTP client, which ranges from 0 to 63.

Description

Use **sftp client dscp** to set the DSCP value for IPv4 packets sent by the SFTP client.

Use **undo sftp client dscp** to restore the default.

By default, the DSCP value in IPv4 packets sent by the SFTP client is 16.

Examples

```
# Set the DSCP value to 30 for IPv4 packets sent by the SFTP client.  
<Sysname> system-view  
[Sysname] sftp client dscp 30
```

sftp client ipv6 dscp

Syntax

```
sftp client ipv6 dscp dscp-value  
undo sftp client ipv6 dscp
```

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in the IPv6 packets sent by the SFTP client, which ranges from 0 to 63.

Description

Use **sftp client ipv6 dscp** to set the DSCP value for IPv6 packets sent by the SFTP client.

Use **undo sftp client ipv6 dscp** to restore the default.

By default, the DSCP value in IPv6 packets sent by the SFTP client is 8.

Examples

```
# Set the DSCP value to 30 for IPv6 packets sent by the SFTP client.
```

```
<Sysname> system-view
[Sysname] sftp client ipv6 dscp 30
```

sftp client ipv6 source

Syntax

```
sftp client ipv6 source { ipv6 ipv6-address | interface interface-type interface-number }
undo sftp client ipv6 source
```

View

System view

Default level

3: Manage level

Parameters

ipv6 *ipv6-address*: Specifies a source IPv6 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description

Use **sftp client ipv6 source** to specify the source IPv6 address or source interface for an SFTP client.

Use **undo sftp client ipv6 source** to remove the configuration.

By default, an SFTP client uses the IPv6 address of the interface specified by the route of the device to access the SFTP server.

To make sure the SFTP client and the SFTP server can communicate with each other, and to improve the manageability of SFTP clients in the authentication service, HP recommends you specify a loopback interface as the source interface.

Related commands: **display sftp client source**.

Examples

```
# Specify the source IPv6 address of the SFTP client as 2:2::2:2.
```

```
<Sysname> system-view
[Sysname] sftp client ipv6 source ipv6 2:2::2:2
```

sftp client source

Syntax

```
sftp client source { ip ip-address | interface interface-type interface-number }
undo sftp client source
```

View

System view

Default level

3: Manage level

Parameters

ip *ip-address*: Specifies a source IPv4 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description

Use **sftp client source** to specify the source IPv4 address or interface of an SFTP client.

Use **undo sftp client source** to remove the configuration.

By default, an SFTP client uses the IP address of the interface specified by the route of the device to access the SFTP server.

To make sure the SFTP client and the SFTP server can communicate with each other, and to improve the manageability of SFTP clients in the authentication service, HP recommends you specify a loopback interface as the source interface.

Related commands: **display sftp client source**.

Examples

Specify the source IP address of the SFTP client as 192.168.0.1.

```
<Sysname> system-view
[Sysname] sftp client source ip 192.168.0.1
```

sftp ipv6

Syntax

In non-FIPS mode:

```
sftp ipv6 server [ port-number ] [ identity-key { dsa | rsa } | prefer-ctos-cipher { 3des | aes128 | des } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1 | dh-group14 } | prefer-stoc-cipher { 3des | aes128 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } ] *
```

In FIPS mode:

```
sftp ipv6 server [ port-number ] [ identity-key rsa | prefer-ctos-cipher { aes128 | aes256 } | prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher { aes128 | aes256 } | prefer-stoc-hmac { sha1 | sha1-96 } ] *
```

View

User view

Default level

3: Manage level

Parameters

server: Specifies an IPv6 address or host name of the server, a case-insensitive string of 1 to 46 characters.

port-number: Specifies the port number of the server, in the range of 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

prefer-ctos-cipher: Specifies the preferred encryption algorithm from client to server. The default is **aes128**.

- **3des**: Specifies the encryption algorithm **3des-cbc**.
- **aes128**: Specifies the encryption algorithm **aes128-cbc**.
- **aes256**: Specifies the encryption algorithm **aes256-cbc**.

- **des**: Specifies the encryption algorithm **des-cbc**.

prefer-ctos-hmac: Specifies the preferred HMAC algorithm from client to server. The default is **sha1-96**.

- **md5**: Specifies the HMAC algorithm **hmac-md5**.
- **md5-96**: Specifies the HMAC algorithm **hmac-md5-96**.
- **sha1**: Specifies the HMAC algorithm **hmac-sha1**.
- **sha1-96**: Specifies the HMAC algorithm **hmac-sha1-96**.

prefer-kex: Specifies the preferred key exchange algorithm. The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.

- **dh-group-exchange**: Specifies the key exchange algorithm **diffie-hellman-group-exchange-sha1**.
- **dh-group1**: Specifies the key exchange algorithm **diffie-hellman-group1-sha1**.
- **dh-group14**: Specifies the key exchange algorithm **diffie-hellman-group14-sha1**.

prefer-stoc-cipher: Specifies the preferred encryption algorithm from server to client. The default is **aes128**.

prefer-stoc-hmac: Specifies the preferred HMAC algorithm from server to client. The default is **sha1-96**.

Description

Use **sftp ipv6** to establish a connection to a remote IPv6 SFTP server and enter SFTP client view.

When the server adopts publickey authentication to authenticate a client, the client needs to get the local private key for digital signature. As the publickey authentication uses either RSA or DSA algorithm, you must specify an algorithm for the client (by using the **identity-key** keyword) in order to get the correct data for the local private key.

Examples

Connect to server 2:5::8:9, using the following connection scheme:

- Preferred key exchange algorithm: **dh-group1**.
- Preferred encryption algorithm from server to client: **aes128**.
- Preferred HMAC algorithm from client to server: **md5**.
- Preferred HMAC algorithm from server to client: **sha1-96**.

```
<Sysname> sftp ipv6 2:5::8:9 prefer-kex dh-group1 prefer-stoc-cipher aes128
prefer-ctos-hmac md5 prefer-stoc-hmac sha1-96
Input Username:
```

SCP configuration commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

SCP client configuration commands

scp

Command

In non-FIPS mode:

```
scp [ ipv6 ] server [ port-number ] { get | put } source-file-path [ destination-file-path ] [ identity-key { dsa | rsa } | prefer-ctos-cipher { 3des | aes128 | des } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1 | dh-group14 } | prefer-stoc-cipher { 3des | aes128 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } ] *
```

In FIPS mode:

```
scp [ ipv6 ] server [ port-number ] { get | put } source-file-path [ destination-file-path ] [ identity-key rsa | prefer-ctos-cipher { aes128 | aes256 } | prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher { aes128 | aes256 } | prefer-stoc-hmac { sha1 | sha1-96 } ] *
```

View

User view

Default level

3: Manage level

Parameters

ipv6: Specifies the type of the server as IPv6. If you want to specify an IPv4 server, do not specify this keyword.

server: Specifies an IPv4 or IPv6 server by its address or host name. For an IPv4 server, it is a case-insensitive string of 1 to 20 characters. For an IPv6 server, it is a case-insensitive string of 1 to 46 characters.

port-number: Specifies the port number of the server, in the range of 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

- **dsa**: Specifies the public key algorithm **dsa**.
- **rsa**: Specifies the public key algorithm **rsa**.

prefer-ctos-cipher: Specifies the preferred encryption algorithm from client to server. The default is **aes128**.

- **3des**: Specifies the encryption algorithm **3des-cbc**.
- **aes128**: Specifies the encryption algorithm **aes128-cbc**.
- **aes256**: Specifies the encryption algorithm **aes256-cbc**.

- **des**: Specifies the encryption algorithm **des-cbc**.

prefer-ctos-hmac: Specifies the preferred HMAC algorithm from client to server. The default is **sha1-96**.

- **md5**: Specifies the HMAC algorithm **hmac-md5**.
- **md5-96**: Specifies the HMAC algorithm **hmac-md5-96**.
- **sha1**: Specifies the HMAC algorithm **hmac-sha1**.
- **sha1-96**: Specifies the HMAC algorithm **hmac-sha1-96**.

prefer-kex: Specifies the preferred key exchange algorithm. The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.

- **dh-group-exchange**: Specifies the key exchange algorithm **diffie-hellman-group-exchange-sha1**.
- **dh-group1**: Specifies the key exchange algorithm **diffie-hellman-group1-sha1**.
- **dh-group14**: Specifies the key exchange algorithm **diffie-hellman-group14-sha1**.

prefer-stoc-cipher: Specifies the preferred encryption algorithm from server to client. The default is **aes128**.

prefer-stoc-hmac: Specifies the preferred HMAC algorithm from server to client. The default is **sha1-96**.

Description

Use **scp** to transfer files with an SCP server.

When the server adopts publickey authentication to authenticate a client, the client needs to get the local private key for digital signature. As the publickey authentication uses either RSA or DSA algorithm, you must specify an algorithm for the client (by using the **identity-key** keyword) in order to get the correct data for the local private key.

Examples

Connect to the SCP server 192.168.0.1, download the file **remote.bin** from the SCP server, save it locally and change the file name to **local.bin**

```
<Sysname> scp 192.168.0.1 get remote.bin local.bin
```

SSL configuration commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

ciphersuite

Syntax

In non-FIPS mode:

```
ciphersuite [ rsa_3des_ede_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha |  
rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha ] *
```

In FIPS mode:

```
ciphersuite [ dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_256_cbc_sha | rsa_aes_128_cbc_sha |  
rsa_aes_256_cbc_sha ] *
```

View

SSL server policy view

Default level

2: System level

Parameters

dhe_rsa_aes_128_cbc_sha: Specifies the key exchange algorithm of DH_RSA, the data encryption algorithm of 128-bit AES_CBC, and the MAC algorithm of SHA.

dhe_rsa_aes_256_cbc_sha: Specifies the key exchange algorithm of DH_RSA, the data encryption algorithm of 256-bit AES_CBC, and the MAC algorithm of SHA.

rsa_3des_ede_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 3DES_EDE_CBC, and the MAC algorithm of SHA.

rsa_aes_128_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit AES_CBC, and the MAC algorithm of SHA.

rsa_aes_256_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 256-bit AES_CBC, and the MAC algorithm of SHA.

rsa_des_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of DES_CBC, and the MAC algorithm of SHA.

rsa_rc4_128_md5: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of MD5.

rsa_rc4_128_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of SHA.

Description

Use **ciphersuite** to specify the cipher suites for an SSL server policy to support.

By default, an SSL server policy supports all cipher suites.

With no keyword specified, the command configures an SSL server policy to support all cipher suites.
If you execute the command repeatedly, the last one takes effect.
Related commands: **display ssl server-policy**.

Examples

```
# Configure SSL server policy policy1 to support cipher suites rsa_rc4_128_md5 and rsa_rc4_128_sha.
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] ciphersuite rsa_rc4_128_md5 rsa_rc4_128_sha
```

client-verify enable

Syntax

client-verify enable

undo client-verify enable

View

SSL server policy view

Default level

2: System level

Parameters

None

Description

Use **client-verify enable** to configure the SSL server to require the client to pass certificate-based authentication.

Use **undo client-verify enable** to restore the default.

By default, the SSL server does not require certificate-based SSL client authentication.

If you configure the **client-verify enable** command and enable the SSL client weak authentication function, whether the client must be authenticated is up to the client. If the client chooses to be authenticated, the client must pass authentication before accessing the SSL server; otherwise, the client can access the SSL server without authentication.

If you configure the **client-verify enable** command but disable the SSL client weak authentication function, the SSL client must pass authentication before accessing the SSL server.

Related commands: **client-verify weaken** and **display ssl server-policy**.

Examples

```
# Configure the SSL server to require certificate-based SSL client authentication.
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] client-verify enable
```


client-verify weaken

Syntax

client-verify weaken
undo client-verify weaken

View

SSL server policy view

Default level

2: System level

Parameters

None

Description

Use **client-verify weaken** to enable SSL client weak authentication.

Use **undo client-verify weaken** to restore the default.

By default, SSL client weak authentication is disabled.

If the SSL server requires certificate-based client authentication and the SSL client weak authentication function is enabled, whether the client must be authenticated is up to the client. If the client chooses to be authenticated, the client must pass authentication before accessing the SSL server; otherwise, the client can access the SSL server without authentication.

If the SSL server requires certificate-based client authentication and SSL client weak authentication is disabled, the SSL client must pass authentication before accessing the SSL server.

NOTE:

The **client-verify weaken** command takes effect only when the SSL server requires certificate-based client authentication.

Related commands: **client-verify enable** and **display ssl server-policy**.

Examples

```
# Enable SSL client weak authentication.  
<Sysname> system-view  
[Sysname] ssl server-policy policy1  
[Sysname-ssl-server-policy-policy1] client-verify enable  
[Sysname-ssl-server-policy-policy1] client-verify weaken
```

close-mode wait

Syntax

close-mode wait
undo close-mode wait

View

SSL server policy view

Default level

2: System level

Parameters

None

Description

Use **close-mode wait** to set the SSL connection close mode to wait mode. In this mode, after sending a close-notify alert message to a client, the server does not close the connection until it receives a close-notify alert message from the client.

Use **undo close-mode wait** to restore the default.

By default, an SSL server sends a close-notify alert message to the client and closes the connection without waiting for the close-notify alert message from the client.

Related commands: **display ssl server-policy**.

Examples

```
# Set the SSL connection close mode to wait.
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] close-mode wait
```

display ssl client-policy

Syntax

display ssl client-policy { *policy-name* | **all** } [[{ **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

policy-name: SSL client policy name, a case-insensitive string of 1 to 16 characters.

all: Displays information about all SSL client policies.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ssl client-policy** to display information about SSL client policies.

Examples

```
# Display information about SSL client policy policy1.
<Sysname> display ssl client-policy policy1
```

```

SSL Client Policy: policy1
  SSL Version: SSL 3.0
  PKI Domain: 1
  Prefer Ciphersuite:
    RSA_RC4_128_SHA
  Server-verify: enabled

```

Table 50 Command output

Field	Description
SSL Client Policy	SSL client policy name
SSL Version	Version of the protocol used by the SSL client policy, SSL 3.0 or TLS 1.0
PKI Domain	PKI domain of the SSL client policy
Prefer Ciphersuite	Preferred cipher suite of the SSL client policy
Server-verify	Whether server authentication is enabled for the SSL client policy

display ssl server-policy

Syntax

```
display ssl server-policy { policy-name | all } [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

policy-name: SSL server policy name, a case-insensitive string of 1 to 16 characters.

all: Displays information about all SSL server policies.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ssl server-policy** to display information about SSL server policies.

Examples

Display information about SSL server policy **policy1**.

```

<Sysname> display ssl server-policy policy1
  SSL Server Policy: policy1
  PKI Domain: domain1
  Ciphersuite:
    RSA_RC4_128_MD5

```

```

RSA_RC4_128_SHA
RSA_DES_CBC_SHA
RSA_3DES_EDE_CBC_SHA
RSA_AES_128_CBC_SHA
RSA_AES_256_CBC_SHA
Handshake Timeout: 3600
Close-mode: wait disabled
Session Timeout: 3600
Session Cachesize: 500
Client-verify: disabled
Client-verify weaken: disabled

```

Table 51 Command output

Field	Description
SSL Server Policy	SSL server policy name.
PKI Domain	PKI domain used by the SSL server policy. If no PKI domain is specified for the SSL server policy, nothing is displayed for this field, and the SSL server generates a certificate for itself and does not obtain a certificate from a CA server.
Ciphersuite	Cipher suites supported by the SSL server policy.
Handshake Timeout	Handshake timeout time of the SSL server policy, in seconds.
Close-mode	Close mode of the SSL server policy: <ul style="list-style-type: none"> wait disabled—In this mode, the server sends a close-notify alert message to the client and then closes the connection immediately without waiting for the close-notify alert message of the client. wait enabled—In this mode, the server sends a close-notify alert message to the client and then waits for the close-notify alert message of the client. Only after receiving the expected message, does the server close the connection.
Session Timeout	Session timeout time of the SSL server policy, in seconds.
Session Cachesize	Maximum number of buffered sessions of the SSL server policy.
Client-verify	Whether the SSL server policy requires the client to be authenticated.

handshake timeout

Syntax

handshake timeout *time*

undo handshake timeout

View

SSL server policy view

Default level

2: System level

Parameters

time: Handshake timeout time in seconds, in the range of 180 to 7200.

Description

Use **handshake timeout** to set the handshake timeout time for an SSL server policy.

Use **undo handshake timeout** to restore the default.

By default, the handshake timeout time is 3600 seconds.

If the SSL server does not receive any packet from the SSL client before the handshake timeout time expires, the SSL server will terminate the handshake process.

Related commands: **display ssl server-policy**.

Examples

Set the handshake timeout time of SSL server policy **policy1** to 3000 seconds.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] handshake timeout 3000
```

pki-domain

Syntax

pki-domain *domain-name*

undo pki-domain

View

SSL server policy view, SSL client policy view

Default level

2: System level

Parameters

domain-name: Name of a PKI domain, a case-insensitive string of 1 to 15 characters.

Description

Use **pki-domain** to specify a PKI domain for an SSL server policy or SSL client policy.

Use **undo pki-domain** to restore the default.

By default, no PKI domain is configured for an SSL server policy or SSL client policy.

If you do not specify a PKI domain for an SSL server policy, the SSL server generates a certificate for itself rather than obtaining one from a CA server.

Related commands: **display ssl server-policy** and **display ssl client-policy**.

Examples

Configure SSL server policy **policy1** to use PKI domain **server-domain**.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] pki-domain server-domain
```

Configure SSL client policy **policy1** to use PKI domain **client-domain**.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] pki-domain client-domain
```

prefer-cipher

Syntax

In non-FIPS mode:

```
prefer-cipher { rsa_3des_ede_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha |  
rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha }
```

```
undo prefer-cipher
```

In FIPS mode:

```
prefer-cipher { dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_256_cbc_sha | rsa_aes_128_cbc_sha |  
rsa_aes_256_cbc_sha }
```

```
undo prefer-cipher
```

View

SSL client policy view

Default level

2: System level

Parameters

dhe_rsa_aes_128_cbc_sha: Specifies the key exchange algorithm of DH_RSA, the data encryption algorithm of 128-bit AES_CBC, and the MAC algorithm of SHA.

dhe_rsa_aes_256_cbc_sha: Specifies the key exchange algorithm of DH_RSA, the data encryption algorithm of 256-bit AES_CBC, and the MAC algorithm of SHA.

rsa_3des_ede_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 3DES_EDE_CBC, and the MAC algorithm of SHA.

rsa_aes_128_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit AES_CBC, and the MAC algorithm of SHA.

rsa_aes_256_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 256-bit AES_CBC, and the MAC algorithm of SHA.

rsa_des_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of DES_CBC, and the MAC algorithm of SHA.

rsa_rc4_128_md5: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of MD5.

rsa_rc4_128_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of SHA.

Description

Use **prefer-cipher** to specify the preferred cipher suite for an SSL client policy.

Use **undo prefer-cipher** to restore the default.

By default, the preferred cipher suite for an SSL client policy is **rsa_rc4_128_md5**.

Related commands: **display ssl client-policy**.

Examples

```
# Set the preferred cipher suite for SSL client policy policy1 to rsa_aes_128_cbc_sha.  
<Sysname> system-view
```

```
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] prefer-cipher rsa_aes_128_cbc_sha
```

server-verify enable

Syntax

```
server-verify enable
undo server-verify enable
```

View

SSL client policy view

Default level

2: System level

Parameters

None

Description

Use **server-verify enable** to enable certificate-based SSL server authentication so that the SSL client authenticates the server by the server's certificate during the SSL handshake process.

Use **undo server-verify enable** to disable certificate-based SSL server authentication. When certificate-based SSL server authentication is disabled, it is assumed that the SSL server is valid.

By default, certificate-based SSL server authentication is enabled.

Related commands: **display ssl client-policy**.

Examples

```
# Enable certificate-based SSL server authentication.
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] server-verify enable
```

session

Syntax

```
session { cachesize size | timeout time } *
undo session { cachesize | timeout } *
```

View

SSL server policy view

Default level

2: System level

Parameters

cachesize size: Specifies the maximum number of cached sessions, in the range of 100 to 1000.

timeout time: Specifies the caching timeout time in seconds, in the range of 1800 to 72000.

Description

Use **session** to set the maximum number of cached sessions and the caching timeout time.

Use **undo session** to restore the default.

By default, the maximum number of cached sessions is 500 and the caching timeout time is 3600 seconds.

It is a complicated process to use the SSL handshake protocol to negotiate session parameters and establish sessions. To simplify the process, SSL allows reusing negotiated session parameters to establish sessions. This feature requires that the SSL server maintain information about existing sessions.

The number of cached sessions and the session information caching time are limited:

- If the number of sessions in the cache reaches the maximum, SSL rejects to cache new sessions.
- If a session has been cached for a period equal to the caching timeout time, SSL will remove the information of the session.

Related commands: **display ssl server-policy**.

Examples

Set the caching timeout time to 4000 seconds and the maximum number of cached sessions to 600.

```
<Sysname> system-view
```

```
[Sysname] ssl server-policy policy1
```

```
[Sysname-ssl-server-policy-policy1] session timeout 4000 cachesize 600
```

ssl client-policy

Syntax

ssl client-policy *policy-name*

undo ssl client-policy { *policy-name* | **all** }

View

System view

Default level

2: System level

Parameters

policy-name: SSL client policy name, a case-insensitive string of 1 to 16 characters, which cannot be **a**, **al**, or **all**.

all: Specifies all SSL client policies.

Description

Use **ssl client-policy** to create an SSL policy and enter its view.

Use **undo ssl client-policy** to delete SSL client policies.

Related commands: **display ssl client-policy**.

Examples

Create SSL client policy **policy1** and enter its view.

```
<Sysname> system-view
```

```
[Sysname] ssl client-policy policy1
```


[Sysname-ssl-client-policy-policy1]

ssl server-policy

Syntax

ssl server-policy *policy-name*

undo ssl server-policy { *policy-name* | **all** }

View

System view

Default level

2: System level

Parameters

policy-name: SSL server policy name, a case-insensitive string of 1 to 16 characters, which cannot be "a", "al", or "all".

all: Specifies all SSL server policies.

Description

Use **ssl server-policy** to create an SSL server policy and enter its view.

Use **undo ssl server-policy** to delete SSL server policies.

You cannot delete an SSL server policy that has been associated with one or more application layer protocols.

Related commands: **display ssl server-policy**.

Examples

Create SSL server policy **policy1** and enter its view.

```
<Sysname> system-view
```

```
[Sysname] ssl server-policy policy1
```

```
[Sysname-ssl-server-policy-policy1]
```

version

Syntax

In non-FIPS mode:

version { **ssl3.0** | **tls1.0** }

undo version

In FIPS mode:

version **tls1.0**

undo version

View

SSL client policy view

Default level

2: System level

Parameters

ssl3.0: Specifies SSL 3.0.

tls1.0: Specifies TLS 1.0.

Description

Use **version** to specify the SSL protocol version for an SSL client policy.

Use **undo version** to restore the default.

By default, the SSL protocol version for an SSL client policy is TLS 1.0.

Related commands: **display ssl client-policy**.

Examples

Specify the SSL protocol version for SSL client policy **policy1** as TLS 1.0.

```
<Sysname> system-view
```

```
[Sysname] ssl client-policy policy1
```

```
[Sysname-ssl-client-policy-policy1] version tls1.0
```

TCP attack protection configuration commands

display tcp status

Syntax

display tcp status [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display tcp status** to display status of all TCP connections for monitoring TCP connections.

Examples

Display status of all TCP connections.

```
<Sysname> display tcp status
```

```
*: TCP MD5 Connection
```

TCPCB	Local Add:port	Foreign Add:port	State
03e37dc4	0.0.0.0:4001	0.0.0.0:0	Listening
04217174	100.0.0.204:23	100.0.0.253:65508	Established

Table 52 Command output

Field	Description
: TCP MD5 Connection	If the status information of a TCP connection contains an asterisk (), the TCP adopts the MD5 algorithm for authentication.
TCPCB	TCP control block.
Local Add:port	Local IP address and port number.
Foreign Add:port	Remote IP address and port number.
State	State of the TCP connection.

tcp syn-cookie enable

Syntax

tcp syn-cookie enable

undo tcp syn-cookie enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **tcp syn-cookie enable** to enable the SYN Cookie feature to protect the device against SYN Flood attacks.

Use **undo tcp syn-cookie enable** to disable the SYN Cookie feature.

By default, the SYN Cookie feature is enabled.

Examples

Enable the SYN Cookie feature.

```
<Sysname> system-view
```

```
[Sysname] tcp syn-cookie enable
```

IP source guard configuration commands

display ip source binding

Syntax

```
display ip source binding [ static ] [ interface interface-type interface-number | ip-address ip-address | mac-address mac-address ] [ slot slot-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

static: Displays static IPv4 source guard entries, including global static IPv4 binding entries and port-based static IPv4 binding entries. If you do not specify this keyword, the command displays all static and dynamic IPv4 source guard entries.

interface *interface-type interface-number*: Displays IPv4 source guard entries of the interface specified by its type and number.

ip-address *ip-address*: Displays IPv4 source guard entries of an IP address.

mac-address *mac-address*: Displays IPv4 source guard entries of a MAC address (in the format H-H-H).

slot *slot-number*: Displays IPv4 source guard entries on an IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip source binding** to display IPv4 source guard entries.

Note the following when you do not use the **static** keyword:

If you do not specify any other parameters either, the command displays static and dynamic IPv4 binding entries on all ports and the global static IPv4 binding entries on the master device.

Note the following when you use the **static** keyword:

If you do not specify any other parameters, the command displays all global and port-based static IPv4 binding entries.

Related commands: **ip verify source** and **ip source binding**.

Examples

Display all IPv4 source guard entries.

```
<Sysname> display ip source binding
```

Total entries found: 3

MAC Address	IP Address	VLAN	Interface	Type
040a-0000-4000	10.1.0.9	N/A	GE1/0/1	Static
040a-0000-3000	10.1.0.8	2	GE1/0/2	DHCP-SNP
040a-0000-2000	10.1.0.7	2	GE1/0/2	DHCP-SNP

Display all static IPv4 source guard entries.

```
<Sysname> display ip source binding static
```

Total entries found: 3

MAC Address	IP Address	VLAN	Interface	Type
040a-0000-0011	10.1.1.11	N/A	N/A	Static
040a-0000-0012	10.1.0.12	N/A	GE1/0/3	Static
040a-0000-0013	10.1.0.13	N/A	GE1/0/3	Static

Table 53 Command output

Field	Description
Total entries found	Total number of found entries
MAC Address	MAC address of the IP source guard entry. N/A means that no MAC address is bound in the entry.
IP Address	IP address of the IP source guard entry. N/A means that no IP address is bound in the entry.
VLAN	VLAN bound to the IP source guard entry. N/A means that no VLAN information exists in the entry.
Interface	Interface of the IPv4 source guard entry
Type	Type of the IPv4 source guard entry: <ul style="list-style-type: none">• Static—Static IPv4 binding entry• DHCP-SNP—Entry generated based on DHCP snooping entry• DHCP-RLY—Entry generated based on DHCP relay entry

display ipv6 source binding

Syntax

```
display ipv6 source binding [ static ] [ interface interface-type interface-number | ipv6-address  
ipv6-address | mac-address mac-address ] [ slot slot-number ] [ | { begin | exclude | include }  
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

static: Displays static IPv6 source guard entries, including global static IPv6 binding entries and port-based static IPv6 binding entries. If you do not specify this keyword, the command displays all static and dynamic IPv6 source guard entries.

interface *interface-type interface-number*: Displays the IPv6 source guard entries of an interface.

ipv6-address *ipv6-address*: Displays the IPv6 source guard entries of an IPv6 address.

mac-address *mac-address*: Displays the IPv6 source guard entries of a MAC address. The MAC address must be in the format H-H-H.

slot *slot-number*: Displays the IPv6 source guard entries on an IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 source binding** to display IPv6 source guard entries.

Note the following when you do not use the **static** keyword:

- If you do not specify any other parameters either, the command displays static and dynamic IPv6 binding entries on all ports and the global static IPv6 binding entries on the master device.

Note the following when you use the **static** keyword:

- If you do not specify any other parameters, the command displays all global and port-based static IPv6 binding entries.

Related commands: **ipv6 verify source** and **ipv6 source binding**.

Examples

Display all IPv6 source guard entries.

```
<Sysname> display ipv6 source binding
```

Total entries found: 4

MAC Address	IP Address	VLAN	Interface	Type
040a-0000-0013	2001::4	N/A	N/A	Static-IPv6
040a-0000-0001	2001::1	N/A	GE1/0/1	Static-IPv6
040a-0000-0001	2001::3	2	GE1/0/1	DHCPv6-SNP
040a-0000-0002	2001::4	6	GE1/0/2	ND-SNP

Display all static IPv6 source guard entries.

```
<Sysname> display ipv6 source binding static
```

Total entries found: 3

MAC Address	IP Address	VLAN	Interface	Type
040a-0000-0011	2001::3	N/A	N/A	Static-IPv6
040a-0000-0012	2001::4	N/A	GE1/0/3	Static-IPv6
040a-0000-0013	2001::5	N/A	GE1/0/3	Static-IPv6

Table 54 Command output

Field	Description
Total entries found	Total number of found entries
MAC Address	MAC address bound in the entry. N/A means that no MAC address is bound in the entry.
IPv6 Address	IPv6 address bound in the entry. N/A means that no IP address is bound in the entry.
VLAN	VLAN bound in the entry. N/A means that no VLAN information exists in the entry.
Interface	Interface of the binding entry. N/A means that the entry is a global static binding entry.
Type	Type of the IPv6 source guard entry: <ul style="list-style-type: none"> • Static-IPv6—Static IPv6 binding entry • DHCPv6-SNP—Entry generated based on DHCPv6 snooping entry • ND-SNP—Entry generated based on ND snooping entry

ip source binding (interface view)

Syntax

ip source binding { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

undo ip source binding { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

ip-address *ip-address*: Specifies the IPv4 address for the static binding entry. The IPv4 address cannot be 127.x.x.x, 0.0.0.0, or a multicast IP address.

mac-address *mac-address*: Specifies the MAC address for the static binding in the format H-H-H. The MAC address cannot be all 0s, all Fs (a broadcast address), or a multicast address.

vlan *vlan-id*: Specifies the VLAN for the static binding. *vlan-id* is the ID of the VLAN to be bound, in the range of 1 to 4094.

Description

Use **ip source binding** to configure a static IPv4 source guard entry on a port.

Use **undo ip source binding** to delete a static IPv4 source guard entry from a port.

By default, no static IPv4 binding entry exists on a port.

IP source guard does not use the VLAN information (if specified) in static IPv4 binding entries to filter packets.

When the ARP detection function is configured, be sure to specify the VLAN where ARP detection is configured in static IPv4 binding entries. Otherwise, ARP packets are discarded because they cannot

match any static IPv4 binding entry. For more information about the ARP detection function, see *Security Configuration Guide*.

You cannot configure the same static binding entry repeatedly on one port, but you can configure the same static entry on different ports.

You cannot configure a static binding entry on a port that is in an aggregation group.

Related commands: **display ip source binding static**.

Examples

```
# Configure a static IPv4 binding entry (IP+MAC binding) on port GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address
0001-0001-0001
```

ip source binding (system view)

Syntax

```
ip source binding ip-address ip-address mac-address mac-address
undo ip source binding { all | ip-address ip-address mac-address mac-address }
```

View

System view

Default level

2: System level

Parameters

ip-address *ip-address*: Specifies the IPv4 address for the static binding entry. The IPv4 address cannot be 127.x.x.x, 0.0.0.0, or a multicast IP address.

mac-address *mac-address*: Specifies the MAC address for the static binding in the format H-H-H. The MAC address cannot be all 0s, all Fs (a broadcast address), or a multicast address.

all: Specifies all global static binding entries.

Description

Use **ip source binding** in system view to configure a global static IPv4 source guard entry.

Use **undo ip source binding** in system view to delete one or all global static IPv4 source guard entries.

By default, no global static IPv4 binding entry exists.

A global static IPv4 binding entry takes effect on all ports.

Related commands: **display ip source binding static**.

Examples

```
# Configure a global static IPv4 binding entry to bind IP address 192.168.0.1 with MAC address
0001-0001-0001.
<Sysname> system-view
[Sysname] ip source binding ip-address 192.168.0.1 mac-address 0001-0001-0001
```

ip verify source

Syntax

```
ip verify source { ip-address | ip-address mac-address | mac-address }  
undo ip verify source
```

View

Layer 2 Ethernet interface view, VLAN interface view, port group view

Default level

2: System level

Parameters

ip-address: Binds source IPv4 addresses to the port.

ip-address mac-address: Binds source IPv4 addresses and MAC addresses to the port.

mac-address: Binds source MAC addresses to the port.

Description

Use **ip verify source** to enable the IPv4 source guard function on a port and specify the elements to be included in the port's dynamic binding entries.

Use **undo ip verify source** to restore the default.

By default, the IPv4 source guard function is disabled on a port.

After you configure the IPv4 source guard function on a port, IPv4 source guard dynamically generates IPv4 source guard entries based on the DHCP snooping entries (on a Layer 2 Ethernet port) or the DHCP-relay entries (on a VLAN interface), and all static IPv4 source guard entries on the port become effective.

You cannot configure the IPv4 source guard function on a port that is in an aggregation group.

Related commands: **display ip source binding**.

Examples

```
# Configure dynamic IPv4 binding on Layer 2 Ethernet port GigabitEthernet 1/0/1 to filter packets  
based on the source IPv4 address and MAC address.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

```
# Configure dynamic IPv4 binding on VLAN-interface 100 to filter packets based on the source IPv4  
address and MAC address.
```

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] ip verify source ip-address mac-address
```

ip verify source max-entries

Syntax

```
ip verify source max-entries number  
undo ip verify source max-entries
```

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

number: Maximum number of IPv4 source guard entries allowed on a port. The value is in the range of 0 to 640.

Description

Use **ip verify source max-entries** to set the maximum number of static and dynamic IPv4 source guard entries on a port. When the number of IPv4 binding entries on a port reaches the maximum, the port no longer allows new IPv4 binding entries.

Use **undo ip verify source max-entries** to cancel the limit set on the number of IPv4 source guard entries.

By default, the maximum number of IPv4 source guard entries allowed on a port is 640.

If the maximum number of IPv4 binding entries to be configured is smaller than the number of existing IPv4 binding entries on the port, the maximum number can be configured successfully and the existing entries are not affected. New IPv4 binding entries, however, cannot be added any more unless the number of IPv4 binding entries on the port drops below the configured maximum.

Examples

Set the maximum number of IPv4 source guard entries to 100 on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip verify source max-entries 100
```

ipv6 source binding (interface view)

Syntax

```
ipv6 source binding { ipv6-address ipv6-address | ipv6-address ipv6-address mac-address mac-address | mac-address mac-address } [ vlan vlan-id ]
```

```
undo ipv6 source binding { ipv6-address ipv6-address | ipv6-address ipv6-address mac-address mac-address | mac-address mac-address } [ vlan vlan-id ]
```

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

ipv6-address *ipv6-address*: Specifies the IPv6 address for the static binding entry. The IPv6 address cannot be an all-zero address, a multicast address, or a loopback address.

mac-address *mac-address*: Specifies the MAC address for the static binding in the format H-H-H. The MAC address cannot be all 0s, all Fs (a broadcast MAC address), or a multicast MAC address.

vlan *vlan-id*: Specifies the VLAN for the static binding. *vlan-id* is the ID of the VLAN to be bound, in the range of 1 to 4094.

Description

Use **ipv6 source binding** to configure a static IPv6 source guard entry on a port.

Use **undo ipv6 source binding** to delete a static IPv6 source guard entry from a port.

By default, no static IPv6 binding entry exists on a port.

IP source guard does not use the VLAN information (if specified) in static IPv6 binding entries to filter packets.

When the ND detection function is configured, be sure to specify the VLAN where ND detection is configured in static IPv6 binding entries. Otherwise, ND packets are discarded because they cannot match any static IPv6 binding entry. For more information about the ND detection function, see *Security Configuration Guide*.

You cannot configure the same static binding entry repeatedly on one port, but you can configure the same static entry on different ports.

You cannot configure a static binding entry on a port that is in an aggregation group.

Related commands: **display ipv6 source binding static**.

Examples

```
# Configure a static IPv6 binding entry (IP+MAC binding) on port GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 source binding ipv6-address 2001::1 mac-address
0002-0002-0002
```

ipv6 source binding (system view)

Syntax

```
ipv6 source binding ipv6-address ipv6-address mac-address mac-address
undo ipv6 source binding { all | ipv6-address ipv6-address mac-address mac-address }
```

View

System view

Default level

2: System level

Parameters

ipv6-address *ipv6-address*: Specifies the IPv6 address for the static binding entry. The IPv6 address cannot be an all-zero address, a multicast address, or a loopback address.

mac-address *mac-address*: Specifies the MAC address for the static binding in the format H-H-H. The MAC address cannot be all 0s, all Fs (a broadcast MAC address), or a multicast MAC address.

all: Specifies all global static binding entries.

Description

Use **ipv6 source binding** in system view to configure a global static IPv6 source guard entry.

Use **undo ipv6 source binding** in system view to delete one or all global static IPv6 source guard entries.

By default, no global static IPv6 binding entry exists.

A global static IPv6 binding entry takes effect on all ports.

Related commands: **display ipv6 source binding static**.

Examples

Configure a global static IPv6 binding entry to bind IP address 2001::1 with MAC address 0002-0002-0002.

```
<Sysname> system-view
```

```
[Sysname] ipv6 source binding ipv6-address 2001::1 mac-address 0002-0002-0002
```

ipv6 verify source

Syntax

ipv6 verify source { ipv6-address | ipv6-address mac-address | mac-address }

undo ipv6 verify source

View

Layer 2 Ethernet interface view, port group view

Default level

2: System level

Parameters

ipv6-address: Binds source IPv6 addresses to the port.

ipv6-address mac-address: Binds source IPv6 addresses and MAC addresses to the port.

mac-address: Binds source MAC addresses to the port.

Description

Use **ipv6 verify source** to enable the IPv6 source guard function on a port and specify the elements to be included in the port's dynamic binding entries.

Use **undo ipv6 verify source** to restore the default.

By default, the IPv6 source guard function is disabled on a port.

After you configure the IPv6 source guard function on a port, the IPv6 source guard function dynamically generates IPv6 source guard entries based on the DHCPv6 snooping entries or ND snooping entries, and all static IPv6 source guard entries become effective.

You cannot configure the IPv6 source guard function on a port that is in an aggregation group.

Related commands: **display ipv6 source binding**.

Examples

Configure dynamic IPv6 binding on Layer 2 Ethernet port GigabitEthernet 1/0/1 to filter IPv6 packets based on the source IPv6 address and MAC address.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 verify source ipv6-address mac-address
```

ipv6 verify source max-entries

Syntax

ipv6 verify source max-entries *number*

undo ipv6 verify source max-entries

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

number: Maximum number of IPv6 source guard entries allowed on a port. The value is in the range of 0 to 640.

Description

Use **ipv6 verify source max-entries** to set the maximum number of static and dynamic IPv6 source guard entries on a port. When the number of IPv6 binding entries on a port reaches the maximum, the port does not allowed new IPv6 binding entries any more.

Use **undo ipv6 verify source max-entries** to cancel the limit set on the number of IPv6 source guard entries.

By default, the maximum number of IPv6 source guard entries allowed on a port is 640.

If the maximum number of IPv6 binding entries to be configured is smaller than the number of existing IPv6 binding entries on the port, the maximum number can be configured successfully and the existing entries are not affected. New IPv6 binding entries, however, cannot be added any more unless the number of IPv6 binding entries on the port drops below the configured maximum.

Examples

Set the maximum number of IPv6 source guard entries to 100 on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 verify source max-entries 100
```

ARP attack protection configuration commands

ARP defense against IP packet attacks configuration commands

arp resolving-route enable

Syntax

```
arp resolving-route enable
undo arp resolving-route enable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **arp resolving-route enable** to enable ARP black hole routing.

Use **undo arp resolving-route enable** to disable the function.

By default, the function is enabled.

Examples

```
# Enable ARP black hole routing.
<Sysname> system-view
[Sysname] arp resolving-route enable
```

arp source-suppression enable

Syntax

```
arp source-suppression enable
undo arp source-suppression enable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **arp source-suppression enable** to enable the ARP source suppression function.

Use **undo arp source-suppression enable** to disable the function.

By default, the ARP source suppression function is disabled.

Related commands: **display arp source-suppression**.

Examples

```
# Enable the ARP source suppression function.
<Sysname> system-view
[Sysname] arp source-suppression enable
```

arp source-suppression limit

Syntax

arp source-suppression limit *limit-value*

undo arp source-suppression limit

View

System view

Default level

2: System level

Parameters

limit-value: Specifies the maximum number of packets with the same source IP address but unresolvable destination IP addresses that the device can receive in 5 seconds. It ranges from 2 to 1024.

Description

Use **arp source-suppression limit** to set the maximum number of packets with the same source IP address but unresolvable destination IP addresses that the device can receive in 5 seconds.

Use **undo arp source-suppression limit** to restore the default value, which is 10.

With this feature configured, whenever the number of packets with unresolvable destination IP addresses from a host within 5 seconds exceeds the specified threshold, the device suppresses the sending host from triggering any ARP requests within the following 5 seconds.

Related commands: **display arp source-suppression**.

Examples

```
# Set the maximum number of packets with the same source address but unresolvable destination IP
addresses that the device can receive in 5 seconds to 100.
<Sysname> system-view
[Sysname] arp source-suppression limit 100
```

display arp source-suppression

Syntax

display arp source-suppression [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp source-suppression** to display information about the current ARP source suppression configuration.

Examples

Display information about the current ARP source suppression configuration.

```
<Sysname> display arp source-suppression
ARP source suppression is enabled
Current suppression limit: 100
Current cache length: 16
```

Table 55 Command output

Field	Description
ARP source suppression is enabled	The ARP source suppression function is enabled.
Current suppression limit	Maximum number of packets with the same source IP address but unresolvable destination IP addresses that the device can receive in 5 seconds.
Current cache length	Size of cache used to record source suppression information.

ARP packet rate limit configuration commands

arp rate-limit

Syntax

```
arp rate-limit { disable | rate pps drop }
undo arp rate-limit
```

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

disable: Disables ARP packet rate limit.

rate pps: Specifies the ARP packet rate in pps, in the range of 5 to 100.

drop: Discards the exceeded packets.

Description

Use **arp rate-limit** to configure or disable ARP packet rate limit on an interface.

Use **undo arp rate-limit** to restore the default.

By default, ARP packet rate limit is disabled.

Examples

Specify the ARP packet rate on layer 2 Ethernet port GigabitEthernet 1/0/1 as 50 pps, and exceeded packets will be discarded.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] arp rate-limit rate 50 drop
```

arp rate-limit information

Syntax

arp rate-limit information interval seconds

undo arp rate-limit information

View

System view

Default level

2: System level

Parameters

interval seconds: Specifies the interval for sending trap and log messages when ARP packet rate exceeds the threshold rate. The *seconds* argument ranges from 1 to 86400, in seconds.

Description

Use **arp rate-limit information** to set the interval for sending trap and log messages when ARP packet rate exceeds the threshold rate.

Use **undo arp rate-limit information** to restore the default.

By default, the interval is 60 seconds.

This command must work in cooperation with the **arp rate-limit** command.

Examples

Configure the device to send trap and log messages every 120 seconds when ARP packet rate exceeds the threshold rate.

```
<Sysname> system-view
```

```
[Sysname] arp rate-limit information interval 120
```

Source MAC address based ARP attack detection configuration commands

arp anti-attack source-mac

Syntax

```
arp anti-attack source-mac { filter | monitor }  
undo arp anti-attack source-mac [ filter | monitor ]
```

View

System view

Default level

2: System level

Parameters

filter: Generates log messages and discards subsequent ARP packets from the MAC address.

monitor: Only generates log message.

Description

Use **arp anti-attack source-mac** to enable the source MAC address based ARP attack detection and specify a handling method.

Use **undo arp anti-attack source-mac** to restore the default.

By default, source MAC address based ARP attack detection is disabled.

This function enables the router to check the source MAC address of ARP packets received from the same MAC address within 5 seconds against a specific threshold. If the threshold is exceeded, the router takes the preconfigured method to handle the attack.

If neither the **filter** nor the **monitor** keyword is specified in the **undo arp anti-attack source-mac** command, both handling methods are disabled.

Examples

```
# Enable the source MAC address based ARP attack detection and specify the filter handling method.  
<Sysname> system-view  
[Sysname] arp anti-attack source-mac filter
```

arp anti-attack source-mac aging-time

Syntax

```
arp anti-attack source-mac aging-time time  
undo arp anti-attack source-mac aging-time
```

View

System view

Default level

2: System level

Parameters

time: Specifies the age time for ARP attack entries, in the range of 60 to 6000 seconds.

Description

Use **arp anti-attack source-mac aging-time** to configure the age time for source MAC addresses based ARP attack detection entries.

Use **undo arp anti-attack source-mac aging-time** to restore the default.

By default, the age time for ARP attack entries is 300 seconds (5 minutes).

Examples

```
# Set the age time for ARP attack entries as 60 seconds.
<Sysname> system-view
[Sysname] arp anti-attack source-mac aging-time 60
```

arp anti-attack source-mac exclude-mac

Syntax

```
arp anti-attack source-mac exclude-mac mac-address&<1-10>
undo arp anti-attack source-mac exclude-mac [ mac-address&<1-10> ]
```

View

System view

Default level

2: System level

Parameters

mac-address&<1-10>: Specifies a MAC address list. The *mac-address* argument indicates an excluded MAC address in the format H-H-H. &<1-10> indicates the number of MAC addresses that you can exclude.

Description

Use **arp anti-attack source-mac exclude-mac** to exclude specific MAC addresses from source MAC address based ARP attack detection.

Use **undo arp anti-attack source-mac exclude-mac** to remove the specified MAC addresses.

By default, no MAC address is excluded from source MAC address based ARP attack detection.

If no MAC address is specified in the **undo arp anti-attack source-mac exclude-mac** command, all configured protected MAC addresses are removed.

Examples

```
# Exclude a MAC address from source MAC based ARP attack detection.
<Sysname> system-view
[Sysname] arp anti-attack source-mac exclude-mac 2-2-2
```

arp anti-attack source-mac threshold

Syntax

```
arp anti-attack source-mac threshold threshold-value
```

undo arp anti-attack source-mac threshold

View

System view

Default level

2: System level

Parameters

threshold-value: Specifies the threshold for source MAC address based ARP attack detection, in the range of 10 to 100.

Description

Use **arp anti-attack source-mac threshold** to configure the threshold for source MAC address based ARP attack detection. If the number of ARP packets from a MAC address within 5 seconds exceeds this threshold, the device considers this an attack.

Use **undo arp anti-attack source-mac threshold** to restore the default.

By default, the threshold for source MAC address based ARP attack detection is 50.

Examples

Configure the threshold for source MAC address based ARP attack detection as 30.

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac threshold 30
```

display arp anti-attack source-mac

Syntax

```
display arp anti-attack source-mac { slot slot-number | interface interface-type interface-number } [ |
{ begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays ARP attack entries detected on the interface.

slot *slot-number*: Displays ARP attack entries detected on a specific IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the switch.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp anti-attack source-mac** to display ARP attack entries detected by source MAC address based ARP attack detection.

If no interface is specified, the **display arp anti-attack source-mac** command displays ARP attack entries detected on all interfaces.

Examples

Display ARP attack entries detected by source MAC address based ARP attack detection. Display ARP attack entries detected by source MAC address based ARP attack detection.

```
<Sysname> display arp anti-attack source-mac slot 1
```

Source-MAC	VLAN ID	Interface	Aging-time
23f3-1122-3344	4094	GE1/0/1	10
23f3-1122-3355	4094	GE1/0/2	30
23f3-1122-33ff	4094	GE1/0/3	25
23f3-1122-33ad	4094	GE1/0/4	30
23f3-1122-33ce	4094	GE1/0/5	2

ARP packet source mac address consistency check configuration commands

arp anti-attack valid-check enable

Syntax

arp anti-attack valid-check enable

undo arp anti-attack valid-check enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **arp anti-attack valid-check enable** to enable ARP packet source MAC address consistency check on the gateway. After you execute this command, the gateway device can filter out ARP packets with the source MAC address in the Ethernet header different from the sender MAC address in the ARP message.

Use **undo arp anti-attack valid-check enable** to restore the default.

By default, ARP packet source MAC address consistency check is disabled.

Examples

Enable ARP packet source MAC address consistency check.

```
<Sysname> system-view
```

```
[Sysname] arp anti-attack valid-check enable
```

ARP active acknowledgement configuration commands

arp anti-attack active-ack enable

Syntax

```
arp anti-attack active-ack enable  
undo arp anti-attack active-ack enable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **arp anti-attack active-ack enable** to enable the ARP active acknowledgement function.

Use **undo arp anti-attack active-ack enable** to restore the default.

By default, the ARP active acknowledgement function is disabled.

This feature is configured on gateway devices to identify invalid ARP packets.

Examples

```
# Enable the ARP active acknowledgement function.  
<Sysname> system-view  
[Sysname] arp anti-attack active-ack enable
```

ARP detection configuration commands

arp detection

Syntax

```
arp detection id-number { permit | deny } ip { any | ip-address [ ip-address-mask ] } mac { any | mac-address [ mac-address-mask ] } [ vlan vlan-id ]  
undo arp detection id-number
```

Views

System view

Default level

2: System level

Parameters

id-number: Specifies the ID of the rule, in the range of 0 to 511. A lower value refers to a higher priority.

deny: Denies ARP packets matching the rule.

permit: Permit ARP packets matching the rule.

ip { any | ip-address [ip-address-mask] }: Specifies an IP address range for matching sender IP addresses of ARP packets.

- **any:** Matches any sender IP address.
- **ip-address:** Matches the specified sender IP address.
- **ip-address-mask:** Specifies a mask for the IP address, in dotted-decimal format. The *ip-address* argument without a mask indicates a host address.

mac { any | mac-address [mac-address-mask] }: Specifies a MAC address range for matching sender MAC addresses of ARP packets.

- **any:** Matches any sender MAC address.
- **mac-address:** Matches the specified sender MAC address, in the format of H-H-H.
- **mac-address-mask:** Specifies a mask for the MAC address, in the format of H-H-H.

vlan vlan-id: Specifies the VLAN where the rule applies. The *vlan-id* argument is in the range of 1 to 4094.

Description

Use **arp detection** to set a rule for user validity check.

Use **undo arp detection** to restore the default.

By default, no rule is set for user validity check.

User validity check inspects each ARP packet received on an ARP untrusted interface against the configured rules. If a match is found, the ARP packet is processed according to the matching rule. If no match is found, the device checks the packet against static IP Source Guard binding entries, the DHCP snooping entries, 802.1X security entries, and OUI MAC addresses in turn.

Related command: **arp detection enable**.

Examples

Set a rule for user validity check and enable user validity check.

```
<Sysname> system-view
[Sysname] arp detection 0 permit ip 3.1.1.1 255.255.0.0 mac 0001-0203-0607 ffff-ffff-0000
[Sysname] vlan 1
[Sysname-Vlan1] arp detection enable
```

arp detection enable

Syntax

arp detection enable

undo arp detection enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **arp detection enable** to enable ARP detection for the VLAN.

Use **undo arp detection enable** to restore the default.

By default, ARP detection is disabled for a VLAN.

Examples

```
# Enable ARP detection for VLAN 1.
<Sysname> system-view
[Sysname] vlan 1
[Sysname-Vlan1] arp detection enable
```

arp detection trust

Syntax

arp detection trust

undo arp detection trust

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **arp detection trust** to configure the port as an ARP trusted port.

Use **undo arp detection trust** to restore the default.

By default, the port is an ARP untrusted port.

Examples

```
# Configure layer 2 Ethernet port GigabitEthernet 1/0/1 as an ARP trusted port.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp detection trust
```

arp detection validate

Syntax

arp detection validate { dst-mac | ip | src-mac } *

undo arp detection validate [dst-mac | ip | src-mac] *

View

System view

Default level

2: System level

Parameters

dst-mac: Checks the target MAC address of ARP responses. If the target MAC address is all-zero, all-one, or inconsistent with the destination MAC address in the Ethernet header, the packet is considered invalid and discarded.

ip: Checks the source and destination IP addresses of ARP packets. The all-zero, all-one or multicast IP addresses are considered invalid and the corresponding packets are discarded. With this keyword specified, the source and destination IP addresses of ARP replies, and the source IP address of ARP requests will be checked.

src-mac: Checks whether the sender MAC address of an ARP packet is identical to the source MAC address in the Ethernet header. If they are identical, the packet is considered valid. Otherwise, the packet is discarded.

Description

Use **arp detection validate** to configure ARP detection based on specified objects. You can specify one or more objects in one command line.

Use **undo arp detection validate** to remove detected objects. If no keyword is specified, all detected objects are removed.

By default, ARP detection based on specified objects is disabled.

Examples

```
# Enable the checking of the MAC addresses and IP addresses of ARP packets.  
<Sysname> system-view  
[Sysname] arp detection validate dst-mac src-mac ip
```

arp restricted-forwarding enable

Syntax

arp restricted-forwarding enable

undo arp restricted-forwarding enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **arp restricted-forwarding enable** to enable ARP restricted forwarding.

Use **undo arp restricted-forwarding enable** to disable ARP restricted forwarding.

By default, ARP restricted forwarding is disabled.

Examples

```
# Enable ARP restricted forwarding in VLAN 1.
```

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] arp restricted-forwarding enable
```

display arp detection

Syntax

```
display arp detection [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp detection** to display the VLAN(s) enabled with ARP detection.

Related commands: **arp detection enable**.

Examples

Display the VLANs enabled with ARP detection.

```
<Sysname> display arp detection
ARP detection is enabled in the following VLANs:
1, 2, 4-5
```

Table 56 Command output

Field	Description
ARP detection is enabled in the following VLANs	VLANs that are enabled with ARP detection

display arp detection statistics

Syntax

```
display arp detection statistics [ interface interface-type interface-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the ARP detection statistics of a specific interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp detection statistics** to display statistics about ARP detection. This command only displays numbers of discarded packets. If no interface is specified, the statistics of all interfaces will be displayed.

Examples

Display the ARP detection statistics of all interfaces.

```
<Sysname> display arp detection statistics
```

```
State: U-Untrusted T-Trusted
```

```
ARP packets dropped by ARP inspect checking:
```

Interface(State)	IP	Src-MAC	Dst-MAC	Inspect
GE1/0/1(U)	40	0	0	78
GE1/0/2(U)	0	0	0	0
GE1/0/3(T)	0	0	0	0
GE1/0/4(U)	0	0	30	0

Table 57 Command output

Field	Description
Interface(State)	State T or U identifies a trusted or untrusted port.
IP	Number of ARP packets discarded due to invalid source and destination IP addresses.
Src-MAC	Number of ARP packets discarded due to invalid source MAC address.
Dst-MAC	Number of ARP packets discarded due to invalid destination MAC address.
Inspect	Number of ARP packets that failed to pass ARP detection (based on static IP Source Guard binding entries/DHCP snooping entries/802.1X security entries/OUI MAC addresses).

reset arp detection statistics

Syntax

reset arp detection statistics [**interface** *interface-type interface-number*]

View

User view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Clears the ARP detection statistics of a specific interface.

Description

Use **reset arp detection statistics** to clear ARP detection statistics of a specific interface. If no interface is specified, the statistics of all interfaces will be cleared.

Examples

```
# Clear the ARP detection statistics of all interfaces.
<Sysname> reset arp detection statistics
```

ARP automatic scanning and fixed ARP configuration commands

arp fixup

Syntax

arp fixup

View

System view

Default level

2: System level

Parameters

None

Description

Use **arp fixup** to change the existing dynamic ARP entries into static ARP entries. You can use this command again to change the dynamic ARP entries learned later into static ARP entries.

The static ARP entries changed from dynamic ARP entries have the same attributes as the manually configured static ARP entries.

The number of static ARP entries changed from dynamic ARP entries is restricted by the number of static ARP entries that the device supports. As a result, the device may fail to change all dynamic ARP entries into static ARP entries.

Suppose that the number of dynamic ARP entries is D and that of the existing static ARP entries is S . When the dynamic ARP entries are changed into static, new dynamic ARP entries may be created (suppose the number is M) and some of the dynamic ARP entries may be aged out (suppose the number is N). After the process is complete, the number of static ARP entries is $D + S + M - N$.

To delete a specific static ARP entry changed from a dynamic one, use the **undo arp ip-address** command. To delete all such static ARP entries, use the **reset arp all** or **reset arp static** command.

Examples

```
# Enable fixed ARP.
<Sysname> system-view
[Sysname] arp fixup
```

arp scan

Syntax

arp scan [*start-ip-address to end-ip-address*]

View

VLAN interface view

Default level

2: System level

Parameters

start-ip-address: Specifies the start IP address of the scanning range.

end-ip-address: Specifies the end IP address of the scanning range. The end IP address must be higher than or equal to the start IP address.

Description

Use **arp scan** to enable ARP automatic scanning in the specified address range for neighbors.

If the start IP and end IP addresses are specified, the device scans the specific address range for neighbors and learns their ARP entries, so that the scanning time is reduced. If the specified address range contains multiple network segments, the sender IP address in the ARP request is the interface address on the smallest network segment.

If no address range is specified, the device only scans the network where the primary IP address of the interface resides for neighbors. The sender IP address in the ARP requests is the primary IP address of the interface.

The start IP address and end IP address must be on the same network as the primary IP address or manually configured secondary IP addresses of the interface.

IP addresses that already exist in ARP entries are not scanned.

ARP automatic scanning may take some time. To stop an ongoing scan, press **Ctrl + C**. Dynamic ARP entries are created based on ARP replies received before the scan is terminated.

Examples

Configure the device to scan the network where the primary IP address of VLAN-interface 2 resides for neighbors.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan
```

Configure the device to scan a specific address range for neighbors.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan 1.1.1.1 to 1.1.1.20
```

ARP gateway protection configuration commands

arp filter source

Syntax

arp filter source *ip-address*

undo arp filter source *ip-address*

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

ip-address: Specifies the IP address of a protected gateway.

Description

Use **arp filter source** to enable ARP gateway protection for a specific gateway.

Use **undo arp filter source** to disable ARP gateway protection for a specific gateway.

By default, ARP gateway protection is disabled.

You can enable ARP gateway protection for up to eight gateways on a port.

You cannot configure both the **arp filter source** and **arp filter binding** commands on a port.

Examples

Enable ARP gateway protection for the gateway with IP address 1.1.1.1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] arp filter source 1.1.1.1
```

ARP filtering configuration commands

arp filter binding

Syntax

arp filter binding *ip-address mac-address*

undo arp filter binding *ip-address*

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

ip-address: Specifies the permitted sender IP address.

mac-address: Specifies the permitted sender MAC address.

Description

Use **arp filter binding** to configure an ARP filtering entry. If the sender IP and MAC addresses of an ARP packet match an ARP filtering entry, the ARP packet is permitted. If not, it is discarded.

Use **undo arp filter binding** to remove an ARP filtering entry.

By default, no ARP filtering entry is configured.

You can configure up to eight ARP filtering entries on a port.

You cannot configure both the **arp filter source** and **arp filter binding** commands on a port.

Examples

Configure an ARP filtering entry with permitted sender IP address 1.1.1.1 and MAC address 2-2-2.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] arp filter binding 1.1.1.1 2-2-2
```

ND attack defense configuration commands

Source MAC consistency check commands

ipv6 nd mac-check enable

Syntax

```
ipv6 nd mac-check enable
undo ipv6 nd mac-check enable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **ipv6 nd mac-check enable** to enable source MAC consistency check for ND packets.

Use **undo ipv6 nd mac-check enable** to disable source MAC consistency check for ND packets.

By default, source MAC consistency check is disabled for ND packets.

In a typical forged ND packet, the Ethernet frame header conveys a source MAC address different than the source link layer address option. To filter out these invalid ND packets, use the source MAC consistency check function to check ND packets for MAC address inconsistency.

Examples

```
# Enable source MAC consistency check for ND packets.
<Sysname> system-view
[Sysname] ipv6 nd mac-check enable
```

ND detection configuration commands

display ipv6 nd detection

Syntax

```
display ipv6 nd detection [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 nd detection** to display ND detection configuration.

Related commands: **ipv6 nd detection enable** and **ipv6 nd detection trust**.

Examples

Display ND detection configuration.

```
<Sysname> display ipv6 nd detection
```

ND detection is enabled on the following VLANs:

```
1, 2, 4-5
```

ND detection trust is configured on the following interfaces:

```
GigabitEthernet1/0/1
```

```
GigabitEthernet1/0/2
```

Table 58 Command output

Field	Description
ND detection is enabled on the following VLANs	List of VLANs enabled with ND detection.
ND detection trust is configured on the following interfaces	List of ND-trusted ports. On an ND-trusted port, ND packets are not checked. By default, all ports are ND-untrusted ports on which ND packets in an ND detection-enabled VLAN will be checked.

display ipv6 nd detection statistics

Syntax

```
display ipv6 nd detection statistics [ interface interface-type interface-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays ND detection statistics for the interface identified by *interface-type interface-number*. The *interface-type interface-number* arguments represent the interface type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 nd detection statistics** to display ND detection statistics. The statistics count only ND packets discarded for validity check failure.

If an interface is specified, the command displays only the statistic for the interface. If no interface is specified, the command displays statistics for all interfaces.

Examples

Display the statistics for discarded ND packets on all interfaces.

```
<Sysname> display ipv6 nd detection statistics
```

ND packets dropped by ND detection:

Interface	Packets Dropped
GE1/0/1	78
GE1/0/2	0
GE1/0/3	0
GE1/0/4	0

ipv6 nd detection enable

Syntax

ipv6 nd detection enable

undo ipv6 nd detection enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use **ipv6 nd detection enable** to enable ND detection in a VLAN to check ND packets for source spoofing.

Use **undo ipv6 nd detection enable** to disable ND detection.

By default, ND detection is disabled.

Examples

Enable ND detection in VLAN 10.

```
<Sysname> system-view
```

```
[Sysname] vlan 10
```

```
[Sysname-vlan 10] ipv6 nd detection enable
```

ipv6 nd detection trust

Syntax

```
ipv6 nd detection trust
undo ipv6 nd detection trust
```

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **ipv6 nd detection trust** to configure a port as an ND-trusted port.

Use **undo ipv6 nd detection trust** to configure a port as an ND-untrusted port.

By default, a port is ND-untrusted. In an ND detection-enabled VLAN, ports are assigned two roles: ND-trusted and ND-untrusted.

On an ND-trusted port, the ND detection function does not check ND packets for address spoofing.

On an ND-untrusted port, RA and RR messages are considered illegal and discarded directly. All other ND packets in the VLAN are checked for source spoofing.

Examples

```
# Configure Layer 2 port GigabitEthernet1/0/1 as an ND-trusted port.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 nd detection trust
```

```
# Configure interface Bridge-Aggregation 1 as an ND-trusted port.
```

```
<Sysname> system-view
```

```
[Sysname] interface bridge-Aggregation 1
```

```
[Sysname-Bridge-Aggregation1] ipv6 nd detection trust
```

reset ipv6 nd detection statistics

Syntax

```
reset ipv6 nd detection statistics [ interface interface-type interface-number ]
```

View

User view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Clears the statistics of the interface identified by *interface-type interface-number*. The *interface-type interface-number* arguments represent the interface type and number.

Description

Use **reset ipv6 nd detection statistics** to clear the ND detection statistics of an interface. If no interface is specified, the ND detection statistics of all interfaces are cleared.

Examples

```
# Clear the ND detection statistics of all interfaces.  
<Sysname> reset ipv6 nd detection statistics
```

SAVI configuration commands

ipv6 savi dad-delay

Syntax

```
ipv6 savi dad-delay value  
undo ipv6 savi dad-delay
```

View

System view

Default level

2: System level

Parameters

value: Specifies the time in centiseconds to wait for a duplicate address detection (DAD) NA, ranging from 0 to 2147483647.

Description

Use **ipv6 savi dad-delay** to set the time to wait for a DAD NA.

Use **undo ipv6 savi dad-delay** to restore the default.

By default, the time to wait for a DAD NA is 100 centiseconds (1 second).

Examples

```
# Set the time to wait for a DAD NA to 100 seconds.  
<Sysname> system-view  
[Sysname] ipv6 savi dad-delay 10000
```

ipv6 savi dad-preparedelay

Syntax

```
ipv6 savi dad-preparedelay value  
undo ipv6 savi dad-preparedelay
```

View

System view

Default level

2: System level

Parameters

value: Specifies the time in centiseconds to wait for a DAD NS from a DHCPv6 client after the DHCPv6 client obtains an IP address. This argument ranges from 0 to 2147483647.

Description

Use **ipv6 savi dad-preparedelay** to set the time to wait for a DAD NS from a DHCPv6 client.

Use **undo ipv6 savi dad-preparedelay** to restore the default.

By default, the time to wait for a DAD NS from a DHCPv6 client is 100 centiseconds (1 second).

This command is used with the DHCPv6 snooping function. After DHCPv6 snooping detects that a client obtains an IPv6 address, it monitors whether the client detects IP address conflict. If DHCPv6 snooping does not receive any DAD NS from the client before the set time expires, SAVI sends a DAD NS on behalf of the client.

Examples

```
# Set the time to wait for a DAD NS from a DHCPv6 client to 100 seconds.
```

```
<Sysname> system-view
```

```
[Sysname] ipv6 savi dad-preparedelay 10000
```

ipv6 savi down-delay

Syntax

ipv6 savi down-delay *time*

undo ipv6 savi down-delay

View

System view

Default level

2: System level

Parameters

time: Specifies the delay time in the range of 0 to 86400 seconds.

Description

Use **ipv6 savi down-delay** to set the deletion delay time for SAVI.

Use **undo ipv6 savi down-delay** to restore the default.

By default, the deletion delay time is 30 seconds.

If a port is down for a period of time that exceeds the deletion delay time, the switch deletes the DHCPv6 snooping entries and ND snooping entries for that port.

Examples

```
# Set the deletion delay time for SAVI to 360 seconds.
```

```
<Sysname> system-view
```

```
[Sysname] ipv6 savi down-delay 360
```

ipv6 savi strict

Syntax

ipv6 savi strict

undo ipv6 savi strict

View

System view

Default level

2: System level

Parameters

None

Description

Use **ipv6 savi strict** to enable the SAVI function.

Use **undo ipv6 savi strict** to disable the SAVI function.

By default, the SAVI function is disabled.

Examples

Enable the SAVI function.

```
<Sysname> system-view
```

```
[Sysname] ipv6 savi strict
```

Blacklist configuration commands

blacklist enable

Syntax

blacklist enable
undo blacklist enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **blacklist enable** to enable the blacklist feature. With the blacklist feature enabled, the switch filters all packets from IP addresses on the blacklist.

Use **undo blacklist enable** to restore the default.

By default, the blacklist feature is disabled.

After you enable the blacklist feature, you can manually add blacklist entries, or have the switch cooperate with the login user authentication feature to add blacklist entries automatically.

Examples

```
# Enable the blacklist feature.  
<Sysname> system-view  
[Sysname] blacklist enable
```

blacklist ip

Syntax

blacklist ip *source-ip-address* [**timeout** *minutes*]
undo blacklist { **all** | **ip** *source-ip-address* [**timeout**] }

View

System view

Default level

2: System level

Parameters

source-ip-address: IP address to be added to the blacklist. It cannot be the broadcast address, 127.0.0.0/8, a class D address, or a class E address.

all: Specifies all blacklist entries.

timeout *minutes*: Specifies the aging time for the entry in minutes, in the range of 1 to 1000. If you do not specify this option, the entry does not age and is always effective, unless you manually remove it.

Description

Use **blacklist ip** to add a blacklist entry. Then, the blacklist feature filters all packets from the IP address before the entry is aged out or manually removed.

Use **undo blacklist** to remove all blacklist entries in one operation, remove a single blacklist entry, or cancel the aging time setting of a blacklist entry.

The **undo blacklist ip source-ip-address timeout** command does not remove the entry. It only cancels the aging time setting of the entry, making the entry never aging out.

Blacklist entries are effective only when the blacklist feature is enabled.

You can change the aging time of an existing blacklist entry, and your change takes effect immediately.

Related commands: **blacklist enable** and **display blacklist**.

Examples

Add the IP address 192.168.1.2 to the blacklist, and set the aging time to 20 minutes.

```
<Sysname> system-view
[Sysname] blacklist ip 192.168.1.2 timeout 20
```

display blacklist

Syntax

display blacklist { **all** | **ip** *source-ip-address* [**slot** *slot-number*] | **slot** *slot-number* } [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ip *source-ip-address*: Displays information about the blacklist entry for an IP address. The *source-ip-address* argument cannot be the broadcast address, 127.0.0.0/8, a class D address, or a class E address.

all: Displays information about all blacklist entries.

slot *slot-number*: Displays information about the blacklist entries on an IRF member device. The *slot-number* argument represents the ID of the IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Description

Use **display blacklist** to display blacklist information.

Related commands: **blacklist enable** and **blacklist ip**.

Examples

Display information about all blacklist entries.

```
<Sysname> display blacklist all
                        Blacklist information
-----
Blacklist                : enabled
Blacklist items          : 3
-----

IP            Type    Aging started      Aging finished      Dropped packets
              YYYY/MM/DD hh:mm:ss  YYYY/MM/DD hh:mm:ss
2.2.1.1.2     manual  2011/05/27 19:15:39  Never                0
1.1.1.1.2     auto    2011/05/01 18:26:31  2011/05/01 18:36:31  4294967295
1.1.1.1.3     manual  2011/05/02 06:13:20  2011/05/02 07:54:47  4294967295
-----
```

Table 59 Command output

Field	Description
Blacklist	Whether the blacklist feature is enabled.
Blacklist items	Number of blacklist entries.
IP	IP address of the blacklist entry.
Type	Type of the blacklist entry: <ul style="list-style-type: none">• manual—The entry was manually added.• auto—The entry was automatically added.
Aging started	Installation time of the entry.
Aging finished	Expiration time of the entry. For an entry with no aging time setting, the value Never is displayed.
Dropped packets	Number of packets from the IP address that have been dropped.

FIPS configuration commands

display fips status

Syntax

display fips status

View

Any view

Default level

1: Monitor level

Parameters

None

Description

Use the **display fips status** command to display the current FIPS mode.

Related commands: **fips mode enable**.

Examples

```
# Display the current FIPS mode.  
<Sysname> display fips status  
FIPS mode is enabled
```

fips mode enable

Syntax

fips mode enable

undo fips mode enable

View

System view

Default level

2: System level

Parameters

None

Description

Use the **fips mode enable** command to enable the FIPS mode.

Use the **undo fips mode enable** command to disable the FIPS mode.

By default, the FIPS mode is disabled.

After you enable the FIPS mode, reboot the switch to make your configuration effective. After the switch starts up, the switch works in FIPS mode. The FIPS mode complies with the FIPS 140-2 standard.

Related commands: **display fips status**.

Examples

```
# Enable the FIPS mode.
<Sysname> system-view
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue?[Y/N]:y
Change the configuration to meet FIPS mode requirements, save the configuration to the
next-startup configuration file, and then reboot to enter FIPS mode.
```

fips self-test

Syntax

fips self-test

Views

System view

Default level

3: Manage level

Parameters

None

Description

Use **fips self-test** to trigger a self-test on the password algorithms.

To examine whether the cryptography modules operate normally, you can use a command to trigger a self-test on the cryptographic algorithms. The triggered self-test is the same as the power-up self-test.

If the self-test fails, the device automatically reboots.

Examples

```
# Trigger a self-test on the cryptographic algorithms.
<Sysname> system-view
[Sysname] fips self-test
Self-tests are running. Please wait...
Self-tests succeeded.
```

Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

<http://www.hp.com/support>

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

<http://www.hp.com/go/wwalerts>

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

<http://www.hp.com/support/manuals>

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

Websites

- HP.com <http://www.hp.com>
- HP Networking <http://www.hp.com/go/networking>
- HP manuals <http://www.hp.com/support/manuals>
- HP download drivers and software <http://www.hp.com/support/downloads>
- HP software depot <http://www.software.hp.com>
- HP Education <http://www.hp.com/learn>

Conventions

This section describes the conventions used in this documentation set.





Command conventions

Convention	Description
Boldface	Bold text represents commands and keywords that you enter literally as shown.
<i>Italic</i>	<i>Italic</i> text represents arguments that you replace with actual values.
[]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x y ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x y ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x y ... } *	Asterisk-marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x y ...] *	Asterisk-marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.








GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in bold text. For example, the New User window appears; click OK .
>	Multi-level menus are separated by angle brackets. For example, File > Create > Folder .

Symbols

Convention	Description
 WARNING	An alert that calls attention to important information that if not understood or followed can result in personal injury.
 CAUTION	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
 IMPORTANT	An alert that calls attention to essential information.
NOTE	An alert that contains additional or supplementary information.
 TIP	An alert that provides helpful information.

Network topology icons

	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the switching engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a security product, such as a firewall, a UTM, or a load-balancing or security card that is installed in a device.
	Represents a security card, such as a firewall card, a load-balancing card, or a NetStream card.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#)

A

aaa nas-id profile, [1](#)
access-limit, [26](#)
access-limit enable, [1](#)
accounting command, [2](#)
accounting default, [3](#)
accounting lan-access, [4](#)
accounting login, [4](#)
accounting optional, [5](#)
accounting portal, [6](#)
accounting-on enable, [39](#)
ah authentication-algorithm, [230](#)
arp anti-attack active-ack enable, [355](#)
arp anti-attack source-mac, [351](#)
arp anti-attack source-mac aging-time, [351](#)
arp anti-attack source-mac exclude-mac, [352](#)
arp anti-attack source-mac threshold, [352](#)
arp anti-attack valid-check enable, [354](#)
arp detection, [355](#)
arp detection enable, [356](#)
arp detection trust, [357](#)
arp detection validate, [357](#)
arp filter binding, [363](#)
arp filter source, [363](#)
arp fixup, [361](#)
arp rate-limit, [349](#)
arp rate-limit information, [350](#)
arp resolving-route enable, [347](#)
arp restricted-forwarding enable, [358](#)
arp scan, [362](#)
arp source-suppression enable, [347](#)
arp source-suppression limit, [348](#)
attribute, [205](#)
attribute 25 car, [40](#)
authentication default, [7](#)
authentication lan-access, [8](#)
authentication login, [8](#)
authentication portal, [9](#)

authentication super, [10](#)
authentication-algorithm, [262](#)
authentication-method, [262](#)
authorization command, [11](#)
authorization default, [12](#)
authorization lan-access, [13](#)
authorization login, [13](#)
authorization portal, [14](#)
authorization-attribute (local user view/user group view), [26](#)
authorization-attribute (RADIUS-server user view), [89](#)
authorization-attribute user-profile, [15](#)

B

bind-attribute, [28](#)
blacklist enable, [373](#)
blacklist ip, [373](#)
bye, [306](#)

C

ca identifier, [206](#)
cd, [307](#)
cdup, [307](#)
certificate domain, [263](#)
certificate request entity, [206](#)
certificate request from, [207](#)
certificate request mode, [207](#)
certificate request polling, [208](#)
certificate request url, [209](#)
ciphersuite, [323](#)
client-verify enable, [324](#)
client-verify weaken, [325](#)
close-mode wait, [325](#)
common-name, [210](#)
connection-name, [230](#)
country, [210](#)
crl check, [211](#)
crl update-period, [211](#)
crl url, [212](#)

cut connection, [16](#)

D

data-flow-format (HWTACACS scheme view), [71](#)

data-flow-format (RADIUS scheme view), [40](#)

delete, [308](#)

description, [89](#)

dh, [263](#)

dir, [308](#)

display arp anti-attack source-mac, [353](#)

display arp detection, [359](#)

display arp detection statistics, [359](#)

display arp source-suppression, [348](#)

display blacklist, [374](#)

display connection, [17](#)

display domain, [20](#)

display dot1x, [94](#)

display fips status, [376](#)

display habp, [188](#)

display habp table, [189](#)

display habp traffic, [189](#)

display hwtacacs, [72](#)

display ike dpd, [264](#)

display ike peer, [265](#)

display ike proposal, [266](#)

display ike sa, [267](#)

display ip source binding, [337](#)

display ipsec policy, [231](#)

display ipsec proposal, [234](#)

display ipsec sa, [235](#)

display ipsec session, [238](#)

display ipsec statistics, [239](#)

display ipsec tunnel, [241](#)

display ipv6 nd detection, [365](#)

display ipv6 nd detection statistics, [366](#)

display ipv6 source binding, [338](#)

display local-user, [29](#)

display mac-authentication, [122](#)

display password-control, [170](#)

display password-control blacklist, [171](#)

display pki certificate, [212](#)

display pki certificate access-control-policy, [214](#)

display pki certificate attribute-group, [215](#)

display pki crl domain, [216](#)

display portal free-rule, [132](#)

display portal interface, [133](#)

display portal local-server, [134](#)

display portal tcp-cheat statistics, [135](#)

display portal user, [136](#)

display port-security, [148](#)

display port-security mac-address block, [151](#)

display port-security mac-address security, [152](#)

display public-key local public, [194](#)

display public-key peer, [196](#)

display radius scheme, [41](#)

display radius statistics, [44](#)

display sftp client source, [309](#)

display ssh client source, [295](#)

display ssh server, [287](#)

display ssh server-info, [296](#)

display ssh user-information, [288](#)

display ssl client-policy, [326](#)

display ssl server-policy, [327](#)

display stop-accounting-buffer (for HWTACACS), [75](#)

display stop-accounting-buffer (for RADIUS), [47](#)

display tcp status, [335](#)

display user-group, [31](#)

display user-profile, [167](#)

domain, [22](#)

domain default enable, [22](#)

dot1x, [97](#)

dot1x attempts max-fail, [99](#)

dot1x authentication-method, [99](#)

dot1x auth-fail vlan, [101](#)

dot1x critical recovery-action, [103](#)

dot1x critical vlan, [101](#)

dot1x domain-delimiter, [103](#)

dot1x eapol untag, [104](#)

dot1x free-ip, [119](#)

dot1x guest-vlan, [105](#)

dot1x handshake, [106](#)

dot1x handshake secure, [107](#)

dot1x mandatory-domain, [107](#)

dot1x max-user, [108](#)

dot1x multicast-trigger, [110](#)

dot1x port-control, [110](#)

dot1x port-method, [111](#)

dot1x quiet-period, [112](#)

dot1x re-authenticate, [113](#)

dot1x retry, [114](#)

dot1x timer, 115
dot1x timer ead-timeout, 119
dot1x unicast-trigger, 116
dot1x url, 120
dpd, 270

E

encapsulation-mode, 242
encryption-algorithm, 271
esp authentication-algorithm, 243
esp encryption-algorithm, 243
exchange-mode, 272
exit, 310
expiration-date (local user view), 32
expiration-date (RADIUS-server user view), 90

F

fips mode enable, 376
fips self-test, 377
fqdn, 217

G

get, 310
group, 33
group-attribute allow-guest, 33

H

habp client vlan, 190
habp enable, 191
habp server vlan, 191
habp timer, 192
handshake timeout, 328
help, 311
hwtacacs nas-ip, 75
hwtacacs scheme, 76

I

idle-cut enable, 23
id-type, 272
ike dpd, 273
ike local-name, 273
ike next-payload check disabled, 274
ike peer (system view), 275
ike proposal, 275
ike sa keepalive-timer interval, 276
ike sa keepalive-timer timeout, 276
ike sa nat-keepalive-timer interval, 277

ike-peer (IPsec policy view), 244
interval-time, 278
ip (PKI entity view), 218
ip source binding (interface view), 340
ip source binding (system view), 341
ip verify source, 342
ip verify source max-entries, 342
ipsec anti-replay check, 245
ipsec anti-replay window, 245
ipsec decrypt check, 246
ipsec policy (interface view), 246
ipsec policy (system view), 247
ipsec proposal, 248
ipsec sa global-duration, 249
ipsec session idle-time, 249
ipv6 nd detection enable, 367
ipv6 nd detection trust, 368
ipv6 nd mac-check enable, 365
ipv6 savi dad-delay, 370
ipv6 savi dad-preparedelay, 370
ipv6 savi down-delay, 371
ipv6 savi strict, 371
ipv6 source binding (interface view), 343
ipv6 source binding (system view), 344
ipv6 verify source, 345
ipv6 verify source max-entries, 346

K

key (HWTACACS scheme view), 77
key (RADIUS scheme view), 48

L

ldap-server, 219
local-address, 278
locality, 219
local-name, 279
local-user, 34
ls, 311

M

mac-authentication, 124
mac-authentication critical vlan, 125
mac-authentication domain, 126
mac-authentication guest-vlan, 127
mac-authentication max-user, 128
mac-authentication timer, 128

mac-authentication timer auth-delay, [129](#)
mac-authentication user-name-format, [130](#)
mkdir, [312](#)

N

nas-id bind vlan, [24](#)
nas-ip (HWTACACS scheme view), [78](#)
nas-ip (RADIUS scheme view), [49](#)
nat traversal, [280](#)

O

organization, [220](#)
organization-unit, [220](#)

P

password, [172](#)
password (local user view), [35](#)
password (RADIUS-server user view), [91](#)
password-control { aging | composition | history | length } enable, [173](#)
password-control aging, [174](#)
password-control alert-before-expire, [175](#)
password-control authentication-timeout, [176](#)
password-control complexity, [176](#)
password-control composition, [177](#)
password-control enable, [178](#)
password-control expired-user-login, [179](#)
password-control history, [179](#)
password-control length, [180](#)
password-control login idle-time, [181](#)
password-control login-attempt, [182](#)
password-control password update interval, [183](#)
password-control super aging, [184](#)
password-control super composition, [184](#)
password-control super length, [185](#)
peer, [280](#)
peer-public-key end, [197](#)
pfs, [250](#)
pki certificate access-control-policy, [221](#)
pki certificate attribute-group, [221](#)
pki delete-certificate, [222](#)
pki domain, [223](#)
pki entity, [223](#)
pki import-certificate, [224](#)
pki request-certificate domain, [224](#)
pki retrieval-certificate, [225](#)

pki retrieval-crl domain, [226](#)
pki validate-certificate, [226](#)
pki-domain, [329](#)
policy enable, [251](#)
portal auth-fail vlan, [137](#)
portal delete-user, [138](#)
portal domain, [139](#)
portal free-rule, [139](#)
portal local-server, [140](#)
portal local-server enable, [141](#)
portal local-server ip, [142](#)
portal max-user, [143](#)
portal move-mode auto, [143](#)
portal offline-detect interval, [144](#)
portal redirect-url, [145](#)
portal server banner, [145](#)
portal web-proxy port, [146](#)
port-security authorization ignore, [154](#)
port-security enable, [155](#)
port-security intrusion-mode, [155](#)
port-security mac-address aging-type inactivity, [156](#)
port-security mac-address dynamic, [157](#)
port-security mac-address security, [158](#)
port-security max-mac-count, [159](#)
port-security ntk-mode, [160](#)
port-security oui, [161](#)
port-security port-mode, [162](#)
port-security timer autolearn aging, [164](#)
port-security timer disableport, [164](#)
port-security trap, [165](#)
prefer-cipher, [330](#)
pre-shared-key, [281](#)
primary accounting (HWTACACS scheme view), [79](#)
primary accounting (RADIUS scheme view), [50](#)
primary authentication (HWTACACS scheme view), [79](#)
primary authentication (RADIUS scheme view), [51](#)
primary authorization, [80](#)
proposal (IKE peer view), [281](#)
proposal (IPsec policy view), [251](#)
public-key local create, [199](#)
public-key local destroy, [200](#)
public-key local export dsa, [201](#)
public-key local export rsa, [202](#)
public-key peer, [203](#)
public-key peer import sshkey, [204](#)

public-key-code begin, [198](#)
public-key-code end, [198](#)
put, [312](#)
pwd, [313](#)

Q

qos pre-classify, [252](#)
quit, [313](#)

R

radius client, [53](#)
radius dscp, [54](#)
radius ipv6 dscp, [54](#)
radius nas-ip, [55](#)
radius scheme, [55](#)
radius trap, [56](#)
radius-server client-ip, [91](#)
radius-server user, [92](#)
remote-address, [282](#)
remote-name, [283](#)
remove, [314](#)
rename, [314](#)
reset arp detection statistics, [360](#)
reset dot1x statistics, [117](#)
reset hwtacacs statistics, [81](#)
reset ike sa, [284](#)
reset ipsec sa, [253](#)
reset ipsec session, [254](#)
reset ipsec statistics, [254](#)
reset ipv6 nd detection statistics, [368](#)
reset mac-authentication statistics, [131](#)
reset password-control blacklist, [186](#)
reset password-control history-record, [186](#)
reset portal tcp-cheat statistics, [147](#)
reset radius statistics, [57](#)
reset stop-accounting-buffer (for HWTACACS), [82](#)
reset stop-accounting-buffer (for RADIUS), [57](#)
retry, [58](#)
retry realtime-accounting, [59](#)
retry stop-accounting (HWTACACS scheme view), [82](#)
retry stop-accounting (RADIUS scheme view), [60](#)
rmdir, [315](#)
root-certificate fingerprint, [227](#)
rule (PKI CERT ACP view), [228](#)

S

sa authentication-hex, [255](#)
sa duration, [285](#)
sa duration, [256](#)
sa encryption-hex, [257](#)
sa spi, [258](#)
scp, [321](#)
secondary accounting (HWTACACS scheme view), [83](#)
secondary accounting (RADIUS scheme view), [61](#)
secondary authentication (HWTACACS scheme view), [84](#)
secondary authentication (RADIUS scheme view), [62](#)
secondary authorization, [84](#)
security acl, [258](#)
security-policy-server, [64](#)
self-service-url enable, [24](#)
server-type, [64](#)
server-verify enable, [331](#)
service-type, [36](#)
session, [331](#)
sftp, [315](#)
sftp client dscp, [317](#)
sftp client ipv6 dscp, [317](#)
sftp client ipv6 source, [318](#)
sftp client source, [318](#)
sftp ipv6, [319](#)
sftp server enable, [305](#)
sftp server idle-timeout, [305](#)
ssh client authentication server, [297](#)
ssh client dscp, [298](#)
ssh client first-time, [298](#)
ssh client ipv6 dscp, [299](#)
ssh client ipv6 source, [300](#)
ssh client source, [300](#)
ssh server authentication-retries, [289](#)
ssh server authentication-timeout, [290](#)
ssh server compatible-ssh1x, [291](#)
ssh server dscp, [291](#)
ssh server enable, [292](#)
ssh server ipv6 dscp, [292](#)
ssh server rekey-interval, [293](#)
ssh user, [294](#)
ssh2, [301](#)
ssh2 ipv6, [302](#)
ssl client-policy, [332](#)
ssl server-policy, [333](#)

- state, [228](#)
- state (ISP domain view), [25](#)
- state (local user view), [37](#)
- state primary, [65](#)
- state secondary, [66](#)
- stop-accounting-buffer enable (HWTACACS scheme view), [85](#)
- stop-accounting-buffer enable (RADIUS scheme view), [67](#)

T

- tcp syn-cookie enable, [336](#)
- time-out, [285](#)
- timer quiet (HWTACACS scheme view), [86](#)
- timer quiet (RADIUS scheme view), [67](#)
- timer realtime-accounting (HWTACACS scheme view), [86](#)
- timer realtime-accounting (RADIUS scheme view), [68](#)
- timer response-timeout (HWTACACS scheme view), [87](#)
- timer response-timeout (RADIUS scheme view), [69](#)
- transform, [259](#)
- tunnel local, [260](#)
- tunnel remote, [261](#)

U

- user-group, [37](#)
- user-name-format (HWTACACS scheme view), [88](#)
- user-name-format (RADIUS scheme view), [70](#)
- user-profile, [168](#)
- user-profile enable, [168](#)

V

- validity-date, [38](#)
- version, [333](#)
- vlan-group, [117](#)
- vlan-list, [118](#)