Cisco IOS Security Command Reference: Commands D to L

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided “as is” with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice. In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.
## CONTENTS

### CHAPTER 1

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>database archive through dns</td>
<td>1</td>
</tr>
<tr>
<td>data</td>
<td>3</td>
</tr>
<tr>
<td>database archive</td>
<td>4</td>
</tr>
<tr>
<td>database level</td>
<td>7</td>
</tr>
<tr>
<td>database url</td>
<td>11</td>
</tr>
<tr>
<td>database username</td>
<td>16</td>
</tr>
<tr>
<td>deadtime (config-ldap-server)</td>
<td>19</td>
</tr>
<tr>
<td>deadtime (server-group configuration)</td>
<td>21</td>
</tr>
<tr>
<td>debug cts sxp filter events</td>
<td>23</td>
</tr>
<tr>
<td>def-domain</td>
<td>24</td>
</tr>
<tr>
<td>default (cs-server)</td>
<td>25</td>
</tr>
<tr>
<td>default (ca-trustpoint)</td>
<td>28</td>
</tr>
<tr>
<td>default (ca-trustpool)</td>
<td>29</td>
</tr>
<tr>
<td>default-group-policy</td>
<td>31</td>
</tr>
<tr>
<td>deny</td>
<td>32</td>
</tr>
<tr>
<td>deny (Catalyst 6500 series switches)</td>
<td>43</td>
</tr>
<tr>
<td>deny (IP)</td>
<td>54</td>
</tr>
<tr>
<td>deny (IPv6)</td>
<td>64</td>
</tr>
<tr>
<td>deny (MAC ACL)</td>
<td>72</td>
</tr>
<tr>
<td>deny (WebVPN)</td>
<td>75</td>
</tr>
<tr>
<td>description (dot1x credentials)</td>
<td>78</td>
</tr>
<tr>
<td>description (identify zone)</td>
<td>79</td>
</tr>
<tr>
<td>description (identity policy)</td>
<td>80</td>
</tr>
<tr>
<td>description (identity profile)</td>
<td>81</td>
</tr>
<tr>
<td>description (IKEv2 keyring)</td>
<td>82</td>
</tr>
<tr>
<td>description (isakmp peer)</td>
<td>83</td>
</tr>
</tbody>
</table>
CHAPTER 2  

dnsix-dmdp retries through dynamic  

dnsix-dmdp retries  

dnsix-nat authorized-redirection  

dnsix-nat primary  

dnsix-nat authorized-redirection
dnsix-nat secondary 132

dnsix-nat source 133

dnsix-nat transmit-count 134

dns-timeout 135

domain (AAA) 136

domain (isakmp-group) 138

domain-stripping 139

dot1x control-direction 141

dot1x credentials 144

dot1x critical (global configuration) 145

dot1x critical (interface configuration) 146

dot1x default 147

dot1x guest-vlan 149

dot1x guest-vlan supplicant 151

dot1x host-mode 152

dot1x initialize 154

dot1x mac-auth-bypass 155

dot1x max-reauth-req 157

dot1x max-req 159

dot1x max-start 162

dot1x multi-hosts 164

dot1x multiple-hosts 165

dot1x pae 167

dot1x port-control 169

dot1x re-authenticate (EtherSwitch) 172

dot1x re-authenticate (privileged EXEC) 173

dot1x reauthentication 175

dot1x re-authentication (EtherSwitch) 178

dot1x supplicant interface 179

dot1x system-auth-control 180

dot1x timeout 182

dot1x timeout (EtherSwitch) 187

dpd 189

drop (type access-control) 190
identity policy 363
identity profile 364
identity profile eap oudp 366
idle-timeout (WebVPN) 367
if-state nhrp 368
import 369
include-local-lan 370
incoming 372
initial-contact force 374
initiate mode 375
inservice (WebVPN) 376
inspect 377
inspect (config-profile) 379
integrity 380
interface (RITE) 382
interface (VASI) 384
interface virtual-template 386
ip (webvpn url rewrite) 389
ip access-group 390
ip access-list 392
ip access-list hardware permit fragments 395
ip access-list logging interval 397
ip access-list log-update 398
ip access-list resequence 400
ip access-list logging hash-generation 402
ip-address (ca-trustpoint) 404
ip address dhcp 406
ip address (WebVPN) 409
ip admission 411
ip admission consent banner 414
ip admission name 416
ip admission name bypass regex 421
ip admission name http-basic 422
ip admission name method-list 424
ip admission name ntlm 426
ip admission name order 428
ip admission proxy http 429
ip admission virtual-ip 432
ip audit 433
ip audit attack 434
ip audit info 435
ip audit name 436
ip audit notify 438
ip audit po local 439
ip audit po max-events 440
ip audit po protected 441
ip audit po remote 442
ip audit signature 444
ip audit smtp 445
ip auth-proxy (global configuration) 446
ip auth-proxy (interface configuration) 448
ip auth-proxy auth-proxy-banner 449
ip auth-proxy max-login-attempts 451
ip auth-proxy name 453
ip auth-proxy watch-list 456
ip device tracking probe 458
ip dhcp client broadcast-flag (interface) 459
ip dhcp support tunnel unicast 460
ip-extension 461
ip http ezvpn 465

CHAPTER 6
ip inspect through ip security strip 467
ip inspect 469
ip inspect alert-off 471
ip inspect audit-trail 472
ip inspect dns-timeout 474
ip inspect hashtable 476
ip inspect L2-transparent dhcp-passthrough 477
ip inspect log drop-pkt  479
ip inspect max-incomplete high  482
ip inspect max-incomplete low  484
ip inspect name  486
ip inspect one-minute high  498
ip inspect one-minute low  500
ip inspect tcp block-non-session  502
ip inspect tcp finwait-time  504
ip inspect tcp idle-time  506
ip inspect tcp max-incomplete host  508
ip inspect tcp reassembly  510
ip inspect tcp synwait-time  512
ip inspect tcp window-scale-enforcement loose  513
ip inspect udp idle-time  515
ip inspect waas enable  517
integrity  518
ip interface  520
ip ips  522
ip ips auto-update  524
ip ips config location  526
ip ips deny-action ips-interface  528
ip ips enable-clidelta  530
ip ips event-action-rules  531
ip ips fail closed  532
ip ips inherit-obsolete-tunings  533
ip ips memory regex chaining  535
ip ips memory threshold  537
ip ips name  539
ip ips notify  541
ip ips sdf location  542
ip ips signature  544
ip ips signature-category  546
ip ips signature-definition  547
ip ips signature disable  548
ip trigger-authentication (global)  675  
ip trigger-authentication (interface)  677  
ip urlfilter alert  678  
ip urlfilter allowmode  680  
ip urlfilter audit-trail  681  
ip urlfilter cache  683  
ip urlfilter exclusive-domain  685  
ip urlfilter max-request  687  
ip urlfilter max-resp-pak  688  
ip urlfilter server vendor  689  
ip urlfilter source-interface  691  
ip urlfilter truncate  692  
ip urlfilter urlf-server-log  694  
ip verify drop-rate compute interval  695  
ip verify drop-rate compute window  697  
ip verify drop-rate notify hold-down  699  
ip verify unicast notification threshold  700  
ip verify unicast reverse-path  701  
ip verify unicast source reachable-via  705  
ip virtual-reassembly  711  
ip virtual-reassembly-out  714  
ip vrf  716  
ip vrf forwarding  718  
ip vrf forwarding (server-group)  719  
ip wccp web-cache accelerated  721  
ips signature update cisco  723  
ipsec profile  724  
ipv4 (ldap)  725  
ipv6 crypto map  726  
ipv6 cga modifier rsakeypair  727  
ipv6 cga rsakeypair  729  
ipv6 inspect  730  
ipv6 inspect alert-off  731  
ipv6 inspect audit trail  732
K through L

keepalive (isakmp profile) 803
kerberos clients mandatory 804
kerberos credentials forward 805
kerberos instance map 806
kerberos local-realm 807
kerberos password 808
kerberos preauth 809
kerberos processes 811
kerberos realm 812
kerberos retry 814
kerberos server 815
kerberos srvtab entry 817
kerberos srvtab remote 819
kerberos timeout 820
key (config-radius-server) 821
key (isakmp-group) 823
key (TACACS+) 824
key config-key 825
key config-key password-encryption 826
key-hash 828
keyring 829
keyring (IKEv2 profile) 830
key-set 832
key-string (IKE) 834
key-string (SSH) 836
language 837
ldap attribute-map 838
ldap search 839
ldap server 840
length (RITE) 841
license (parameter-map) 843
lifetime (cs-server) 844
lifetime (IKE policy) 847
lifetime (IKEv2 profile) 849
lifetime crl 850
lifetime enrollment-request 851
limit address-count 852
list (LSP Attributes) 853
list (WebVPN) 854
li-view 855
load-balance (server-group) 857
load classification 861
local-address 865
local-port (WebVPN) 867
local priority 869
lockdown (LSP Attributes) 871
log (policy-map) 872
log (parameter-map type) 873
log (type access-control) 875
logging (parameter-map) 877
logging dmvpn 878
logging enabled 880
logging ip access-list cache (global configuration) 881
logging ip access-list cache (interface configuration) 883
login authentication 885
login-auth-bypass 887
login block-for 888
Contents

login delay 891
login-message 893
login quiet-mode access-class 894
login-photo 896
logo 897
database archive through dns

- data, on page 3
- database archive, on page 4
- database level, on page 7
- database url, on page 11
- database username, on page 16
- deadline (config-ldap-server), on page 19
- deadline (server-group configuration), on page 21
- debug cts xsp filter events, on page 23
- def-domain, on page 24
- default (cs-server), on page 25
- default (ca-trustpoint), on page 28
- default (ca-trustpool), on page 29
- default-group-policy, on page 31
- deny, on page 32
- deny (Catalyst 6500 series switches), on page 43
- deny (IP), on page 54
- deny (IPv6), on page 64
- deny (MAC ACL), on page 72
- deny (WebVPN), on page 75
- description (dot1x credentials), on page 78
- description (identify zone), on page 79
- description (identity policy), on page 80
- description (identity profile), on page 81
- description (IKEv2 keyring), on page 82
- description (isakmp peer), on page 83
- destination host, on page 84
- destination realm, on page 85
- device (identity profile), on page 86
- device-role, on page 88
- device-sensor accounting, on page 90
- device-sensor filter-list cdp, on page 91
- device-sensor filter-list dhcp, on page 93
- device-sensor filter-list lldp, on page 95
- device-sensor filter-spec, on page 97
- device-sensor filter-spec http, on page 99
- device-sensor notify, on page 101
- dhcp (IKEv2), on page 103
- dhcp server (isakmp), on page 104
- dhcp timeout, on page 105
- dialer aaa, on page 106
- diameter origin host, on page 108
- diameter origin realm, on page 109
- diameter peer, on page 110
- diameter redundancy, on page 111
- diameter timer, on page 112
- diameter vendor supported, on page 114
- disable open-media-channel, on page 115
- disconnect ssh, on page 116
- dn, on page 117
- dn (IKEv2), on page 119
- dnis (AAA preauthentication), on page 120
- dnis (RADIUS), on page 122
- dnis bypass (AAA preauthentication configuration), on page 124
- dns, on page 125
data

To configure the data interface type and number for a redundancy group, use the `data` command in redundancy application group configuration mode. To remove the configuration, use the `no` form of this command.

```
data interface-type interface-number
no data interface-type interface-number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface-type</code></td>
<td>Interface type.</td>
</tr>
<tr>
<td><code>interface-number</code></td>
<td>Interface number.</td>
</tr>
</tbody>
</table>

**Command Default**

No data interface is configured.

**Command Modes**

Redundancy application group configuration (config-red-app-grp)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.1S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `data` command to configure the data interface. The data interface can be the same physical interface as the control interface.

**Examples**

The following example shows how to configure the data Gigabit Ethernet interface for group 1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# data GigabitEthernet 0/0/0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>application redundancy</code></td>
<td>Enters redundancy application configuration mode.</td>
</tr>
<tr>
<td><code>authentication</code></td>
<td>Configures clear text authentication and MD5 authentication for a redundancy group.</td>
</tr>
<tr>
<td><code>control</code></td>
<td>Configures the control interface type and number for a redundancy group.</td>
</tr>
<tr>
<td><code>group(firewall)</code></td>
<td>Enters redundancy application group configuration mode.</td>
</tr>
<tr>
<td><code>name</code></td>
<td>Configures the redundancy group with a name.</td>
</tr>
<tr>
<td><code>preempt</code></td>
<td>Enables preemption on the redundancy group.</td>
</tr>
<tr>
<td><code>protocol</code></td>
<td>Defines a protocol instance in a redundancy group.</td>
</tr>
</tbody>
</table>
database archive

To set the certification authority (CA) certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file, use the `database archive` command in certificate server configuration mode. To disable the auto-archive feature, use the `no` form of this command.

database archive {pkcs12|pem} [password password]
no database archive {pkcs12|pem} [password password]

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pkcs12</td>
<td>Export as a PKCS12 file. The default is PKCS12.</td>
</tr>
<tr>
<td>pem</td>
<td>Export as a privacy-enhanced mail (PEM) file.</td>
</tr>
<tr>
<td>password</td>
<td>(Optional) Password to encrypt the CA certificate and CA key. If a password is not specified, you will be prompted for the password.</td>
</tr>
</tbody>
</table>

**Command Default**

The archive format is PKCS (that is, the CA certificate and CA key are exported into a PKCS12 file, and you are prompted for the password when the certificate server is turned on the first time).

**Command Modes**

Certificate server configuration (cs-server)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must configure the `crypto pki server` command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

Use this command to configure the autoarchive format for the CA certificate and CA key. The archive can later be used to restore your certificate server.

If autoarchiving is not explicitly turned off when the certificate server is first enabled (using the `no shutdown` command), the CA certificate and CA key will be archived automatically, applying the following rule:

- The CA key must be (1) manually generated and marked “exportable” or (2) automatically generated by the certificate server (it will be marked nonexportable).

**Note**

It is strongly recommended that if the password is included in the configuration to suppress the prompt after the `no shutdown` command, the password should be removed from the configuration after the archiving is finished.

**Examples**

The following example shows that certificate server autoarchiving has been enabled. The CA certificate and CA key format has been set to PEM, and the password has been set as cisco123.
Router (config)# crypto pki server myserver
Router (cs-server)# database archive pem password cisco123

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-rollover</td>
<td>Enables the automated CA certificate rollover functionality.</td>
</tr>
<tr>
<td>cdp-url</td>
<td>Specifies a CDP to be used in certificates that are issued by the certificate server.</td>
</tr>
<tr>
<td>crl (cs-server)</td>
<td>Specifies the CRL PKI CS.</td>
</tr>
<tr>
<td>crypto pki server</td>
<td>Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials</td>
</tr>
<tr>
<td>database level</td>
<td>Controls what type of data is stored in the certificate enrollment database.</td>
</tr>
<tr>
<td>database url</td>
<td>Specifies the location where database entries for the CS is stored or published.</td>
</tr>
<tr>
<td>database username</td>
<td>Specifies the requirement of a username or password to be issued when accessing the primary database location.</td>
</tr>
<tr>
<td>default (cs-server)</td>
<td>Resets the value of the CS configuration command to its default.</td>
</tr>
<tr>
<td>grant auto rollover</td>
<td>Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.</td>
</tr>
<tr>
<td>grant auto trustpoint</td>
<td>Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.</td>
</tr>
<tr>
<td>grant none</td>
<td>Specifies all certificate requests to be rejected.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>grant ra-auto</td>
<td>Specifies that all enrollment requests from an RA be granted automatically.</td>
</tr>
<tr>
<td>hash (cs-server)</td>
<td>Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.</td>
</tr>
<tr>
<td>issuer-name</td>
<td>Specifies the DN as the CA issuer name for the CS.</td>
</tr>
<tr>
<td>lifetime (cs-server)</td>
<td>Specifies the lifetime of the CA or a certificate.</td>
</tr>
<tr>
<td>mode ra</td>
<td>Enters the PKI server into RA certificate server mode.</td>
</tr>
<tr>
<td>mode sub-cs</td>
<td>Enters the PKI server into sub-certificate server mode.</td>
</tr>
<tr>
<td>redundancy (cs-server)</td>
<td>Specifies that the active CS is synchronized to the standby CS.</td>
</tr>
<tr>
<td>serial-number (cs-server)</td>
<td>Specifies whether the router serial number should be included in the certificate request.</td>
</tr>
<tr>
<td>show (cs-server)</td>
<td>Displays the PKI CS configuration.</td>
</tr>
<tr>
<td>shutdown (cs-server)</td>
<td>Allows a CS to be disabled without removing the configuration.</td>
</tr>
</tbody>
</table>
database level

To control what type of data is stored in the certificate enrollment database, use the database level command in certificate server configuration mode. To return to the default functionality, use the no form of this command.

database level {minimal|names|complete}
no database level {minimal|names|complete}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>minimal</th>
<th>names</th>
<th>complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>minimal</td>
<td>Enough information is stored only to continue issuing new certificates without conflict. This is the default functionality.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>names</td>
<td>The serial number and subject name of each certificate are stored in the database, providing enough information for the administrator to find and revoke and particular certificate, if necessary.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>complete</td>
<td>Each issued certificate is written to the database. If this keyword is used, you should enable the database url command; see “Usage Guidelines” for more information.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Command Default

minimal

Command Modes

Certificate server configuration (cs-server)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You must configure the crypto pki server command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

The database level command is used to describe the database of certificates and certification authority (CA) states. After the user downgrades the database level, the old data stays the same and the new data is logged at the new level.

minimum Level

The ca-label.ser file is always available. It contains the previously issued certificate’s serial number, which is always 1. If the .ser file is unavailable and the CA server has a self-signed certificate in the local configuration, the CA server will refuse to issue new certificates.

The file format is as follows:

```
last_serial =
serial-number
```

names Level

The serial-number.cnm file, which is written for each issued certificate, contains the “human readable decoded subject name” of the issued certificate and the “der encoded” values. This file can also include a certificate expiration date and the current status. (The minimum level files are also written out.)

The file format is as follows:
subjectname_der = <base64 encoded der value>
subjectname_str = <human readable decode subjectname>
expiration = <expiration date>
status = valid | revoked

**complete Level**

The *serial-number*.cer file, which is written for each issued certificate, is the binary certificate without additional encoding. (The *minimum* and *names* level files are also written out.)

The **complete** level produces a large amount of information, so you may want to store all database entries on an external TFTP server via the **database url** command unless your router does one of the following:

- Issues only a small number of certificates
- Has a local file system that is designed to support a large number of write operations and has sufficient storage for the certificates that are being issued

**Examples**

The following example shows how configure a minimum database to be stored on the local system:

```
Router#(config) ip http server
Router#(config) crypto pki server myserver
Router#(cs-server) database level minimum
Router#(cs-server) database url nvram:
Router#(cs-server) issuer-name CN = ipsec_cs,L = Santa Cruz,C = US
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-rollover</td>
<td>Enables the automated CA certificate rollover functionality.</td>
</tr>
<tr>
<td>cdp-url</td>
<td>Specifies a CDP to be used in certificates that are issued by the certificate server.</td>
</tr>
<tr>
<td>crl (cs-server)</td>
<td>Specifies the CRL PKI CS.</td>
</tr>
<tr>
<td>crypto pki server</td>
<td>Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials</td>
</tr>
<tr>
<td>database archive</td>
<td>Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.</td>
</tr>
<tr>
<td>database url</td>
<td>Specifies the location where database entries for the CS is stored or published.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>database username</td>
<td>Specifies the requirement of a username or password to be issued when accessing the primary database location.</td>
</tr>
<tr>
<td>default (cs-server)</td>
<td>Resets the value of the CS configuration command to its default.</td>
</tr>
<tr>
<td>grant auto rollover</td>
<td>Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.</td>
</tr>
<tr>
<td>grant auto trustpoint</td>
<td>Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.</td>
</tr>
<tr>
<td>grant none</td>
<td>Specifies all certificate requests to be rejected.</td>
</tr>
<tr>
<td>grant ra-auto</td>
<td>Specifies that all enrollment requests from an RA be granted automatically.</td>
</tr>
<tr>
<td>hash (cs-server)</td>
<td>Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.</td>
</tr>
<tr>
<td>issuer-name</td>
<td>Specifies the DN as the CA issuer name for the CS.</td>
</tr>
<tr>
<td>lifetime (cs-server)</td>
<td>Specifies the lifetime of the CA or a certificate.</td>
</tr>
<tr>
<td>mode ra</td>
<td>Enters the PKI server into RA certificate server mode.</td>
</tr>
<tr>
<td>mode sub-cs</td>
<td>Enters the PKI server into sub-certificate server mode.</td>
</tr>
<tr>
<td>redundancy (cs-server)</td>
<td>Specifies that the active CS is synchronized to the standby CS.</td>
</tr>
<tr>
<td>serial-number (cs-server)</td>
<td>Specifies whether the router serial number should be included in the certificate request.</td>
</tr>
<tr>
<td>show (cs-server)</td>
<td>Displays the PKI CS configuration.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| shutdown (cs-server)    | Allows a CS to be disabled without removing the configuration.
database url

To specify the location where database entries for the certificate server (CS) is stored or published, use the database url command in certificate server configuration mode. To return to the default location, use the no form of this command.

Storing Files to a Primary Location
database url root-url

Storing Critical CS Files to a Specific Location
database url [{cnm|crl|crt|p12|pem|ser}] root-url [username username] [password [encrypt-type] password]
no database url [{cnm|crl|crt|p12|pem|ser}] root-url [username username] [password [encrypt-type] password]

Publishing Noncritical CS Files to a Specific Location
database url {cnm|crl|crt} publish root-url [username username] [password [encrypt-type] password]
no database url {cnm|crl|crt} publish root-url [username username] [password [encrypt-type] password]

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>root-url</th>
<th>Location where database entries will be written out. The URL can be any URL that is supported by the Cisco IOS file system (IFS).</th>
</tr>
</thead>
<tbody>
<tr>
<td>cnm</td>
<td>(Optional) Specifies the certificate name and expiration file to be stored or published to a specific location.</td>
<td></td>
</tr>
<tr>
<td>crl</td>
<td>(Optional) Specifies the DER-encoded certificate revocation list to be stored or published to a specific location</td>
<td></td>
</tr>
<tr>
<td>crt</td>
<td>(Optional) Specifies the DER-encoded certificate files to be stored or published to a specific location.</td>
<td></td>
</tr>
<tr>
<td>p12</td>
<td>(Optional) Specifies the CS certificate and key archive file in PKCS12 format to be stored to a specific location.</td>
<td></td>
</tr>
<tr>
<td>pem</td>
<td>(Optional) Specifies the CS certificate and key archive file in privacy-enhanced mail format to be stored to a specific location.</td>
<td></td>
</tr>
<tr>
<td>ser</td>
<td>(Optional) Specifies the current serial number to be stored to a specific location.</td>
<td></td>
</tr>
<tr>
<td>publish</td>
<td>Specifies that the files will be made available to a published location.</td>
<td></td>
</tr>
<tr>
<td>username username</td>
<td>(Optional) When prompted, a username will be used to access a storage location.</td>
<td></td>
</tr>
<tr>
<td>password password</td>
<td>(Optional) When prompted, a password will be used to access a storage location.</td>
<td></td>
</tr>
</tbody>
</table>
**encrypt-type**

(Optional) Type of encryption to be used for the password. If no password type is specified the password is sent as clear text.

- Default is 0; specifies that the password entered will be encrypted.
- 7; specifies that the password entered is already encrypted.

---

**Command Default**

The default file storage location is flash.

No default file publish location is specified.

**Command Modes**

Certificate server configuration (cs-server)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(4)T</td>
<td>This command was modified. The following keywords and arguments were added\r\ncnm, crl,\r\ncrt, p12, pem, ser, publish, username username, encrypt-type and password password.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must configure the `crypto pki server` command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

The `database url` command specifies a combined list of all the certificates that have been issued and the current command revocation list (CRL). The CRL is written to the certificate enrollment database with the name of the certificate server.

**Note**

Although issuing the `database url` command is not required, it is recommended. Unless your router has a local file system that is designed for a large number of write operations and has sufficient storage for the certificates that are issued, you should issue this command.

**Cisco IOS File System**

The router uses any file system that is supported by your version of Cisco IOS software (such as TFTP, FTP, flash, and NVRAM) to send a certificate request and to receive the issued certificate. A user may wish to enable IFS certificate enrollment when his or her certification authority (CA) does not support Simple Certificate Enrollment Protocol (SCEP).

**Specifying CS Storage and Publication Location by File Type**

The CS allows the flexibility to store different critical file types to specific storage locations and publish non-critical files to the same or alternate locations. When choosing storage locations consider the file security needed and server performance. For instance, serial number files (.ser) and archive files (.p12 or .pem) might have greater security restrictions than the general certificates storage location (.crt) or the name file storage location (.cnm). Performance of your certificate server may be affected by the storage location(s) you choose, for example, reading from a network location would likely take more time than reading directly from a router’s local storage device.
Examples

The following example shows how to configure all database entries to be written out to a TFTP server:

Router# (config) ip http server
Router# (config) crypto pki server myserver
Router# (cs-server) database level complete
Router# (cs-server) database url tftp://mytftp

The following example shows the configuration of a primary storage location for critical files, a specific storage location for the critical file serial number file, the main CS database file, and a password protected file publication location for the CRL file:

Router (config)# crypto pki server mycs
Router (cs-server)# database url ftp://cs-db.company.com

% Server database url was changed. You need to move the % existing database to the new location.
!
Router (cs-server)# database url ser nvram:
Router (cs-server)# database url crl publish ftp://crl.company.com username myname password mypassword
Router (cs-server)# end

The following show output displays the specified primary storage location and critical file storage locations specified:

Router# show
Sep 3 20:19:34.216: %SYS-5-CONFIG_I: Configured from console by user on console Router# show crypto pki server

Certificate Server mycs:
    Status: disabled
    Server's configuration is unlocked (enter "no shut" to lock it)
    Issuer name: CN=mycs
    CA cert fingerprint: -Not found-
    Granting mode is: manual
    Last certificate issued serial number: 0x0
    CA certificate expiration timer: 00:00:00 GMT Jan 1 1970
    CRL not present.
    Current primary storage dir: ftp://cs-db.company.com
    Current storage dir for .ser files: nvram:
    Database Level: Minimum - no cert data written to storage
Router#

The following show output displays all storage and publication locations. The serial number file (.ser) is stored in NVRAM. The CRL file will be published to ftp://crl.company.com with a username and password. All other critical files will be stored to the primary location, ftp://cs-db.company.com.

Router# show running-config
section crypto pki server
    crypto pki server mycs shutdown database url ftp://cs-db.company.com
database url crl publish ftp://crl.company.com username myname password 7
12141c0713181f13253920
database url ser nvram:
Router#
Verifying the Database URL

To ensure that the specified URL is working correctly, configure the `database url` command before you issue the `no shutdown` command on the certificate server for the first time. If the URL is broken, you will see output as follows:

```
Router(config)# crypto pki server mycs
Router(cs-server)# database url ftp://myftpserver
Router(cs-server)# no shutdown
% Once you start the server, you can no longer change some of
% the configuration.
Are you sure you want to do this? [yes/no]: yes
```

Translating "myftpserver"

% There was a problem reading the file 'mycs.ser' from certificate storage.

% Please verify storage accessibility and enable the server again.

```
% Failed to generate CA certificate - 0xFFFFFFFF
% The Certificate Server has been disabled.
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>auto-rollover</code></td>
<td>Enables the automated CA certificate rollover functionality.</td>
</tr>
<tr>
<td><code>cdp-url</code></td>
<td>Specifies a CDP to be used in certificates that are issued by the certificate server.</td>
</tr>
<tr>
<td><code>crl (cs-server)</code></td>
<td>Specifies the CRL PKI CS.</td>
</tr>
<tr>
<td><code>crypto pki server</code></td>
<td>Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials</td>
</tr>
<tr>
<td><code>database archive</code></td>
<td>Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.</td>
</tr>
<tr>
<td><code>database level</code></td>
<td>Controls what type of data is stored in the certificate enrollment database.</td>
</tr>
<tr>
<td><code>database username</code></td>
<td>Specifies the requirement of a username or password to be issued when accessing the primary database location.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>default (cs-server)</td>
<td>Resets the value of the CS configuration command to its default.</td>
</tr>
<tr>
<td>grant auto rollover</td>
<td>Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.</td>
</tr>
<tr>
<td>grant auto trustpoint</td>
<td>Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.</td>
</tr>
<tr>
<td>grant none</td>
<td>Specifies all certificate requests to be rejected.</td>
</tr>
<tr>
<td>grant ra-auto</td>
<td>Specifies that all enrollment requests from an RA be granted automatically.</td>
</tr>
<tr>
<td>hash (cs-server)</td>
<td>Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.</td>
</tr>
<tr>
<td>issuer-name</td>
<td>Specifies the DN as the CA issuer name for the CS.</td>
</tr>
<tr>
<td>lifetime (cs-server)</td>
<td>Specifies the lifetime of the CA or a certificate.</td>
</tr>
<tr>
<td>mode ra</td>
<td>Enters the PKI server into RA certificate server mode.</td>
</tr>
<tr>
<td>mode sub-cs</td>
<td>Enters the PKI server into sub-certificate server mode</td>
</tr>
<tr>
<td>redundancy (cs-server)</td>
<td>Specifies that the active CS is synchronized to the standby CS.</td>
</tr>
<tr>
<td>serial-number (cs-server)</td>
<td>Specifies whether the router serial number should be included in the certificate request.</td>
</tr>
<tr>
<td>show (cs-server)</td>
<td>Displays the PKI CS configuration.</td>
</tr>
<tr>
<td>shutdown (cs-server)</td>
<td>Allows a CS to be disabled without removing the configuration.</td>
</tr>
</tbody>
</table>
**database username**

To require a username or password to be issued when accessing the primary database location, use the `database username` command in certificate server configuration mode. To return to the default value, use the `no` form of this command.

```
database username username [password [encr-type] password]
no database username username [password [encr-type] password]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>username</code></td>
<td>When prompted, a username will be used to access a storage location.</td>
</tr>
<tr>
<td><code>password</code> <code>password</code></td>
<td>(Optional) When prompted, a password will be used to access a storage location.</td>
</tr>
</tbody>
</table>
| `encr-type` `password` | (Optional) Type of encryption to be used for the password. If no password encryption type is specified, the password is sent as clear text.  
  - Default is 0; specifies that the password entered will be encrypted.  
  - 7; specifies the password entered is already encrypted. |

**Command Default**

No username or password will be used to access the primary database storage location.

**Command Modes**

Certificate server configuration (cs-server)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(4)T</td>
<td>The command name was changed from <code>database (certificate server)</code> to <code>database username</code>.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must configure the `crypto pki server` command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

All information stored in the remote database is public: there are no private keys stored in the database location. Using a password helps to protect against a potential attacker who can change the contents of the .ser or .crl file. If the contents of the files are changed, the certificate server may shut down, refusing to either issue new certificates or respond to Simple Certificate Enrollment Protocol (SCEP) requests until the files are restored.

It is good security practice to protect all information exchanges with the database server using IP Security (IPsec). To protect your information, use a remote database to obtain the appropriate certificates and setup the necessary IPsec connections to protect all future access to the database server.

**Examples**

The following example shows how to specify the username “mystorage” when the primary storage location is on an external TFTP server:

```
Router (config)# ip http server
Router (config)# crypto pki server myserver
Router (cs-server)# database level complete
Router (cs-server)# database url tftp://mytftp
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-rollover</td>
<td>Enables the automated CA certificate rollover functionality.</td>
</tr>
<tr>
<td>cdp-url</td>
<td>Specifies a CDP to be used in certificates that are issued by the certificate server.</td>
</tr>
<tr>
<td>crl (cs-server)</td>
<td>Specifies the CRL PKI CS.</td>
</tr>
<tr>
<td>crypto pki server</td>
<td>Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials.</td>
</tr>
<tr>
<td>database archive</td>
<td>Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.</td>
</tr>
<tr>
<td>database level</td>
<td>Controls what type of data is stored in the certificate enrollment database.</td>
</tr>
<tr>
<td>database url</td>
<td>Specifies the location where database entries for the CS is stored or published.</td>
</tr>
<tr>
<td>default (cs-server)</td>
<td>Resets the value of the CS configuration command to its default.</td>
</tr>
<tr>
<td>grant auto rollover</td>
<td>Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.</td>
</tr>
<tr>
<td>grant auto trustpoint</td>
<td>Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.</td>
</tr>
<tr>
<td>grant none</td>
<td>Specifies all certificate requests to be rejected.</td>
</tr>
<tr>
<td>grant ra-auto</td>
<td>Specifies that all enrollment requests from an RA be granted automatically.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>hash (cs-server)</td>
<td>Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.</td>
</tr>
<tr>
<td>issuer-name</td>
<td>Specifies the DN as the CA issuer name for the CS.</td>
</tr>
<tr>
<td>lifetime (cs-server)</td>
<td>Specifies the lifetime of the CA or a certificate.</td>
</tr>
<tr>
<td>mode ra</td>
<td>Enters the PKI server into RA certificate server mode.</td>
</tr>
<tr>
<td>mode sub-cs</td>
<td>Enters the PKI server into sub-certificate server mode.</td>
</tr>
<tr>
<td>redundancy (cs-server)</td>
<td>Specifies that the active CS is synchronized to the standby CS.</td>
</tr>
<tr>
<td>serial-number (cs-server)</td>
<td>Specifies whether the router serial number should be included in the certificate request.</td>
</tr>
<tr>
<td>show (cs-server)</td>
<td>Displays the PKI CS configuration.</td>
</tr>
<tr>
<td>shutdown (cs-server)</td>
<td>Allows a CS to be disabled without removing the configuration.</td>
</tr>
</tbody>
</table>
deadtime (config-ldap-server)

To configure the duration during which no new transaction requests are sent to the Lightweight Directory Access Protocol (LDAP) server, use the deadtime command in LDAP server configuration mode. To set the deadtime to 0 minutes, use the no form of this command.

```
deadtime minutes
no deadtime
```

**Syntax Description**

| minutes | Length of time, in minutes, for which an LDAP server is skipped over by transaction requests. The range is from 1 to 1440. |

**Command Default**

Deadtime is set to 0 minutes.

**Command Modes**

LDAP server configuration (config-ldap-server)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.4(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The authentication, authorization, and accounting (AAA) client components make use of the DEAD and ALIVE states to keep track of each server state to handle protocol transactions effectively. If the state is DEAD, the client component applies a default set of policies to users or subscribers and allows them to access the default web content. If the state is ALIVE, the client component gets the actual policies from the LDAP server.

If the automate-tester command is configured along with the deadtime command, after every deadtime expiry, the AAA test APIs send a dummy bind request packet to the LDAP server.

- If a bind response is received, the server state is updated as ALIVE and further dummy bind requests are not sent.
- If a bind response is not received, the server state remains as DEAD and after every deadtime expiry, AAA test APIs send dummy bind request packets to the LDAP server.

If the deadtime command is configured and the automate-tester command is not configured when the server is not reachable, the server state remains DEAD until the deadtime expiry is reached, after which the state changes to ALIVE.

**Examples**

The following example specifies a one-minute deadtime for LDAP server server1 once it has failed to respond to transaction requests:

```
Device> enable
Device# configure terminal
Device(config)# username user1 password 0 pwd1
Device(config)# aaa new-model
Device(config)# ldap server server1
Device(config-ldap-server)# deadtime 1
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa new-model</td>
<td>Enables the AAA access control model.</td>
</tr>
<tr>
<td>ldap server</td>
<td>Specifies the name for the LDAP server configuration and enters LDAP server configuration mode.</td>
</tr>
</tbody>
</table>
deadtime (server-group configuration)

To configure deadtime within the context of RADIUS server groups, use the `deadtime` command in server group configuration mode. To set deadtime to 0, use the `no` form of this command.

```
deadtime  minutes
no  deadtime
```

**Syntax Description**

<table>
<thead>
<tr>
<th>minutes</th>
<th>Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours).</th>
</tr>
</thead>
</table>

**Command Default**

Deadtime is set to 0.

**Command Modes**

Server-group configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to configure the deadtime value of any RADIUS server group. The value of deadtime set in the server groups will override the server that is configured globally. If deadtime is omitted from the server group configuration, the value will be inherited from the master list. If the server group is not configured, the default value (0) will apply to all servers in the group.

**When the RADIUS Server Is Marked As Dead**

For Cisco IOS versions prior to 12.2(13.7)T, the RADIUS server will be marked as dead if a transaction is transmitted for the configured number of retransmits and a valid response is not received from the server within the configured timeout for any of the RADIUS packet transmissions.

For Cisco IOS versions 12.2(13.7)T and later, the RADIUS server will be marked as dead if both of the following conditions are met:

1. A valid response has not been received from the RADIUS server for any outstanding transaction for at least the timeout period that is used to determine whether to retransmit to that server, and

2. Across all transactions being sent to the RADIUS server, at least the requisite number of retransmits +1 (for the initial transmission) have been sent consecutively without receiving a valid response from the server with the requisite timeout.

**Examples**

The following example specifies a one-minute deadtime for RADIUS server group group1 once it has failed to respond to authentication requests:

```
aaa group server radius group1
```
server 10.1.1.1 auth-port 1645 acct-port 1646
server 10.2.2.2 auth-port 2000 acct-port 2001
deadtime 1

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>radius-server</td>
<td>Sets the deadtime value globally.</td>
</tr>
</tbody>
</table>

| deadtime (server-group configuration) |
debug cts sxp filter events

To log events related to the creation, deletion, update of filter-lists and filter-groups, and also to capture match actions that happen during filtering, use the `debug cts sxp filter events` command in privileged EXEC mode.

```
d debug cts sxp filter events
no debug cts sxp filter events
```

**Syntax Description**
This command has no keywords or arguments

**Command Default**
Debugging is not enabled

**Command Modes**
Privileged EXEC mode (#)

**Command History**
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example**

```
Device# debug cts sxp filter events
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cts sxp filter-list</td>
<td>Creates a SXP filter list to filter IP-SGT bindings based on IP prefixes, SGT or a combination of both.</td>
</tr>
<tr>
<td>cts sxp filter-group</td>
<td>Creates a filter group for grouping a set of peers and applying a filter list to them.</td>
</tr>
<tr>
<td>cts sxp filter-enable</td>
<td>Enable SXP IP-prefix and SGT-based filtering.</td>
</tr>
<tr>
<td>show cts sxp filter-group</td>
<td>Displays information about the configured filter groups.</td>
</tr>
<tr>
<td>show cts sxp filter-list</td>
<td>Displays information about the configured filter lists.</td>
</tr>
<tr>
<td>debug cts sxp error</td>
<td>Generates the error log for filtering.</td>
</tr>
</tbody>
</table>
def-domain

To specify the default domain for the client to use, use the def-domain command in IKEv2 authorization policy configuration mode. To disable, use the no form of this command.

```plaintext
def-domain  domain-name
no def-domain  domain-name
```

**Syntax Description**

```
domain-name  Domain name.
```

**Command Default**

The default domain is not specified.

**Command Modes**

IKEv2 authorization policy configuration (config-ikev2-author-policy)

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(1T)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

Before using the def-domain command, you must first configure the crypto ikev2 authorization policy command. This value set in this command is sent to the client via the nonstandard Cisco unity configuration attribute.

**Examples**

The following example show how to configure the def-domain command:

```
Router(config)# crypto ikev2 authorization policy policy1
Router(config-ikev2-profile)# def-domain cisco
```

**Related Commands**

```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2 authorization policy</td>
<td>Specifies an IKEv2 authorization policy group.</td>
</tr>
</tbody>
</table>
```
default (cs-server)

To reset the value of the certificate server (CS) configuration subcommand to its default, use the `default` command in ca-trustpoint configuration mode.

```
default command-name
```

**Syntax Description**

| command-name | Certificate server configuration subcommand. |

**Command Default**

No default behavior or values.

**Command Modes**

Certificate server configuration (cs-server)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must configure the `crypto pki server` command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

**Examples**

The following example shows how to remove the `crl` command from your configuration; the default of `crl` is off.

```
Router(cs-server)# default crl
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>auto-rollover</code></td>
<td>Enables the automated CA certificate rollover functionality.</td>
</tr>
<tr>
<td><code>cdp-url</code></td>
<td>Specifies a CDP to be used in certificates that are issued by the certificate server.</td>
</tr>
<tr>
<td><code>crl (cs-server)</code></td>
<td>Specifies the CRL PKI CS.</td>
</tr>
<tr>
<td><code>crypto pki server</code></td>
<td>Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials.</td>
</tr>
<tr>
<td><code>database archive</code></td>
<td>Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>database level</td>
<td>Controls what type of data is stored in the certificate enrollment database.</td>
</tr>
<tr>
<td>database url</td>
<td>Specifies the location where database entries for the CS is stored or published.</td>
</tr>
<tr>
<td>database username</td>
<td>Specifies the requirement of a username or password to be issued when accessing the primary database location.</td>
</tr>
<tr>
<td>grant auto rollover</td>
<td>Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.</td>
</tr>
<tr>
<td>grant auto trustpoint</td>
<td>Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.</td>
</tr>
<tr>
<td>grant none</td>
<td>Specifies all certificate requests to be rejected.</td>
</tr>
<tr>
<td>grant ra-auto</td>
<td>Specifies that all enrollment requests from an RA be granted automatically.</td>
</tr>
<tr>
<td>hash (cs-server)</td>
<td>Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.</td>
</tr>
<tr>
<td>issuer-name</td>
<td>Specifies the DN as the CA issuer name for the CS.</td>
</tr>
<tr>
<td>lifetime (cs-server)</td>
<td>Specifies the lifetime of the CA or a certificate.</td>
</tr>
<tr>
<td>mode ra</td>
<td>Enters the PKI server into RA certificate server mode.</td>
</tr>
<tr>
<td>mode sub-cs</td>
<td>Enters the PKI server into sub-certificate server mode.</td>
</tr>
<tr>
<td>redundancy (cs-server)</td>
<td>Specifies that the active CS is synchronized to the standby CS.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>serial-number (cs-server)</td>
<td>Specifies whether the router serial number should be included in the certificate request.</td>
</tr>
<tr>
<td>show (cs-server)</td>
<td>Displays the PKI CS configuration.</td>
</tr>
<tr>
<td>shutdown (cs-server)</td>
<td>Allows a CS to be disabled without removing the configuration.</td>
</tr>
</tbody>
</table>
default (ca-trustpoint)

To reset the value of a ca-trustpoint configuration subcommand to its default, use the default command in ca-trustpoint configuration mode.

```
default command-name
```

**Syntax Description**

| command-name | Ca-trustpoint configuration subcommand. |

**Command Default**

No default behavior or values.

**Command Modes**

Ca-trustpoint configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(8)T</td>
<td>The command mode was changed from default (ca-root) to default (ca-trustpoint) to support the crypto ca trustpoint command and all related subcommands.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>The default (ca-root) command was integrated into Cisco IOS Release 12.2(18)SXD.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>The default (ca-root) command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before you can configure this command, you must enable the crypto ca trustpoint command, which enters ca-trustpoint configuration mode.

Use this command to reset the value of a ca-trustpoint configuration mode subcommand to its default.

**Note**

The crypto ca trustpoint command deprecates the crypto ca identity and crypto ca trusted-root commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

**Examples**

The following example shows how to remove the crl optional command from your configuration; the default of crl optional is off.

```
default crl optional
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ca trustpoint</td>
<td>Declares the CA that your router should use.</td>
</tr>
</tbody>
</table>
default (ca-trustpool)

To reset the value of a ca-trustpool configuration command to its default in the public key infrastructure (PKI) trustpool, use the `default` command in ca-trustpool configuration mode.

```
default command-name
```

**Command Modes**

Ca-trustpool configuration (ca-trustpool)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(1)SY</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)SY.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before you can configure this command, you must enable the `crypto pki trustpool policy` command, which enters ca-trustpool configuration mode.

**Examples**

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# default crl query
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cabundle url</td>
<td>Configures the URL from which the PKI trustpool CA bundle is downloaded.</td>
</tr>
<tr>
<td>chain-validation</td>
<td>Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool.</td>
</tr>
<tr>
<td>crl</td>
<td>Specifies the CRL query and cache options for the PKI trustpool.</td>
</tr>
<tr>
<td>crypto pki trustpool import</td>
<td>Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle.</td>
</tr>
<tr>
<td>crypto pki trustpool policy</td>
<td>Configures PKI trustpool policy parameters.</td>
</tr>
<tr>
<td>match</td>
<td>Enables the use of certificate maps for the PKI trustpool.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ocspr</td>
<td>Specifies OCSP settings for the PKI trustpool.</td>
</tr>
<tr>
<td>revocation-check</td>
<td>Disables revocation checking when the PKI trustpool policy is being used.</td>
</tr>
<tr>
<td>show</td>
<td>Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.</td>
</tr>
<tr>
<td>show crypto pki trustpool</td>
<td>Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy.</td>
</tr>
<tr>
<td>source interface</td>
<td>Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.</td>
</tr>
<tr>
<td>storage</td>
<td>Specifies a file system location where PKI trustpool certificates are stored on the router.</td>
</tr>
<tr>
<td>vrf</td>
<td>Specifies the VRF instance to be used for CRL retrieval.</td>
</tr>
</tbody>
</table>
default-group-policy

To associate a policy group with a SSL VPN context configuration, use the `default-group-policy` command in webvpn context configuration mode. To remove the policy group from the webvpn context configuration, use the `no` form of this command.

```
default-group-policy name
no default-group-policy
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>name</code></td>
<td>Name of the policy configured with the <code>policy group</code> command.</td>
</tr>
</tbody>
</table>

**Command Default**

A policy group is not associated with a SSL VPN context configuration.

**Command Modes**

Webvpn context configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `policy group` command is first configured to define policy group configuration parameters. This command is configured to attach the policy group to the SSL VPN context when multiple policy groups are defined under the context. This policy will be used as the default unless an authentication, authorization, and accounting (AAA) server pushes an attribute that specifically requests another group policy.

**Examples**

The following example configures policy group ONE as the default policy group:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy-group ONE
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# policy-group TWO
Router(config-webvpn-group)# exit
Router(config-webvpn-context)# default-group-policy ONE
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>policy group</code></td>
<td>Enters webvpn group policy configuration mode to configure a policy group.</td>
</tr>
<tr>
<td><code>webvpn context</code></td>
<td>Enters webvpn context configuration mode to configure the SSL VPN context.</td>
</tr>
</tbody>
</table>
deny

To set conditions in a named IP access list or object group access control list (OGACL) that will deny packets, use the `deny` configuration command in the appropriate configuration mode. To remove a deny condition from an IP access list or OGACL, use the `no` form of this command.

```
deny protocol {src-addr src-wildcard|object-group object-group-name|any|host {addrname}} {dest-addr dest-wildcard|any|eq port|gt port|lt port|neq port|portgroup srcport-groupname|object-group dest-addr-groupname|range port[[ {dscp type|fragments|option option|precedence precedence|log|log-input|time-range time-range-name|tos|tos|ttl|ttl-value}]]}
```

This command takes the following parameters:

- **protocol**
  - Name or number of a protocol; valid values are `eigrp`, `gre`, `icmp`, `igmp`, `igrp`, `ip`, `ipinip`, `ospf`, `tcp`, or `udp`, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword `ip`. See the “Usage Guidelines” section for additional qualifiers.

- **src-addr**
  - Number of the source network or host from which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.

- **src-wildcard**
  -Wildcard bits to be applied to source network in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.

- **object-group object-group-name**
  - Specifies the source or destination name of the object group.

- **any**
  - Specifies any source or any destination host as an abbreviation for the `source-addr` or `destination-addr` value and the `source-wildcard` or `destination-wildcard` value of 0.0.0.0 to 255.255.255.255.

- **host addr**
  - Specifies the source or destination address of a single host.

- **host name**
  - Specifies the source or destination name of a single host.

- **tcp**
  - Specifies the TCP protocol.

- **udp**
  - Specifies the UDP protocol.

- **object-group source-addr-group-name**
  - Specifies the source address group name.

- **destination-addr**
  - Number of the network or host to which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.

- **destination-wildcard**
  - Wildcard bits to be applied to the destination in a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>protocol</strong></td>
<td>Name or number of a protocol; valid values are <code>eigrp</code>, <code>gre</code>, <code>icmp</code>, <code>igmp</code>, <code>igrp</code>, <code>ip</code>, <code>ipinip</code>, <code>ospf</code>, <code>tcp</code>, or <code>udp</code>, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword <code>ip</code>. See the “Usage Guidelines” section for additional qualifiers.</td>
</tr>
<tr>
<td><strong>src-addr</strong></td>
<td>Number of the source network or host from which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.</td>
</tr>
<tr>
<td><strong>src-wildcard</strong></td>
<td>Wildcard bits to be applied to source network in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.</td>
</tr>
<tr>
<td><strong>object-group</strong></td>
<td>Specifies the source or destination name of the object group.</td>
</tr>
<tr>
<td><strong>any</strong></td>
<td>Specifies any source or any destination host as an abbreviation for the <code>source-addr</code> or <code>destination-addr</code> value and the <code>source-wildcard</code> or <code>destination-wildcard</code> value of 0.0.0.0 to 255.255.255.255.</td>
</tr>
<tr>
<td><strong>host addr</strong></td>
<td>Specifies the source or destination address of a single host.</td>
</tr>
<tr>
<td><strong>host name</strong></td>
<td>Specifies the source or destination name of a single host.</td>
</tr>
<tr>
<td><strong>tcp</strong></td>
<td>Specifies the TCP protocol.</td>
</tr>
<tr>
<td><strong>udp</strong></td>
<td>Specifies the UDP protocol.</td>
</tr>
<tr>
<td><strong>object-group</strong></td>
<td>Specifies the source address group name.</td>
</tr>
<tr>
<td><strong>destination-addr</strong></td>
<td>Number of the network or host to which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.</td>
</tr>
<tr>
<td><strong>destination-wildcard</strong></td>
<td>Wildcard bits to be applied to the destination in a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.</td>
</tr>
<tr>
<td><strong>eq</strong></td>
<td>port</td>
</tr>
<tr>
<td><strong>gt</strong></td>
<td>port</td>
</tr>
<tr>
<td><strong>lt</strong></td>
<td>port</td>
</tr>
<tr>
<td><strong>neq</strong></td>
<td>port</td>
</tr>
<tr>
<td><strong>portgroup</strong></td>
<td></td>
</tr>
<tr>
<td><strong>srcport-group-name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>object-group</strong></td>
<td></td>
</tr>
<tr>
<td><strong>dest-addr-group-name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>portgroup</strong></td>
<td></td>
</tr>
<tr>
<td><strong>destport-group-name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>dscp</strong></td>
<td></td>
</tr>
<tr>
<td><strong>type</strong></td>
<td></td>
</tr>
<tr>
<td><strong>fragments</strong></td>
<td></td>
</tr>
<tr>
<td><strong>option</strong></td>
<td></td>
</tr>
<tr>
<td><strong>option</strong></td>
<td></td>
</tr>
<tr>
<td><strong>precedence</strong></td>
<td></td>
</tr>
<tr>
<td><strong>precedence</strong></td>
<td></td>
</tr>
</tbody>
</table>
Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the `logging console` command.)

The message for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets.

The message for an extended list includes the access list number; whether the packet was permitted or denied; the protocol; whether the protocol was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers.

For both standard and extended lists, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.

The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from reloading because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

<table>
<thead>
<tr>
<th>log</th>
<th>(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the <code>logging console</code> command.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>log-input</td>
<td>(Optional) Matches the log against this entry, including the input interface.</td>
</tr>
<tr>
<td>time-range</td>
<td>(Optional) Specifies a time-range entry name.</td>
</tr>
<tr>
<td>time-range-name</td>
<td>(Optional) Specifies the service filtering level for packets; valid values are a number from 0 to 15 or by a name as listed in the “Usage Guidelines” section of the <code>access-list(IP extended)</code> command.</td>
</tr>
<tr>
<td>tos tos</td>
<td>(Optional) Matches packets with the IP options value; see the “Usage Guidelines” section for the valid values.</td>
</tr>
<tr>
<td>option option</td>
<td>(Optional) Matches packets with the IP options value; see the “Usage Guidelines” section for the valid values.</td>
</tr>
<tr>
<td>fragments</td>
<td>(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the <code>fragments</code> keyword, see the “Usage Guidelines” section.</td>
</tr>
<tr>
<td>ttl ttl-value</td>
<td>(Optional) Matches packets with a given Time-to-live (ttl) value.</td>
</tr>
</tbody>
</table>

**Command Default**

There is no specific condition under which a packet is denied passing the access list.

**Command Modes**

Standard access-list configuration (config-std-nacl)
Extended access-list configuration (config-ext-nacl)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command following the `ip access-list` command to specify conditions under which a packet cannot pass the access list.

The `portgroup` keyword appears only when you configure an extended ACL.
The *address or object-group-name* value is created using the *object-group* command.

The *object-group object-group-name* keyword and argument allow you to create logical groups of users (or servers), which you can use to define access policy using ACLs. For example, with one ACL entry you can permit the object group named engineering to access all engineering servers. Otherwise, you would need one ACL entry for every person in the engineering group.

If the operator is positioned after the *source-addr* and *source-wildcard* values, it must match the source port.

If the operator is positioned after the *destination-addr* and *destination-wildcard* values, it must match the destination port.

If you are entering the port number of a TCP or UDP port, you can enter the decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the “Usage Guidelines” section of the *access-list* (IP extended) command. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.

The valid values for the *dscp type* keyword and argument are as follows:

- 0 to 63—Differentiated services code point value.
- *af11*—Matches packets with AF11 dscp (001010).
- *af12*—Matches packets with AF12 dscp (001100).
- *af13*—Matches packets with AF13 dscp (001110).
- *af21*—Matches packets with AF21 dscp (010010).
- *af22*—Matches packets with AF22 dscp (010100).
- *af23*—Matches the packets with the AF23 dscp (010110).
- *af31*—Matches the packets with the AF31 dscp (011010).
- *af32*—Matches the packets with the AF32 dscp (011100).
- *af33*—Matches the packets with the AF33 dscp (011110).
- *af41*—Matches the packets with the AF41 dscp (100010).
- *af42*—Matches the packets with the AF42 dscp (100100).
- *af43*—Matches the packets with the AF43 dscp (100110).
- *cs1*—Matches the packets with the CS1 (precedence 1) dscp (001000).
- *cs2*—Matches the packets with the CS2 (precedence 2) dscp (010000).
- *cs3*—Matches the packets with the CS3 (precedence 3) dscp (011000).
- *cs4*—Matches the packets with the CS4 (precedence 4) dscp (100000).
- *cs5*—Matches the packets with the CS5 (precedence 5) dscp (101000).
- *cs6*—Matches the packets with the CS6 (precedence 6) dscp (110000).
- *cs7*—Matches the packets with the CS7 (precedence 7) dscp (111000).
- *default*—Matches the packets with the default dscp (000000).
- *ef*—Matches the packets with the EF dscp (101110).
The valid values for the eq port keyword and argument are as follows:

- 0 to 65535 -- Port number.
- bgp -- Border Gateway Protocol (179).
- chargen -- Character generator (19).
- cmd -- Remote commands (rcmd, 514).
- daytime -- Daytime (13).
- discard -- Discard (9).
- domain -- Domain Name Service (53).
- echo -- Echo (7).
- exec -- Exec (rsh, 512).
- finger -- Finger (79).
- ftp -- File Transfer Protocol (21).
- ftp-data -- FTP data connections (20).
- gopher -- Gopher (70).
- hostname -- NIC hostname server (101).
- ident -- Ident Protocol (113).
- irc -- Internet Relay Chat (194).
- klogin -- Kerberos login (543).
- kshell -- Kerberos shell (544).
- login -- Login (rlogin, 513).
- lpd -- Printer service (515).
- pim-auto-rp -- PIM Auto-RP (496).
- pop3 -- Post Office Protocol v3 (110).
- smtp -- Simple Mail Transport Protocol (25).
- sunrpc -- Sun Remote Procedure Call (111).
- syslog -- Syslog (514).
- tacacs -- TAC Access Control System (49).
- talk -- Talk (517).
- telnet -- Telnet (23).
- time -- Time (37).
• **uucp** --Unix-to-Unix Copy Program (540).
• **whois** --Nicname (43).
• **www** --World Wide Web (HTTP, 80).

The valid values for the **gt port** keyword and argument are as follows:
• **0-65535**--Port number.
• **biff**--Biff (mail notification, comsat, 512).
• **bootpc**--Bootstrap Protocol (BOOTP) client (68).
• **bootps**--Bootstrap Protocol (BOOTP) server (67).
• **discard**--Discard (9).
• **dnsix**--DNSIX security protocol auditing (195).
• **domain**--Domain Name Service (DNS, 53).
• **echo**--Echo (7).
• **isakmp**--Internet Security Association and Key Management Protocol (500).
• **mobile-ip**--Mobile IP registration (434).
• **nameserver**--IEN116 name service (obsolete, 42).
• **netbios-dgm**--NetBios datagram service (138).
• **netbios-ns**--NetBios name service (137).
• **netbios-ss**--NetBios session service (139).
• **non500-isakmp**--Internet Security Association and Key Management Protocol (4500).
• **ntp**--Network Time Protocol (123).
• **pim-auto-rp**--PIM Auto-RP (496).
• **rip**--Routing Information Protocol (router, in.routed, 520).
• **snmp**--Simple Network Management Protocol (161).
• **snmptrap**--SNMP Traps (162).
• **sunrpc**--Sun Remote Procedure Call (111).
• **syslog**--System Logger (514).
• **tacacs**--TAC Access Control System (49).
• **talk**--Talk (517).
• **tftp**--Trivial File Transfer Protocol (69).
• **time**--Time (37).
• **who**--Who service (rwho, 513).
• **xdmcp**--X Display Manager Control Protocol (177).
The valid values for the **lt** `port` keyword and argument are as follows:

- 0-65535--Port number.
- `biff`--Biff (mail notification, comsat, 512).
- `bootpc`--Bootstrap Protocol (BOOTP) client (68).
- `bootps`--Bootstrap Protocol (BOOTP) server (67).
- `discard`--Discard (9).
- `dnsix`--DNSIX security protocol auditing (195).
- `domain`--Domain Name Service (DNS, 53).
- `echo`--Echo (7).
- `isakmp`--Internet Security Association and Key Management Protocol (500).
- `mobile-ip`--Mobile IP registration (434).
- `nameserver`--IEN116 name service (obsolete, 42).
- `netbios-dgm`--NetBios datagram service (138).
- `netbios-ns`--NetBios name service (137).
- `netbios-ss`--NetBios session service (139).
- `non500-isakmp`--Internet Security Association and Key Management Protocol (4500).
- `ntp`--Network Time Protocol (123).
- `pim-auto-rp`--PIM Auto-RP (496).
- `rip`--Routing Information Protocol (router, in.routed, 520).
- `snmptrap`--SNMP Traps (162).
- `sunrpc`--Sun Remote Procedure Call (111).
- `syslog`--System Logger (514).
- `tacacs`--TAC Access Control System (49).
- `talk`--Talk (517).
- `tftp`--Trivial File Transfer Protocol (69).
- `time`--Time (37).
- `who`--Who service (rwho, 513).
- `xdmcp`--X Display Manager Control Protocol (177).

The valid values for the **neg** `port` keyword and argument are as follows:

- 0 to 65535--Port number.
• biff --Biff (mail notification, comsat, 512).
• bootpc --Bootstrap Protocol (BOOTP) client (68).
• bootps --Bootstrap Protocol (BOOTP) server (67).
• discard --Discard (9).
• dnsix --DNSIX security protocol auditing (195).
• domain --Domain Name Service (DNS, 53).
• echo --Echo (7).
• isakmp --Internet Security Association and Key Management Protocol (500).
• mobile-ip --Mobile IP registration (434).
• nameserver --IEN116 name service (obsolete, 42).
• netbios-dgm --NetBios datagram service (138).
• netbios-ns --NetBios name service (137).
• netbios-ss --NetBios session service (139).
• non500-isakmp --Internet Security Association and Key Management Protocol (4500).
• ntp --Network Time Protocol (123).
• pim-auto-rp --PIM Auto-RP (496).
• rip --Routing Information Protocol (router, in.routed, 520).
• snmp --Simple Network Management Protocol (161).
• snmptrap --SNMP Traps (162).
• sunrpc --Sun Remote Procedure Call (111).
• syslog --System Logger (514).
• tacacs --TAC Access Control System (49).
• talk --Talk (517).
• tftp --Trivial File Transfer Protocol (69).
• time --Time (37).
• who --Who service (rwho, 513).
• xdmcp --X Display Manager Control Protocol (177).

The valid values for the option option keyword and argument are as follows:
• 0 to 255--IP Options value.
• add-ext --Matches the packets with Address Extension Option (147).
• any-options --Matches the packets with ANY Option.
• com-security --Matches the packets with Commercial Security Option (134).
• dps --Matches the packets with Dynamic Packet State Option (151).
• encode --Matches the packets with Encode Option (15).
• cool --Matches the packets with End of Options (0).
• ext-ip --Matches the packets with the Extended IP Option (145).
• ext-security --Matches the packets with the Extended Security Option (133).
• finn --Matches the packets with the Experimental Flow Control Option (205).
  • imitd--Matches the packets with IMI Traffic Desriptor Option (144).
  • lsr--Matches the packets with Loose Source Route Option (131).
  • match-all--Matches the packets if all specified flags are present.
  • match-any--Matches the packets if any specified flag is present.
  • mtup--Matches the packets with MTU Probe Option (11).
  • mtur--Matches the packets with MTU Reply Option (12).
  • no-op--Matches the packets with No Operation Option (1).
  • psh--Match the packets on the PSH bit.
• nsapa--Matches the packets with NSAP Addresses Option (150).
• reflect--Creates reflexive access list entry.
• record-route--Matches the packets with Record Route Option (7).
• rst--Matches the packets on the RST bit.
• router-alert--Matches the packets with Router Alert Option (148).
• sdb--Matches the packets with Selective Directed Broadcast Option (149).
• security--Matches the packets with Basic Security Option (130).
• ssr--Matches the packets with Strict Source Routing Option (137).
• stream-id--Matches the packets with Stream ID Option (136).
• syn--Match the packets on the SYN bit.
• timestamp --Matches the packets with the Time Stamp Option (68).
• traceroute --Matches the packets with the Trace Route Option (82).
• ump --Matches the packets with the Upstream Multicast Packet Option (152).
• visa --Matches the packets with the Experimental Access Control Option (142).
• zu --Matches the packets with the Experimental Measurement Option (10).

The valid values for the tos value keyword and argument are as follows:
• 0 to 15--Type of service value.
• max-reliability --Matches the packets with the maximum reliable ToS (2).
• max-throughput --Matches the packets with the maximum throughput ToS (4).
• min-delay --Matches the packets with the minimum delay ToS (8).
• min-monetary-cost --Matches packets with the minimum monetary cost ToS (1).
• normal --Matches the packets with the normal ToS (0).
Access List or OGACL Processing of Fragments

The behavior of access-list entries regarding the use or lack of the fragments keyword are summarized in the table below:

Table 1: Access list or OGACL Processing of Fragments

<table>
<thead>
<tr>
<th>If the Access-List Entry Has...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>...no fragments keyword (the default behavior), and assuming all of the access-list entry information matches,</td>
<td>For an access-list entry containing only Layer 3 information:</td>
</tr>
<tr>
<td></td>
<td>• The entry is applied to nonfragmented packets, initial fragments, and noninitial fragments.</td>
</tr>
<tr>
<td></td>
<td>For an access list entry containing Layer 3 and Layer 4 information:</td>
</tr>
<tr>
<td></td>
<td>• The entry is applied to nonfragmented packets and initial fragments:</td>
</tr>
<tr>
<td></td>
<td>• If the entry is a permit statement, the packet or fragment is permitted.</td>
</tr>
<tr>
<td></td>
<td>• If the entry is a deny statement, the packet or fragment is denied.</td>
</tr>
<tr>
<td></td>
<td>• The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and</td>
</tr>
<tr>
<td></td>
<td>• If the entry is a permit statement, the noninitial fragment is permitted.</td>
</tr>
<tr>
<td></td>
<td>• If the entry is a deny statement, the next access-list entry is processed.</td>
</tr>
<tr>
<td>Note</td>
<td>The deny statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.</td>
</tr>
<tr>
<td></td>
<td>The access-list entry is applied only to noninitial fragments. The fragments keyword cannot be configured for an access-list entry that contains any Layer 4 information.</td>
</tr>
</tbody>
</table>

Be aware that you should not simply add the fragments keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list permit or deny entry that contains the fragments keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the fragments keyword. Therefore, you may need two access list entries for every deny entry. The first deny entry of the pair will not include the fragments keyword, and applies to the initial fragment. The second deny entry of the pair will include the fragments keyword and applies to the subsequent fragments. In the cases where there are multiple deny access-list entries for the same host but with different Layer 4 ports, a single deny access-list entry with the fragments keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.
The `fragments` keyword cannot solve all cases involving access lists and IP fragments.

**Fragments and Policy Routing**

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the `match ip address` command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the `fragments` keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

The `portgroup srcport-groupname` or `portgroup destport-groupname` keywords and arguments allow you to create an object group based on a source or destination group.

**Examples**

The following example creates an access list that denies all TCP packets:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended my_ogacl_policy
Router(config-ext-nacl)# deny tcp any any
Router(config-ext-nacl)# exit
Router(config)# exit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip access-group</code></td>
<td>Applies an ACL or OGACL to an interface or a service policy map.</td>
</tr>
<tr>
<td><code>ip access-list</code></td>
<td>Defines an IP access list or OGACL by name or number.</td>
</tr>
<tr>
<td><code>object-group network</code></td>
<td>Defines network object groups for use in OGACLs.</td>
</tr>
<tr>
<td><code>object-group service</code></td>
<td>Defines service object groups for use in OGACLs.</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>Sets conditions in a named IP access list or OGACL that will permit packets.</td>
</tr>
<tr>
<td><code>show ip access-list</code></td>
<td>Displays the contents of IP access lists or OGACLs.</td>
</tr>
<tr>
<td><code>show object-group</code></td>
<td>Displays information about object groups that are configured.</td>
</tr>
</tbody>
</table>
deny (Catalyst 6500 series switches)

To set conditions for a named access list, use the `deny` configuration command in access-list configuration mode. To remove a deny condition from an access list, use the `no` form of this command.

`deny protocol {src-addr src-wildcard | object-group object-group-name | any | host {addrname}} {dest-addr dest-wildcard | any | host {addrname}} {eq port | gt port | lt port | neq port | portgroup srcport-groupname | object-group dest-addr-groupname | range port} [{dscp type | fragments | option | precedence precedence | log | log-input | time-range time-range-name | tos tos | ttl ttl-value}]

`nodeny protocol {src-addr src-wildcard | object-group object-group-name | any | host {addrname}} {dest-addr dest-wildcard | any | host {addrname}} {eq port | gt port | lt port | neq port | portgroup srcport-groupname | object-group dest-addr-groupname | range port} [{dscp type | fragments | option | precedence precedence | log | log-input | time-range time-range-name | tos tos | ttl ttl-value}]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>protocol</code></td>
<td>Name or number of a protocol; valid values are <code>eigrp</code>, <code>gre</code>, <code>icmp</code>, <code>igmp</code>, <code>igrp</code>, <code>ip</code>, <code>ipinip</code>, <code>nos</code>, <code>ospf</code>, <code>tcp</code>, or <code>udp</code>, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword <code>ip</code>. See the “Usage Guidelines” section for additional qualifiers.</td>
</tr>
<tr>
<td><code>src-addr</code></td>
<td>Number of the source network or host from which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.</td>
</tr>
<tr>
<td><code>src-wildcard</code></td>
<td>Wildcard bits to be applied to source network in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.</td>
</tr>
<tr>
<td><code>object-group</code></td>
<td>Specifies the source or destination name of the object group.</td>
</tr>
<tr>
<td><code>object-group-name</code></td>
<td>Specifies any source or any destination host as an abbreviation for the source-addr or destination-addr valueand the source-wildcard or destination-wildcard value of 0.0.0.0 255.255.255.255.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>Specifies any source or destination address of a single host.</td>
</tr>
<tr>
<td><code>host addr</code></td>
<td>Specifies the source or destination address of a single host.</td>
</tr>
<tr>
<td><code>host name</code></td>
<td>Specifies the source or destination name of a single host.</td>
</tr>
<tr>
<td><code>tcp</code></td>
<td>Specifies the TCP protocol.</td>
</tr>
<tr>
<td><code>udp</code></td>
<td>Specifies the UDP protocol.</td>
</tr>
<tr>
<td><code>source-addr-group-name</code></td>
<td>Specifies the source address group name.</td>
</tr>
<tr>
<td><code>destination-addr</code></td>
<td>Number of the network or host to which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.</td>
</tr>
<tr>
<td><code>destination-wildcard</code></td>
<td>Wildcard bits to be applied to the destination in a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.</td>
</tr>
<tr>
<td><code>eq port</code></td>
<td>Matches only packets on a given port number; see the “Usage Guidelines” section for valid values.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>gt port</td>
<td>Matches only the packets with a greater port number; see the “Usage Guidelines” section for valid values.</td>
</tr>
<tr>
<td>lt port</td>
<td>Matches only the packets with a lower port number; see the “Usage Guidelines” section for valid values.</td>
</tr>
<tr>
<td>neq port</td>
<td>Matches only the packets that are not on a given port number; see the “Usage Guidelines” section for valid values.</td>
</tr>
<tr>
<td>portgroup srcport-group-name</td>
<td>Specifies the source port object group name.</td>
</tr>
<tr>
<td>object-group dest-addr-group-name</td>
<td>Specifies the destination address group name.</td>
</tr>
<tr>
<td>portgroup destport-group-name</td>
<td>Specifies the destination port object group name.</td>
</tr>
<tr>
<td>dscp type</td>
<td>(Optional) Matches the packets with the given Differentiated Services Code Point (DSCP) value; see the “Usage Guidelines” section for valid values.</td>
</tr>
<tr>
<td>fragments</td>
<td>(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the fragments keyword, see the “Access List Processing of Fragments” and “deny, on page 32” sections in the “Usage Guidelines” section.</td>
</tr>
<tr>
<td>option option</td>
<td>(Optional) Matches the packets with the given IP options value number; see the “Usage Guidelines” section for valid values.</td>
</tr>
<tr>
<td>precedence precedence</td>
<td>(Optional) Specifies the precedence filtering level for packets; valid values are a number from 0 to 7 or by a name. See the “Usage Guidelines” section for a list of valid names.</td>
</tr>
<tr>
<td>log</td>
<td>(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the logging console command.) The message for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message for an extended list includes the access list number, whether the packet was permitted or denied; the protocol; whether the protocol was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. For both standard and extended lists, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from reloading because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.</td>
</tr>
<tr>
<td>log-input</td>
<td>(Optional) Matches the log against this entry, including the input interface.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
| **time-range**
| **time-range-name** | (Optional) Specifies a time-range entry name. |
| **tos**
| **tos** | (Optional) Specifies the service filtering level for packets; valid values are a number from 0 to 15 or by a name as listed in the “Usage Guidelines” section of the `access-list(IP extended)` command. |
| **option**
| **option** | (Optional) Matches packets with the IP options value; see the “Usage Guidelines” section for the valid values. |
| **fragments** | (Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the `fragments` keyword, see the `deny, on page 32` and “deny, on page 32” sections in the “Usage Guidelines” section. |
| **ttl**
| **ttl-value** | (Optional) Matches packets with a given Time-to-live (ttl) value. |

**Command Default**
There is no specific condition under which a packet is denied passing the named access list.

**Command Modes**
Access-list configuration (config-ext-nacl)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXH</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command following the `ip access-list` command to specify conditions under which a packet cannot pass the named access list.

The `portgroup` keyword appears only when you configure an extended ACL.

The `address` or `object-group-name` value is created using the `object-group` command.

The `addrgroup object-group-name` keyword and argument allow you to create logical groups of users (or servers), which you can use to define access policy using ACLs. For example, with one ACL entry you can permit the object group named engineering to access all engineering servers. Otherwise, you would need one ACL entry for every person in the engineering group.

If the operator is positioned after the `source-addr` and `source-wildcard` values, it must match the source port.

If the operator is positioned after the `destination-addr` and `destination-wildcard` values, it must match the destination port.

If you are entering the port number of a TCP or UDP port, you can enter the decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the “Usage Guidelines” section of the `access-list(IP extended)` command. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.

The valid values for the `dscp` type keyword and argument are as follows:

- 0 to 63--Differentiated services code point value.
- `af11` --Match packets with AF11 dscp (001010).
- `af12` --Match packets with AF12 dscp (001100).
• af13 --Match packets with AF13 dscp (001110).
• af21 --Match packets with AF21 dscp (010010).
• af22 --Match packets with AF22 dscp (010100).
• af23 --Matches the patches with the AF23 dscp (010110).
• af31 --Matches the patches with the AF31 dscp (011010).
• af32 --Matches the patches with the AF32 dscp (011100).
• af33 --Matches the patches with the AF33 dscp (011110).
• af41 --Matches the patches with the AF41 dscp (100010).
• af42 --Matches the patches with the AF42 dscp (100100).
• af43 --Matches the patches with the AF43 dscp (100110).
• cs1 --Matches the patches with the CS1(precedence 1) dscp (001000).
• cs2 --Matches the patches with the CS2(precedence 2) dscp (010000).
• cs3 --Matches the patches with the CS3(precedence 3) dscp (011000).
• cs4 --Matches the patches with the CS4(precedence 4) dscp (100000).
• cs5 --Matches the patches with the CS5(precedence 5) dscp (101000).
• cs6 --Matches the patches with the CS6(precedence 6) dscp (110000).
• cs7 --Matches the patches with the CS7(precedence 7) dscp (111000).
• default --Matches the patches with the default dscp (000000).
• ef --Matches the patches with the EF dscp (101110).

The valid values for the eq port keyword and argument are as follows:

• 0 to 65535--Port number.
• bgp --Border Gateway Protocol (179).
• chargen --Character generator (19).
• cmd --Remote commands (rcmd, 514).
• daytime --Daytime (13).
• discard --Discard (9).
• domain --Domain Name Service (53).
• echo --Echo (7).
• exec --Exec (rsh, 512).
• finger --Finger (79).
• ftp --File Transfer Protocol (21).
- **ftp-data** -- FTP data connections (20).
- **gopher** -- Gopher (70).
- **hostname** -- NIC hostname server (101).
- **ident** -- Ident Protocol (113).
- **irc** -- Internet Relay Chat (194).
- **klogin** -- Kerberos login (543).
- **kshell** -- Kerberos shell (544).
- **login** -- Login (rlogin, 513).
- **lpd** -- Printer service (515).
- **nntp** -- Network News Transport Protocol (119).
- **pim-auto-rp** -- PIM Auto-RP (496).
- **pop2** -- Post Office Protocol v2 (109).
- **pop3** -- Post Office Protocol v3 (110).
- **smtp** -- Simple Mail Transport Protocol (25).
- **sunrpe** -- Sun Remote Procedure Call (111).
- **syslog** -- Syslog (514).
- **tacacs** -- TAC Access Control System (49).
- **talk** -- Talk (517).
- **telnet** -- Telnet (23).
- **time** -- Time (37).
- **uucp** -- Unix-to-Unix Copy Program (540).
- **whois** -- Nisname (43).
- **www** -- World Wide Web (HTTP, 80).

The valid values for the `gt port` keyword and argument are as follows:

- **0-65535** -- Port number.
- **biff** -- Biff (mail notification, comsat, 512).
- **bootpc** -- Bootstrap Protocol (BOOTP) client (68).
- **bootps** -- Bootstrap Protocol (BOOTP) server (67).
- **discard** -- Discard (9).
- **dnsix** -- DNSIX security protocol auditing (195).
- **domain** -- Domain Name Service (DNS, 53).
• echo --Echo (7).
• isakmp --Internet Security Association and Key Management Protocol (500).
• mobile-ip --Mobile IP registration (434).
• nameserver --IEN116 name service (obsolete, 42).
• netbios-dgm --NetBios datagram service (138).
• netbios-ns --NetBios name service (137).
• netbios-ss --NetBios session service (139).
• non500-isakmp --Internet Security Association and Key Management Protocol (4500).
• ntp --Network Time Protocol (123).
• pim-auto-rp --PIM Auto-RP (496).
• rip --Routing Information Protocol (router, in.routed, 520).
• snmp --Simple Network Management Protocol (161).
• snmptrap --SNMP Traps (162).
• sunrpc--Sun Remote Procedure Call (111).
• syslog --System Logger (514).
• tacacs --TAC Access Control System (49).
• talk --Talk (517).
• tftp --Trivial File Transfer Protocol (69).
• time --Time (37).
• who --Who service (rwho, 513).
• xdmcp --X Display Manager Control Protocol (177).

The valid values for the **port** keyword and argument are as follows:
• 0-65535--Port number.
• biff --Biff (mail notification, comsat, 512).
• bootpc --Bootstrap Protocol (BOOTP) client (68).
• bootps --Bootstrap Protocol (BOOTP) server (67).
• discard --Discard (9).
• dnsix --DNSIX security protocol auditing (195).
• domain --Domain Name Service (DNS, 53).
• echo --Echo (7).
• isakmp --Internet Security Association and Key Management Protocol (500).
• mobile-ip --Mobile IP registration (434).
• nameserver --IEN116 name service (obsolete, 42).
• netbios-dgm --NetBios datagram service (138).
• netbios-ns --NetBios name service (137).
• netbios-ss --NetBios session service (139).
• non500-isakmp --Internet Security Association and Key Management Protocol (4500).
• ntp --Network Time Protocol (123).
• pim-auto-rp --PIM Auto-RP (496).
• rip --Routing Information Protocol (router, in.routed, 520).
• snmp --Simple Network Management Protocol (161).
• snmptrap --SNMP Traps (162).
• sunrpc --Sun Remote Procedure Call (111).
• syslog --System Logger (514).
• tacacs --TAC Access Control System (49).
• talk --Talk (517).
• tftp --Trivial File Transfer Protocol (69).
• time --Time (37).
• who --Who service (rwho, 513).
• xdmcp --X Display Manager Control Protocol (177).

The valid values for the neg port keyword and argument are as follows:

• 0 to 65535--Port number.
• biff --Biff (mail notification, comsat, 512).
• bootpc --Bootstrap Protocol (BOOTP) client (68).
• bootps --Bootstrap Protocol (BOOTP) server (67).
• discard --Discard (9).
• dnsix --DNSIX security protocol auditing (195).
• domain --Domain Name Service (DNS, 53).
• echo --Echo (7).
• isakmp --Internet Security Association and Key Management Protocol (500).
• mobile-ip --Mobile IP registration (434).
• nameserver --IEN116 name service (obsolete, 42).
• netbios-dgm --NetBios datagram service (138).
- **netbios-ns** -- NetBios name service (137).
- **netbios-ss** -- NetBios session service (139).
- **non500-isakmp** -- Internet Security Association and Key Management Protoc (4500).
- **ntp** -- Network Time Protocol (123).
- **pim-auto-rp** -- PIM Auto-RP (496).
- **rip** -- Routing Information Protocol (router, in.routed, 520).
- **snmp** -- Simple Network Management Protocol (161).
- **snmptrap** -- SNMP Traps (162).
- **sunrpc** -- Sun Remote Procedure Call (111).
- **syslog** -- System Logger (514).
- **tacacs** -- TAC Access Control System (49).
- **talk** -- Talk (517).
- **tftp** -- Trivial File Transfer Protocol (69).
- **time** -- Time (37).
- **who** -- Who service (rwho, 513).
- **xdmcp** -- X Display Manager Control Protocol (177).

The valid values for the `option` keyword and argument are as follows:

- 0 to 255--IP Options value.
- **add-ext** -- Matches the packets with Address Extension Option (147).
- **any-options** -- Matches the packets with ANY Option.
- **com-security** -- Matches the packets with Commercial Security Option (134).
- **dps** -- Matches the packets with Dynamic Packet State Option (151).
- **encode** -- Matches the packets with Encode Option (15).
- **eool** -- Matches the packets with End of Options (0).
- **ext-ip** -- Matches the packets with the Extended IP Option (145).
- **ext-security** -- Matches the packets with the Extended Security Option (133).
- **finn** -- Matches the packets with the Experimental Flow Control Option (205).
  - **imitd** -- Matches the packets with IMI Traffic Descriptor Option (144).
  - **lsr** -- Matches the packets with Loose Source Route Option (131).
  - **match-all** -- Matches the packets if all specified flags are present.
  - **match-any** -- Matches the packets if any specified flag is present.
  - **mtup** -- Matches the packets with MTU Probe Option (11).
  - **mtur** -- Matches the packets with MTU Reply Option (12).
**no-op**--Matches the packets with No Operation Option (1).

**psh**--Match the packets on the PSH bit.

**nsapa**--Matches the packets with NSAP Addresses Option (150).

**reflect**--Creates reflexive access list entry.

**record-route**--Matches the packets with Record Route Option (7).

**rst**--Matches the packets on the RST bit.

**router-alert**--Matches the packets with Router Alert Option (148).

**sdb**--Matches the packets with Selective Directed Broadcast Option (149).

**security**--Matches the packets with Basic Security Option (130).

**ssr**--Matches the packets with Strict Source Routing Option (137).

**stream-id**--Matches the packets with Stream ID Option (136).

**syn**--Match the packets on the SYN bit.

**timestamp** --Matches the packets with the Time Stamp Option (68).

**traceroute**--Matches the packets with the Trace Route Option (82).

**ump** --Matches the packets with the Upstream Multicast Packet Option (152).

**visa** --Matches the packets with the Experimental Access Control Option (142).

**zsu** --Matches the packets with the Experimental Measurement Option (10).

The valid values for the **tos value** keyword and argument are as follows:

- 0 to 15--Type of service value.
- **max-reliability** --Matches the packets with the maximum reliable ToS (2).
- **max-throughput** --Matches the packets with the maximum throughput ToS (4).
- **min-delay** --Matches the packets with the minimum delay ToS (8).
- **min-monetary-cost** --Matches packets with the minimum monetary cost ToS (1).
- **normal** --Matches the packets with the normal ToS (0).

**Access List Processing of Fragments**

The behavior of access-list entries regarding the use or lack of the **fragments** keyword are summarized in the table below:
Table 2: Access list Processing of Fragments

<table>
<thead>
<tr>
<th>If the Access-List Entry Has...</th>
<th>Then...</th>
</tr>
</thead>
</table>
| ...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches, | For an access-list entry containing only Layer 3 information:  
  - The entry is applied to nonfragmented packets, initial fragments, and noninitial fragments.  
  For an access list entry containing Layer 3 and Layer 4 information:  
  - The entry is applied to nonfragmented packets and initial fragments:  
    - If the entry is a **permit** statement, the packet or fragment is permitted.  
    - If the entry is a **deny** statement, the packet or fragment is denied.  
  - The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and  
    - If the entry is a **permit** statement, the noninitial fragment is permitted.  
    - If the entry is a **deny** statement, the next access-list entry is processed. |
| Note | The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments. |
| ...the **fragments** keyword, and assuming all of the access-list entry information matches, | Note | The access-list entry is applied only to noninitial fragments. The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information. |

Be aware that you should not simply add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple **deny** access-list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

---

**Note**  
The **fragments** keyword cannot solve all cases involving access lists and IP fragments.

**Fragments and Policy Routing**
Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the `match ip address` command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

The `portgroup srcport-groupname or portgroup destport-groupname` keywords and arguments allow you to create an object group based on a source or destination group.

**Examples**

The following example creates an access list that denies all TCP packets:

Router(config)# `ip access-list extended my-pbacl-policy`

Router(config-ext-nacl)# `deny tcp any any`

Router(config-ext-nacl)# `exit`

Router(config)# `exit`

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ip access-group</code></td>
<td>Controls access to an interface.</td>
</tr>
<tr>
<td></td>
<td><code>ip access-list</code></td>
<td>Defines an IP access list by name.</td>
</tr>
<tr>
<td></td>
<td><code>logging console</code></td>
<td>Limits messages logged to the console based on severity.</td>
</tr>
<tr>
<td></td>
<td><code>object-group</code></td>
<td>Defines object groups to optimize your configuration</td>
</tr>
<tr>
<td></td>
<td><code>permit (Catalyst 6500 series switches)</code></td>
<td>Sets conditions for a named IP access list.</td>
</tr>
<tr>
<td></td>
<td><code>show ip access-lists</code></td>
<td>Displays the contents of all current IP access lists.</td>
</tr>
</tbody>
</table>
deny (IP)

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

```plaintext
[sequence-number] deny source [source-wildcard]
[sequence-number] deny protocol source source-wildcard destination destination-wildcard [option option-name] [precedence precedence] [tos tos] [ttl operator value] [log] [time-range time-range-name] [fragments]
no sequence-number
no deny source [source-wildcard]
no deny protocol source source-wildcard destination destination-wildcard
```

Internet Control Message Protocol (ICMP)

```plaintext
[sequence-number] deny icmp source source-wildcard destination destination-wildcard [icmp-type [icmp-code][icmp-message]] [precedence precedence] [tos tos] [ttl operator value] [log] [time-range time-range-name] [fragments]
```

Internet Group Management Protocol (IGMP)

```plaintext
[sequence-number] deny igmp source source-wildcard destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [ttl operator value] [log] [time-range time-range-name] [fragments]
```

Transmission Control Protocol (TCP)

```plaintext
[sequence-number] deny tcp source source-wildcard [operator port [port]] destination destination-wildcard [operator [port]] [[established [match-any|match-all] {+-} flag-name[precedence precedence]tos tos]ttl operator value]log] [time-range time-range-name] [fragments;}
```

User Datagram Protocol (UDP)

```plaintext
[sequence-number] deny udp source source-wildcard [operator port [port]] destination destination-wildcard [operator [port]] [precedence precedence] [tos tos] [ttl operator value] [log] [time-range time-range-name] [fragments]
```

### Syntax Description

<table>
<thead>
<tr>
<th>syntax</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sequence-number</td>
<td>(Optional) Sequence number assigned to the deny statement. The sequence number causes the system to insert the statement in that numbered position in the access list.</td>
</tr>
<tr>
<td>source</td>
<td>Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:</td>
</tr>
<tr>
<td></td>
<td>• Use a 32-bit quantity in four-part dotted-decimal format.</td>
</tr>
<tr>
<td></td>
<td>• Use the any keyword as an abbreviation for a source and source-wildcard of 0.0.0.0 255.255.255.255.</td>
</tr>
<tr>
<td></td>
<td>• Use host source as an abbreviation for a source and source-wildcard of source 0.0.0.0.</td>
</tr>
</tbody>
</table>
**source-wildcard**
Wildcard bits to be applied to the source. There are three alternative ways to specify the source wildcard:

- Use a 32-bit quantity in four-part dotted-decimal format. Place 1s in the bit positions that you want to ignore.
- Use the **any** keyword as an abbreviation for a source and source-wildcard of 0.0.0.0 255.255.255.255.
- Use **host source** as an abbreviation for a source and source-wildcard of source 0.0.0.0.

**protocol**
Name or number of an Internet protocol. The protocol argument can be one of the keywords **eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, or udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip** keyword.

**Note** When the **icmp, igmp, tcp, and udp** keywords are entered, they must be followed with the specific command syntax that is shown for the ICMP, IGMP, TCP, and UDP forms of the **deny** command.

**icmp**
Denies only ICMP packets. When you enter the **icmp** keyword, you must use the specific command syntax shown for the ICMP form of the **deny** command.

**igmp**
Denies only IGMP packets. When you enter the **igmp** keyword, you must use the specific command syntax shown for the IGMP form of the **deny** command.

**tcp**
Denies only TCP packets. When you enter the **tcp** keyword, you must use the specific command syntax shown for the TCP form of the **deny** command.

**udp**
Denies only UDP packets. When you enter the **udp** keyword, you must use the specific command syntax shown for the UDP form of the **deny** command.

**destination**
Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination:

- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the **any** keyword as an abbreviation for the destination and destination-wildcard of 0.0.0.0 255.255.255.255.
- Use **host destination** as an abbreviation for a destination and destination-wildcard of destination 0.0.0.0.

**destination-wildcard**
Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:

- Use a 32-bit quantity in four-part dotted-decimal format. Place 1s in the bit positions that you want to ignore.
- Use the **any** keyword as an abbreviation for a destination and destination-wildcard of 0.0.0.0 255.255.255.255.
- Use **host destination** as an abbreviation for a destination and destination-wildcard of destination 0.0.0.0.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>option option-name</td>
<td>(Optional) Packets can be filtered by IP Options, as specified by a number from 0 to 255 or by the corresponding IP Option name, as listed in the table in the “Usage Guidelines” section.</td>
</tr>
<tr>
<td>precedence precedence</td>
<td>(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by a name.</td>
</tr>
<tr>
<td>tos tos</td>
<td>(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by a name as listed in the “Usage Guidelines” section of the access-list (IP extended) command.</td>
</tr>
<tr>
<td>ttl operator value</td>
<td>(Optional) Compares the TTL value in the packet to the TTL value specified in this deny statement.</td>
</tr>
<tr>
<td>log</td>
<td>(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the logging console command.)</td>
</tr>
<tr>
<td>time-range time-range-name</td>
<td>(Optional) Name of the time range that applies to this deny statement. The name of the time range and its restrictions are specified by the time-range and absolute or periodic commands, respectively.</td>
</tr>
<tr>
<td>fragments</td>
<td>(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the fragments keyword, see the “Usage Guidelines” section.</td>
</tr>
<tr>
<td>icmp-type</td>
<td>(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.</td>
</tr>
<tr>
<td>icmp-code</td>
<td>(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.</td>
</tr>
<tr>
<td>icmp-message</td>
<td>(Optional) ICMP packets can be filtered by an ICMP message type name or an ICMP message type and code name. The possible names are listed in the “Usage Guidelines” section of the access-list (IP extended) command.</td>
</tr>
<tr>
<td>igmp-type</td>
<td>(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the “Usage Guidelines” section of the access-list (IP extended) command.</td>
</tr>
</tbody>
</table>
**operator**
(Optional) Compares source or destination ports. Operators include `lt` (less than), `gt` (greater than), `eq` (equal), `neq` (not equal), and `range` (inclusive range).

If the operator is positioned after the source and source-wildcard arguments, it must match the source port. If the operator is positioned after the destination and destination-wildcard arguments, it must match the destination port.

The range operator requires two port numbers. Up to ten port numbers can be entered for the `eq` (equal) and `neq` (not equal) operators. All other operators require one port number.

**port**
(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the “Usage Guidelines” section of the `access-list` (IP extended) command.

TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.

**established**
(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bit set. The nonmatching case is that of the initial TCP datagram to form a connection.

**match-any** | **match-all**
(Optional) For the TCP protocol only: A match occurs if the TCP datagram has certain TCP flags set or not set. You use the `match-any` keyword to allow a match to occur if any of the specified TCP flags are present, or you can use the `match-all` keyword to allow a match to occur only if all of the specified TCP flags are present. You must follow the `match-any` and `match-all` keywords with the `+` or `-` keywords and the `flag-name` argument to match on one or more TCP flags.

**+ | - flag-name**
(Optional) For the TCP protocol only: The `+` keyword allows IP packets if their TCP headers contain the TCP flags that are specified by the `flag-name` argument. The `-` keyword filters out IP packets that do not contain the TCP flags specified by the `flag-name` argument. You must follow the `+` and `-` keywords with the `flag-name` argument. TCP flag names can be used only when filtering TCP. Flag names for the TCP flags are as follows: `urg`, `ack`, `psh`, `rst`, `syn`, and `fin`.

---

**Command Default**
There are no specific conditions under which a packet is denied passing the named access list.

**Command Modes**
Access list configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(1)T</td>
<td>The <code>time-range</code> <code>time-range-name</code> keyword and argument were added.</td>
</tr>
<tr>
<td>12.0(11)</td>
<td>The <code>fragments</code> keyword was added.</td>
</tr>
</tbody>
</table>
The igrp keyword was removed because the IGRP protocol is no longer available in Cisco IOS software.

The sequence-number argument was added.

The sequence-number argument was added.

The option option-name keyword and argument were added. The match-any, match-all, +, and - keywords and the flag-name argument were added.

Command functionality was modified to allow up to ten port numbers to be added after the eq and neq operators so that an access list entry can be created with noncontiguous ports.

The ttl operator value keyword and arguments were added.

This command was integrated into Cisco IOS Release 12.2(27)SBC.

This command was integrated into Cisco IOS Release 12.2(33)SRA.

This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Use this command following the ip access-list command to specify conditions under which a packet cannot pass the named access list.

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

log Keyword

A log message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.

Use the ip access-list log-update command to generate logging messages when the number of matches reaches a configurable threshold (rather than waiting for a 5-minute-interval). See the ip access-list log-update command for more information.

The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

If you enable Cisco Express Forwarding (CEF) and then create an access list that uses the log keyword, the packets that match the access list are not CEF-switched. They are fast-switched. Logging disables CEF.

Access List Filtering of IP Options

Access control lists can be used to filter packets with IP Options to prevent routers from being saturated with spurious packets containing IP Options. To see a complete table of all IP Options, including ones currently not in use, refer to the latest Internet Assigned Numbers Authority (IANA) information that is available from its URL: www.iana.org.
Cisco IOS software allows you to filter packets according to whether they contain one or more of the legitimate IP Options by entering either the IP Option value or the corresponding name for the `option-name` argument as shown in the table below.

**Table 3: IP Option Values and Names**

<table>
<thead>
<tr>
<th>IP Option Value or Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to 255</td>
<td>IP Options values.</td>
</tr>
<tr>
<td>add-ext</td>
<td>Match packets with Address Extension Option (147).</td>
</tr>
<tr>
<td>any-options</td>
<td>Match packets with any IP Option.</td>
</tr>
<tr>
<td>com-security</td>
<td>Match packets with Commercial Security Option (134).</td>
</tr>
<tr>
<td>dps</td>
<td>Match packets with Dynamic Packet State Option (151).</td>
</tr>
<tr>
<td>encode</td>
<td>Match packets with Encode Option (15).</td>
</tr>
<tr>
<td>eool</td>
<td>Match packets with End of Options (0).</td>
</tr>
<tr>
<td>ext-ip</td>
<td>Match packets with Extended IP Options (145).</td>
</tr>
<tr>
<td>ext-security</td>
<td>Match packets with Extended Security Option (133).</td>
</tr>
<tr>
<td>finn</td>
<td>Match packets with Experimental Flow Control Option (205).</td>
</tr>
<tr>
<td>imitd</td>
<td>Match packets with IMI Traffic Descriptor Option (144).</td>
</tr>
<tr>
<td>lsr</td>
<td>Match packets with Loose Source Route Option (131).</td>
</tr>
<tr>
<td>mtup</td>
<td>Match packets with MTU Probe Option (11).</td>
</tr>
<tr>
<td>mtur</td>
<td>Match packets with MTU Reply Option (12).</td>
</tr>
<tr>
<td>no-op</td>
<td>Match packets with No Operation Option (1).</td>
</tr>
<tr>
<td>nsapa</td>
<td>Match packets with NSAP Addresses Option (150).</td>
</tr>
<tr>
<td>psh</td>
<td>Matches the packets on the PSH bit.</td>
</tr>
<tr>
<td>record-route</td>
<td>Match packets with Router Record Route Option (7).</td>
</tr>
<tr>
<td>reflect</td>
<td>Creates reflexive access list entry.</td>
</tr>
<tr>
<td>rst</td>
<td>Matches the packets on the RST bit.</td>
</tr>
<tr>
<td>router-alert</td>
<td>Match packets with Router Alert Option (148).</td>
</tr>
<tr>
<td>sdb</td>
<td>Match packets with Selective Directed Broadcast Option (149).</td>
</tr>
<tr>
<td>security</td>
<td>Match packets with Base Security Option (130).</td>
</tr>
<tr>
<td>ssr</td>
<td>Match packets with Strict Source Routing Option (137).</td>
</tr>
<tr>
<td>stream-id</td>
<td>Match packets with Stream ID Option (136).</td>
</tr>
</tbody>
</table>
### IP Option Value or Name | Description
---|---
syn | Matches the packets on the SYN bit.
timestamp | Match packets with Time Stamp Option (68).

**Filtering IP Packets Based on TCP Flags**

The access list entries that make up an access list can be configured to detect and drop unauthorized TCP packets by allowing only the packets that have very specific groups of TCP flags set or not set. Users can select any desired combination of TCP flags with which to filter TCP packets. Users can configure access list entries in order to allow matching on a flag that is set and on a flag that is not set. Use the + and - keywords with a flag name to specify that a match is made based on whether a TCP header flag has been set. Use the **match-any** and **match-all** keywords to allow the packet if any or all, respectively, of the flags specified by the + or - keyword and *flag-name* argument have been set or not set.

**Access List Processing of Fragments**

The behavior of access list entries regarding the use or lack of use of the **fragments** keyword can be summarized as follows:

<table>
<thead>
<tr>
<th>If the Access-List Entry Has...</th>
<th>Then...</th>
</tr>
</thead>
</table>
| ...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches, | For an access list entry that contains only Layer 3 information:  
• The entry is applied to nonfragmented packets, initial fragments, and noninitial fragments.  

For an access list entry that contains Layer 3 and Layer 4 information:  
• The entry is applied to nonfragmented packets and initial fragments.  
  • If the entry is a **permit** statement, then the packet or fragment is permitted.  
  • If the entry is a **deny** statement, then the packet or fragment is denied.  

• The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access list entry can be applied. If the Layer 3 portion of the access list entry matches, and  
  • If the entry is a **permit** statement, then the noninitial fragment is permitted.  
  • If the entry is a **deny** statement, then the next access list entry is processed.  

| Note | The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments. |

| ...the **fragments** keyword, and assuming all of the access-list entry information matches, | The access list entry is applied only to noninitial fragments. The **fragments** keyword cannot be configured for an access list entry that contains any Layer 4 information. |
Be aware that you should not add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword. The packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases in which there are multiple **deny** access list entries for the same host but with different Layer 4 ports, a single **deny** access list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets, and each counts individually as a packet in access list accounting and access list violation counts.

---

**Note**

The **fragments** keyword cannot solve all cases that involve access lists and IP fragments.

---

**Fragments and Policy Routing**

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address** command and the access list has entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy-routed, even if the first fragment is not policy-routed.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made, and it is more likely that policy routing will occur as intended.

**Creating an Access List Entry with Noncontiguous Ports**

For Cisco IOS Release 12.3(7)T and later releases, you can specify noncontiguous ports on the same access control entry, which greatly reduces the number of access list entries required for the same source address, destination address, and protocol. If you maintain large numbers of access list entries, we recommend that you consolidate them when possible by using noncontiguous ports. You can specify up to ten port numbers following the **eq** and **neq** operators.

**Examples**

The following example sets conditions for a standard access list named Internetfilter:

```bash
ip access-list standard Internetfilter
deny 192.168.34.0 0.0.0.255
permit 172.16.0.0 0.255.255.255
permit 10.0.0.0 0.255.255.255
! (Note: all other access implicitly denied.)
```

The following example denies HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m.:

```bash
time-range no-http
  periodic weekdays 8:00 to 18:00
!
ip access-list extended strict
deny tcp any any eq http time-range no-http
!
interface ethernet 0
  ip access-group strict in
```
The following example adds an entry with the sequence number 25 to extended IP access list 150:

```
ip access-list extended 150
25 deny ip host 172.16.3.3 host 192.168.5.34
```

The following example removes the entry with the sequence number 25 from the extended access list example shown above:

```
no 25
```

The following example sets a deny condition for an extended access list named filter2. The access list entry specifies that a packet cannot pass the named access list if it contains the Strict Source Routing IP Option, which is represented by the IP option value ssr.

```
ip access-list extended filter2
   deny ip any any option ssr
```

The following example sets a deny condition for an extended access list named kmdfilter1. The access list entry specifies that a packet cannot pass the named access list if the RST and FIN TCP flags have been set for that packet:

```
ip access-list extended kmdfilter1
deny tcp any any match-any +rst +fin
```

The following example shows several `deny` statements that can be consolidated into one access list entry with noncontiguous ports. The `show access-lists` command is entered to display a group of access list entries for the access list named abc.

```
Router# show access-lists abc
Extended IP access list abc
  10 deny tcp any eq telnet any eq 450 679
  20 deny tcp any eq telnet any eq 450 679
  30 deny tcp any eq ftp any eq 450 679
  40 deny tcp any eq ftp any eq 450 679
```

Because the entries are all for the same `deny` statement and simply show different ports, they can be consolidated into one new access list entry. The following example shows the removal of the redundant access list entries and the creation of a new access list entry that consolidates the previously displayed group of access list entries:

```
ip access-list extended abc
   no 10
   no 20
   no 30
   no 40
   deny tcp any eq telnet ftp any eq 450 679
```

The following examples shows the creation of the consolidated access list entry:

```
Router# show access-lists abc
Extended IP access list abc
  10 deny tcp any eq telnet ftp any eq 450 679
```

The following access list filters IP packets containing Type of Service (ToS) level 3 with TTL values 10 and 20. It also filters IP packets with a TTL greater than 154 and applies that rule to noninitial fragments. It permits IP packets with a precedence level of flash and a TTL not equal to 1, and sends log messages about such packets to the console. All other packets are denied.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>absolute</td>
<td>Specifies an absolute time when a time range is in effect.</td>
</tr>
<tr>
<td>access-list (IP extended)</td>
<td>Defines an extended IP access list.</td>
</tr>
<tr>
<td>access-list (IP standard)</td>
<td>Defines a standard IP access list.</td>
</tr>
<tr>
<td>ip access-group</td>
<td>Controls access to an interface.</td>
</tr>
<tr>
<td>ip access-list</td>
<td>Defines an IP access list by name.</td>
</tr>
<tr>
<td>ip access-list log-update</td>
<td>Sets the threshold number of packets that cause a logging message.</td>
</tr>
<tr>
<td>ip access-list resequence</td>
<td>Applies sequence numbers to the access list entries in an access list.</td>
</tr>
<tr>
<td>ip options</td>
<td>Drops or ignores IP Options packets that are sent to the router.</td>
</tr>
<tr>
<td>logging console</td>
<td>Sends system logging (syslog) messages to all available TTY lines and limits messages based on severity.</td>
</tr>
<tr>
<td>match ip address</td>
<td>Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, or performs policy routing on packets.</td>
</tr>
<tr>
<td>periodic</td>
<td>Specifies a recurring (weekly) time range for functions that support the time-range feature.</td>
</tr>
<tr>
<td>permit (IP)</td>
<td>Sets conditions under which a packet passes a named IP access list.</td>
</tr>
<tr>
<td>remark</td>
<td>Writes a helpful comment (remark) for an entry in a named IP access list.</td>
</tr>
<tr>
<td>show access-lists</td>
<td>Displays a group of access-list entries.</td>
</tr>
<tr>
<td>show ip access-list</td>
<td>Displays the contents of all current IP access lists.</td>
</tr>
<tr>
<td>time-range</td>
<td>Specifies when an access list or other feature is in effect.</td>
</tr>
</tbody>
</table>
deny (IPv6)

To set deny conditions for an IPv6 access list, use the **deny** command in IPv6 access list configuration mode. To remove the deny conditions, use the **no** form of this command.

```plaintext
deny protocol [source-ipv6-prefix/prefix-length]any[host source-ipv6-address] [operator [port-number]] [destination-ipv6-prefix/prefix-length]any[host destination-ipv6-address] [operator [port-number]] [dest-option-type [doh-numberdoh-type]] [dscp value] [flow-label value] [fragments] [hhb] [log] [log-input] [mobility] [mobility-type [mh-numbermh-type]] [routing] [routing-type routing-number] [sequence value] [time-range name] [undetermined-transport]

no deny protocol [source-ipv6-prefix/prefix-length]any[host source-ipv6-address] [operator [port-number]] [destination-ipv6-prefix/prefix-length]any[host destination-ipv6-address] [operator [port-number]] [dest-option-type [doh-numberdoh-type]] [dscp value] [flow-label value] [fragments] [hhb] [log] [log-input] [mobility] [mobility-type [mh-numbermh-type]] [routing] [routing-type routing-number] [sequence value] [time-range name] [undetermined-transport]
```

**Internet Control Message Protocol**

```plaintext
deny icmp [source-ipv6-prefix/prefix-length]any[host source-ipv6-address] [operator [port-number]] [destination-ipv6-prefix/prefix-length]any[host destination-ipv6-address] [operator [port-number]] [icmp-type [icmp-code]icmp-message] [dest-option-type [doh-numberdoh-type]] [dscp value] [flow-label value] [fragments] [hhb] [log] [log-input] [mobility] [mobility-type [mh-numbermh-type]] [routing] [routing-type routing-number] [sequence value] [time-range name]
```

**Transmission Control Protocol**

```plaintext
deny tcp [source-ipv6-prefix/prefix-length]any[host source-ipv6-address] [operator [port-number]] [destination-ipv6-prefix/prefix-length]any[host destination-ipv6-address] [operator [port-number]] [ack] [dest-option-type [doh-numberdoh-type]] [dscp value] [established] [fin] [flow-label value] [fragments] [hhb] [log] [log-input] [mobility] [mobility-type [mh-numbermh-type]] [neq] [portprotocol] [ps] [range [portprotocol]] [routing] [routing-type routing-number] [rst] [sequence value] [syn] [time-range name] [urg]
```

**User Datagram Protocol**

```plaintext
deny udp [source-ipv6-prefix/prefix-length]any[host source-ipv6-address] [operator [port-number]] [destination-ipv6-prefix/prefix-length]any[host destination-ipv6-address] [operator [port-number]] [dest-option-type [doh-numberdoh-type]] [dscp value] [flow-label value] [fragments] [hhb] [log] [log-input] [mobility] [mobility-type [mh-numbermh-type]] [neq] [portprotocol] [range [portprotocol]] [routing] [routing-type routing-number] [sequence value] [time-range name]
```

### Syntax Description

| **protocol** | Name or number of an Internet protocol. It can be one of the keywords `ahp`, `esp`, `icmp`, `ipv6`, `pcp`, `sctp`, `tcp`, `udp`, or `hhb`, or an integer in the range from 0 to 255 representing an IPv6 protocol number.
|
| **source-ipv6-prefix/prefix-length** | The source IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
|
| **any** | An abbreviation for the IPv6 prefix ::/0.
|
**host source-ipv6-address**

The source IPv6 host address about which to set deny conditions.

This `source-ipv6-address` argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

**operator [port-number]**

(Optional) Specifies an operand that compares the source or destination ports of the specified protocol. Operands are `lt` (less than), `gt` (greater than), `eq` (equal), `neq` (not equal), and `range` (inclusive range).

If the operator is positioned after the `source-ipv6-prefix/prefix-length` argument, it must match the source port.

If the operator is positioned after the `destination-ipv6-prefix/prefix-length` argument, it must match the destination port.

The `range` operator requires two port numbers. All other operators require one port number.

The optional `port-number` argument is a decimal number or the name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.

**destination-ipv6-prefix/prefix-length**

The destination IPv6 network or class of networks about which to set deny conditions.

This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

**host destination-ipv6-address**

The destination IPv6 host address about which to set deny conditions.

This `destination-ipv6-address` argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

**auth**

Allows matching traffic against the presence of the authentication header in combination with any protocol.

**dest-option-type**

(Optional) Matches IPv6 packets against the hop-by-hop option extension header within each IPv6 packet header.

**doh-number**

(Optional) Integer in the range from 0 to 255 representing an IPv6 destination option extension header.

**doh-type**

(Optional) Destination option header types. The possible destination option header type and its corresponding `doh-number` value are home-address—201.

**dscp value**

(Optional) Matches a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.

**flow-label value**

(Optional) Matches a flow label value against the flow label value in the Flow Label field of each IPv6 packet header. The acceptable range is from 0 to 1048575.
| **fragments** | (Optional) Matches non-initial fragmented packets where the fragment extension header contains a non-zero fragment offset. The **fragments** keyword is an option only if the `operator [port-number]` arguments are not specified. |
| **hbh** | (Optional) Specifies a hop-by-hop options header. |
| **log** | (Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the `logging console` command.) The message includes the access list name and sequence number, whether the packet was denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets denied in the prior 5-minute interval. |
| **log-input** | (Optional) Provides the same function as the **log** keyword, except that the logging message also includes the input interface. |
| **mobility** | (Optional) Extension header type. Allows matching of any IPv6 packet including a mobility header, regardless of the value of the mobility-header-type field within that header. |
| **mobility-type** | (Optional) Mobility header type. Either the `mh-number` or `mh-type` argument must be used with this keyword. |
| **mh-number** | (Optional) Integer in the range from 0 to 255 representing an IPv6 mobility header type. |
| **mh-type** | (Optional) Name of a mobility header type. Possible mobility header types and their corresponding `mh-number` value are as follows: |
| | • 0—bind-refresh |
| | • 1—hoti |
| | • 2—coti |
| | • 3—hot |
| | • 4—cot |
| | • 5—bind-update |
| | • 6—bind-acknowledgment |
| | • 7—bind-error |
| **routing** | (Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header. |
| routing-type | (Optional) Allows routing headers with a value in the type field to be matched independently. The routing-number argument must be used with this keyword. |
| routing-number | Integer in the range from 0 to 255 representing an IPv6 routing header type. Possible routing header types and their corresponding routing-number value are as follows:

- 0—Standard IPv6 routing header
- 2—Mobile IPv6 routing header |
| sequence value | (Optional) Specifies the sequence number for the access list statement. The acceptable range is from 1 to 4294967295. |
| time-range name | (Optional) Specifies the time range that applies to the deny statement. The name of the time range and its restrictions are specified by the time-range and absolute or periodic commands, respectively. |
| undetermined-transport | (Optional) Matches packets from a source for which the Layer 4 protocol cannot be determined. The **undetermined-transport** keyword is an option only if the operator [port-number] arguments are not specified. |
| icmp-type | (Optional) Specifies an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. The ICMP message type can be a number from 0 to 255, some of which include the following predefined strings and their corresponding numeric values:

- 144—dhaad-request
- 145—dhaad-reply
- 146—mpd-solicitation
- 147—mpd-advertisement |
<p>| icmp-code | (Optional) Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255. |
| icmp-message | (Optional) Specifies an ICMP message name for filtering ICMP packets. ICMP packets can be filtered by an ICMP message name or ICMP message type and code. The possible names are listed in the “Usage Guidelines” section. |
| ack | (Optional) For the TCP protocol only: acknowledgment (ACK) bit set. |
| established | (Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection. |
| fin | (Optional) For the TCP protocol only: Fin bit set; no more data from sender. |</p>
<table>
<thead>
<tr>
<th>Command Default</th>
<th>No IPv6 access list is defined.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>IPv6 access list configuration (config-ipv6-acl)#</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.0(23)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td></td>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td></td>
<td>12.4(2)T</td>
<td>The icmp-type argument was enhanced. The dest-option-type, mobility, mobility-type, and routing-type keywords were added. The doh-number, doh-type, mh-number, mh-type, and routing-number arguments were added.</td>
</tr>
<tr>
<td></td>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td></td>
<td>12.2(25)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)SG.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on Cisco ASR 1000 Aggregation Series Routers.</td>
</tr>
<tr>
<td></td>
<td>12.4(20)T</td>
<td>The auth keyword was added.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRE</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRE.</td>
</tr>
<tr>
<td></td>
<td>15.2(3)T</td>
<td>This command was modified. Support was added for the hbh keyword.</td>
</tr>
<tr>
<td></td>
<td>15.1(1)SY</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)SY.</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
<tr>
<td></td>
<td>15.4(2)S</td>
<td>This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.</td>
</tr>
</tbody>
</table>

| Usage Guidelines | The deny (IPv6) command is similar to the deny (IP) command, except that it is IPv6-specific. |
Use the `deny (IPv6)` command following the `ipv6 access-list` command to define the conditions under which a packet passes the access list or to define the access list as a reflexive access list.

Specifying IPv6 for the `protocol` argument matches against the IPv6 header of the packet.

By default, the first statement in an access list is number 10, and the subsequent statements are numbered in increments of 10.

You can add `permit`, `deny`, `remark`, or `evaluate` statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, IPv6 access control lists (ACLs) are defined and their deny and permit conditions are set by using the `ipv6 access-list` command with the `deny` and `permit` keywords in global configuration mode. In Cisco IOS Release 12.0(23)S or later releases, IPv6 ACLs are defined by using the `ipv6 access-list` command in global configuration mode and their permit and deny conditions are set by using the `deny` and `permit` commands in IPv6 access list configuration mode. Refer to the `ipv6 access-list` command for more information on defining IPv6 ACLs.

**Note**

In Cisco IOS Release 12.0(23)S or later releases, every IPv6 ACL has implicit `permit icmp any any nd-na`, `permit icmp any any nd-ns`, and `deny ipv6 any any` statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit `deny ipv6 any any` statement to take effect. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Both the `source-ipv6-prefix/prefix-length` and `destination-ipv6-prefix/prefix-length` arguments are used for traffic filtering (the source prefix filters traffic based upon the traffic source; the destination prefix filters traffic based upon the traffic destination).

**Note**

IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

The `fragments` keyword is an option only if the `operator [port-number]` arguments are not specified.

The `undetermined-transport` keyword is an option only if the `operator [port-number]` arguments are not specified.

The following is a list of ICMP message names:

- beyond-scope
- destination-unreachable
- echo-reply
- echo-request
- header
- hop-limit
Examples

The following example configures the IPv6 access list named toCISCO and applies the access list to outbound traffic on Ethernet interface 0. Specifically, the first deny entry in the list keeps all packets that have a destination TCP port number greater than 5000 from exiting out of Ethernet interface 0. The second deny entry in the list keeps all packets that have a source UDP port number less than 5000 from exiting out of Ethernet interface 0. The second deny also logs all matches to the console. The first permit entry in the list permits all ICMP packets to exit out of Ethernet interface 0. The second permit entry in the list permits all other traffic to exit out of Ethernet interface 0. The second permit entry is necessary because an implicit deny all condition is at the end of each IPv6 access list.

ipv6 access-list toCISCO
deny tcp any any gt 5000
deny ::/0 lt 5000 ::/0 log
permit icmp any any
permit any any
interface ethernet 0
ipv6 traffic-filter toCISCO out
The following example shows how to allow TCP or UDP parsing although an IPsec AH is present:

```
IPV6 access list example1
   deny tcp host 2001::1 any log sequence 5
   permit tcp any any auth sequence 10
   permit udp any any auth sequence 20
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ipv6 access-list</code></td>
<td>Defines an IPv6 access list and enters IPv6 access list configuration mode.</td>
</tr>
<tr>
<td></td>
<td><code>ipv6 traffic-filter</code></td>
<td>Filters incoming or outgoing IPv6 traffic on an interface.</td>
</tr>
<tr>
<td></td>
<td><code>permit (IPv6)</code></td>
<td>Sets permit conditions for an IPv6 access list.</td>
</tr>
<tr>
<td></td>
<td><code>show ipv6 access-list</code></td>
<td>Displays the contents of all current IPv6 access lists.</td>
</tr>
</tbody>
</table>
deny (MAC ACL)

To set conditions for a MAC access list, use the `deny` command in MAC access-list extended configuration mode. To remove a condition from an access list, use the `no` form of this command.

```
deny {src_mac_mask|host name src_mac_name|any} {dest_mac_mask|host name dst_mac_name|any} [{protocol_keyword|ethertype_number ethertype_mask} [vlan vlan_ID] [cos cos_value]]
no deny {src_mac_mask|host name src_mac_name|any} {dest_mac_mask|host name dst_mac_name|any} [{protocol_keyword|ethertype_number ethertype_mask} [vlan vlan_ID] [cos cos_value]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>src_mac_mask</td>
<td>Specifies the MAC address mask that identifies a selected block of source MAC addresses. A value of 1 represents a wildcard in that position.</td>
</tr>
<tr>
<td>host name src_mac_name</td>
<td>Specifies a source host that has been named using the <code>mac host name</code> command.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies any source or any destination host as an abbreviation for the <code>src_mac_mask</code> or <code>dest_mac_mask</code> value of 1111.1111.1111, which declares all digits to be wildcards.</td>
</tr>
<tr>
<td>dest_mac_mask</td>
<td>Specifies the MAC address mask that identifies a selected block of destination MAC addresses.</td>
</tr>
<tr>
<td>host name dst_mac_name</td>
<td>Specifies a destination host that has been named using the <code>mac host name</code> command.</td>
</tr>
<tr>
<td>protocol_keyword</td>
<td>(Optional) Specifies a named protocol (for example, ARP).</td>
</tr>
<tr>
<td>ethertype_number</td>
<td>(Optional) The EtherType number specifies the protocol within the Ethernet packet.</td>
</tr>
<tr>
<td>ethertype_mask</td>
<td>(Optional) The EtherType mask allows a range of Ethertypes to be specified together. This is a hexadecimal number from 0 to FFFF. An EtherType mask of 0 requires an exact match of the EtherType.</td>
</tr>
<tr>
<td>vlan vlan_ID</td>
<td>(Optional) Specifies a VLAN.</td>
</tr>
<tr>
<td>cos cos_value</td>
<td>(Optional) Specifies the Layer 2 priority level for packets. The range is from 0 to 7.</td>
</tr>
</tbody>
</table>

**Command Default**

This command has no defaults.

**Command Modes**

MAC access-list extended configuration (config-ext-macl)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXI</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

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

- The `vlan` and `cos` keywords are not supported in MAC ACLs used for VACL filtering.
- The `vlan` keyword for VLAN-based QoS filtering in MAC ACLs can be globally enabled or disabled and is disabled by default.
- Enter MAC addresses as three 2-byte values in dotted hexadecimal format. For example, 0123.4567.89ab.
- Enter MAC address masks as three 2-byte values in dotted hexadecimal format. Use 1 bits as wildcards. For example, to match an address exactly, use 0000.0000.0000 (can be entered as 0.0.0).
- An entry without a protocol parameter matches any protocol.
- Enter an EtherType and an EtherType mask as hexadecimal values from 0 to FFFF.

This list shows the EtherType values and their corresponding protocol keywords:
- `0x0600--xns-idp--Xerox XNS IDP`
- `0x0BAD--vines-ip--Banyan VINES IP`
- `0x0baf--vines-echo--Banyan VINES Echo`
- `0x6000--etype-6000--DEC unassigned, experimental`
- `0x6001--mop-dump--DEC Maintenance Operation Protocol (MOP) Dump/Load Assistance`
- `0x6002--mop-console--DEC MOP Remote Console`
- `0x6003--decn-net-iv--DEC DECnet Phase IV Route`
- `0x6004--lat--DEC Local Area Transport (LAT)`
- `0x6005--diagnostic--DEC DECnet Diagnostics`
- `0x6007--lavc-sca--DEC Local-Area VAX Cluster (LAVC), SCA`
- `0x6008--amber--DEC AMBER`
- `0x6009--mumps--DEC MUMPS`
- `0x0800--ip--Malformed, invalid, or deliberately corrupt IP frames`
- `0x8038--dec-spanning--DEC LANBridge Management`
- `0x8039--dsm--DEC DSM/DDP`
- `0x8040--netbios--DEC PATHWORKS DECnet NETBIOS Emulation`
- `0x8041--msdos--DEC Local Area System Transport`
- `0x8042--etype-8042--DEC unassigned`
- `0x809B--appltalk--Kinetics EtherTalk (AppleTalk over Ethernet)`
- `0x80F3--aarp--Kinetics AppleTalk Address Resolution Protocol (AARP)`

Examples

This example shows how to create a MAC-Layer ACL named `mac_layer` that denies `dec-phase-iv` traffic with source address `0000.4700.0001` and destination address `0000.4700.0009`, but allows all other traffic:

```plaintext
Router(config)# mac access-list extended mac_layer
Router(config-ext-macl)# deny 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 dec-phase-iv
Router(config-ext-macl)# permit any any
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit (MAC ACL)</td>
<td>Sets permit conditions for a named MAC access list.</td>
</tr>
<tr>
<td>mac access-list extended</td>
<td>Defines a MAC access list by name.</td>
</tr>
<tr>
<td>mac host</td>
<td>Assigns a name to a MAC address.</td>
</tr>
<tr>
<td>show mac access-group</td>
<td>Displays the contents of all current MAC access groups.</td>
</tr>
</tbody>
</table>
deny (WebVPN)

To set conditions in a named Secure Sockets Layer Virtual Private Network (SSL VPN) access list that will
deny packets, use the `deny` command in webvpn acl configuration mode. To remove a deny condition from
an access list, use the `no` form of this command.

```
deny [url [{anyurl-string}]][ {ip|tcp|udp|http|https|cifs}][ {any|source-ip source-mask}][{any|destination-ip destination-mask}][time-range time-range-name][syslog]
no deny url [{anyurl-string}] [{ip|tcp|udp|http|https|cifs}][{any|source-ip source-mask}][{any|destination-ip destination-mask}][time-range time-range-name][syslog]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>url</code></td>
<td>(Optional) Filtering rules are applied to the URL.</td>
</tr>
<tr>
<td></td>
<td>- Use the <code>any</code> keyword as an abbreviation for any URL.</td>
</tr>
<tr>
<td><code>url-string</code></td>
<td>(Optional) URL string defined as follows: <code>scheme://host[:port]/path</code></td>
</tr>
<tr>
<td></td>
<td>- <code>scheme</code> -- Can be HTTP, Secure HTTPS (HTTPS), or Common Internet File System (CIFS). This field is required in the URL string.</td>
</tr>
<tr>
<td></td>
<td>- <code>host</code> -- Can be a hostname or a host IP (host mask). The host can have one wildcard (*) .</td>
</tr>
<tr>
<td></td>
<td>- <code>port</code> -- Can be any valid port number (1-65535). It is possible to have multiple port numbers separated by a comma (.). The port range is expressed using a dash (-).</td>
</tr>
<tr>
<td></td>
<td>- <code>path</code> -- Can be any valid path string. In the path string, the $user is translated to the current user name.</td>
</tr>
<tr>
<td><code>ip</code></td>
<td>(Optional) Denies only IP packets. When you enter the <code>ip</code> keyword, you must use the specific command syntax shown for the IP form of the deny command.</td>
</tr>
<tr>
<td><code>tcp</code></td>
<td>(Optional) Denies only TCP packets. When you enter the <code>tcp</code> keyword, you must use the specific command syntax shown for the TCP form of the deny command.</td>
</tr>
<tr>
<td><code>udp</code></td>
<td>(Optional) Denies only UDP packets. When you enter the <code>udp</code> keyword, you must use the specific command syntax shown for the UDP form of the deny command.</td>
</tr>
<tr>
<td><code>http</code></td>
<td>(Optional) Denies only HTTP packets. When you enter the <code>http</code> keyword, you must use the specific command syntax shown for the HTTP form of the deny command.</td>
</tr>
<tr>
<td><code>https</code></td>
<td>(Optional) Denies only HTTPS packets. When you enter the <code>https</code> keyword, you must use the specific command syntax shown for the HTTPS form of the deny command.</td>
</tr>
<tr>
<td><code>cifs</code></td>
<td>(Optional) Denies only CIFS packets. When you enter the <code>cifs</code> keyword, you must use the specific command syntax shown for the CIFS form of the deny command.</td>
</tr>
</tbody>
</table>
source-ip
source-mask

(Optional) Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:

- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the any keyword as an abbreviation for a source and source mask of 0.0.0.0 255.255.255.255.
- Use host source as an abbreviation for a source and source-wildcard of source 0.0.0.0.

destination-ip
destination-mask

(Optional) Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination:

- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the any keyword as an abbreviation for a source and source mask of 0.0.0.0 255.255.255.255.
- Use host source as an abbreviation for a source and source-wildcard of source 0.0.0.0.

time-range
time-range-name

(Optional) Name of the time range that applies to this deny statement. The name of the time range and its restrictions are specified by the time-range and absolute or periodic commands, respectively.

syslog

(Optional) System logging messages are generated.

Command Default
There are no specific conditions under which a packet is denied passing the named access list.

Command Modes
Webvpn acl configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
Use this command following the acl command to specify conditions under which a packet cannot pass the named access list.

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

Examples
The following example shows that all packets from the URL “https://10.168.2.228:34,80-90,100-/public” will be denied:

webvpn context context1
acl acl1
deny url “https://10.168.2.228:34,80-90,100-/public”
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>absolute</td>
<td>Specifies an absolute time for a time range.</td>
</tr>
<tr>
<td>periodic</td>
<td>Specifies a recurring (weekly) time range for functions that support the time-range feature.</td>
</tr>
<tr>
<td>permit (webvpn acl)</td>
<td>Sets conditions to allow a packet to pass a named SSL VPN access list.</td>
</tr>
<tr>
<td>time-range</td>
<td>Enables time-range configuration mode and defines time ranges for functions (such as extended access lists).</td>
</tr>
</tbody>
</table>
description (dot1x credentials)

To specify a description for an 802.1X profile, use the `description` command in dot1x credentials configuration mode. To remove the description, use the `no` form of this command.

```
description text
no description
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>text</code></td>
<td>Text description. The description can be up to 80 characters.</td>
</tr>
</tbody>
</table>

**Command Default**

A description is not specified.

**Command Modes**

Dot1x credentials configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before using this command, the `dot1x credentials` command must have been configured.

An 802.1X credential structure is necessary when configuring a supplicant (client). This credentials structure may contain a username, password, and description.

**Examples**

The following example shows which credentials profile should be used when configuring a supplicant, and it provides a description of the credentials profile:

```
dot1x credentials basic-user
   username router
   password secret
   description This credentials profile should be used for most configured ports
```

The credentials structure can be applied to an interface, along with the `dot1x pae supplicant` command and keyword, to enable supplicant functionality on that interface.

```
interface fastethernet 0/1
   dot1x credentials basic-user
   dot1x pae supplicant
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x credentials</code></td>
<td>Specifies which 802.1X credentials profile to use.</td>
</tr>
</tbody>
</table>
description (identify zone)

To enter a description of a zone, use the `description` command in security zone configuration mode. To remove the description of the zone, use the `no` form of this command.

```
description  line-of-description
no  description  line-of-description
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>line-of-description</th>
<th>Description of the zone. You can enter up to 40 characters.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Security zone configuration</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th>You can use this subcommand after entering the <code>zone security</code> or <code>zone-pair security</code> command.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Examples</th>
<th>The following example specifies that zone z1 is a testzone:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>zone security z1</code></td>
</tr>
<tr>
<td></td>
<td><code>description testzone</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>zone-pair security</code></td>
<td>Creates a zone-pair that is the type security.</td>
</tr>
<tr>
<td></td>
<td><code>zone security</code></td>
<td>Creates a zone.</td>
</tr>
</tbody>
</table>
description (identity policy)

To enter a description for an identity policy, use the description command in identity policy configuration mode. To remove the description, use the no form of this command.

```
description line-of-description
no description line-of-description
```

**Syntax Description**

| line-of-description | Description of the identity policy. |

**Command Default**

A description is not entered for the identity policy.

**Command Modes**

Identity policy configuration (config-identity-policy)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows that a default identity policy and its description ("policyname1") have been specified:

```
Router (config)# identity policy policyname1
Router (config-identity-policy)# description policyABC
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description (identity profile)</td>
<td>Enters a description for an identity profile.</td>
</tr>
</tbody>
</table>
**description (identity profile)**

To enter a description for an identity profile, use the `description` command in identity profile configuration mode. To remove the description of the identity profile, use the `no` form of this command.

```
description line-of-description
no description line-of-description
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description of the identity profile.</th>
</tr>
</thead>
</table>

**Command Default**

A description is not entered for the identity profile.

**Command Modes**

Identity profile configuration (config-identity-prof)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)XA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>This command was previously configured in dot1x configuration mode.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `identity profile` command and one of its keywords (`default`, `dot1x`, or `eapoudp`) must be entered in global configuration mode before the `description` command can be used.

**Examples**

The following example shows that a default identity profile and its description ("ourdefaultpolicy") have been specified:

```
Router (config)# identity profile default
Router (config-identity-prof)# description ourdefaultpolicy
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>description (identity policy)</code></td>
<td>Enters a description for an identity policy.</td>
</tr>
<tr>
<td><code>identity profile</code></td>
<td>Creates an identity profile and enters identity profile configuration mode.</td>
</tr>
</tbody>
</table>
**description (IKEv2 keyring)**

To add the description of an Internet Key Exchange Version 2 (IKEv2) peer or profile, use the `description` command in the IKEv2 keyring peer configuration mode. To delete the description, use the `no` form of this command.

```
description line-of-description
no description line-of-description
```

**Syntax Description**
- `line-of-description` Description given to an IKE peer or profile.

**Command Default**
The peer or profile is not described.

**Command Modes**
IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(T)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use this command to provide a descriptive line about the IKEv2 peer, peer group, or profile.

**Examples**
The following example shows that the description “connection from site A” has been added to an IKEv2 peer:

```
Router(config)# crypto ikev2 keyring keyr 1
Router(configikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description connection from site A
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address (ikev2 keyring)</td>
<td>Specifies the IPv4 address or the range of the peers in IKEv2 keyring.</td>
</tr>
<tr>
<td>crypto ikev2 keyring</td>
<td>Defines an IKEv2 keyring.</td>
</tr>
<tr>
<td>hostname (ikev2 keyring)</td>
<td>Specifies the hostname for the peer in the IKEv2 keyring.</td>
</tr>
<tr>
<td>identity (ikev2 keyring)</td>
<td>Identifies the peer with IKEv2 types of identity.</td>
</tr>
<tr>
<td>peer</td>
<td>Defines a peer or a peer group for the keyring.</td>
</tr>
<tr>
<td>pre-shared-key (ikev2 keyring)</td>
<td>Defines a preshared key for the IKEv2 peer.</td>
</tr>
</tbody>
</table>
**description (isakmp peer)**

To add the description of an Internet Key Exchange (IKE) peer, use the `description` command in ISAKMP peer configuration mode. To delete the description, use the `no` form of this command.

```
description  line-of-description
no description  line-of-description
```

**Syntax Description**

| line-of-description | Description given to an IKE peer |

**Command Default**

No default behavior or values

**Command Modes**

ISAKMP peer configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXD.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

IKE peers that “sit” behind a Network Address Translation (NAT) device cannot be uniquely identified; therefore, they have to share the same peer description.

**Examples**

The following example shows that the description “connection from site A” has been added for an IKE peer:

```
Router# crypto isakmp peer address 10.2.2.9
Router (config-isakmp-peer)# description connection from site A
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear crypto session</td>
<td>Deletes crypto sessions (IPSec and IKE SAs).</td>
</tr>
<tr>
<td>show crypto isakmp peer</td>
<td>Displays peer descriptions.</td>
</tr>
<tr>
<td>show crypto session</td>
<td>Displays status information for active crypto sessions in a router.</td>
</tr>
</tbody>
</table>
destination host

To configure the fully qualified domain name (FQDN) of a Diameter peer, use the `destination host` command in diameter peer configuration submode. To disable the configured FQDN, use the `no` form of this command.

```
destination host string
no destination host string
```

**Syntax Description**
- `string` | The FQDN of the Diameter peer.

**Command Default**
No FQDN is configured.

**Command Modes**
Diameter peer configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the destination host:

```
Router(config-dia-peer)# destination host host1.example.com.
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination realm</td>
<td>Configures the destination realm of a Diameter peer.</td>
</tr>
<tr>
<td>diameter peer</td>
<td>Configures a Diameter peer and enters Diameter peer configuration submode.</td>
</tr>
</tbody>
</table>
destination realm

To configure the destination realm of a Diameter peer, use the `destination realm` command in diameter peer configuration submode. To disable the configured realm, use the `no` form of this command.

```
destination realm string
no destination realm string
```

**Syntax Description**

- `string`  The destination realm (part of the domain `@realm`) in which a Diameter peer is located.

**Command Default**

No realm is configured.

**Command Modes**

Diameter peer configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The realm might be added by the authentication, authorization, and accounting (AAA) client when sending a request to AAA. However, if the client does not add the attribute, then the value configured while in Diameter peer configuration submode is used when sending messages to the destination Diameter peer. If a value is not configured while in Diameter peer configuration submode, the value specified by the `diameter destination realm` global configuration command is used.

**Examples**

The following example shows how to configure the destination realm:

```
router (config-dia-peer)# destination realm example.com
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>diameter destination realm</code></td>
<td>Configures a global Diameter destination realm.</td>
</tr>
<tr>
<td><code>diameter peer</code></td>
<td>Configures a Diameter peer and enters Diameter peer configuration submode.</td>
</tr>
</tbody>
</table>
device (identity profile)

To statically authorize or reject individual devices, use the `device` command in identity profile configuration mode. To disable the authorization or rejection, use the `no` form of this command.

```
device {authorize {ip address ip-address policy policy-name|mac-address mac-address|type {cisco|ip|phone}|[not-authorize]}
no device {authorize {ip address ip-address policy policy-name|mac-address mac-address|type {cisco|ip|phone}|[not-authorize]}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorize</td>
<td>Configures an authorized device.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies a device by its IP address.</td>
</tr>
<tr>
<td>ip-address</td>
<td>The IP address.</td>
</tr>
<tr>
<td>policy</td>
<td>Applies an associated policy with the device.</td>
</tr>
<tr>
<td>policy-name</td>
<td>Name of the policy.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Specifies a device by its MAC address.</td>
</tr>
<tr>
<td>mac-address</td>
<td>The MAC address.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies a device by its type.</td>
</tr>
<tr>
<td>cisco</td>
<td>Specifies a Cisco device.</td>
</tr>
<tr>
<td>ip</td>
<td>Specifies an IP device.</td>
</tr>
<tr>
<td>phone</td>
<td>Specifies a Cisco IP phone.</td>
</tr>
<tr>
<td>not-authorize</td>
<td>Configures an unauthorized device.</td>
</tr>
</tbody>
</table>

### Command Default

A device is not statically authorized or rejected.

### Command Modes

Identity profile configuration (config-identity-prof)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)XA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>The <code>unauthorize</code> keyword was changed to <code>not authorize</code>. The <code>cisco-device</code> argument was deleted. The <code>ip address</code> keyword and <code>ip-address</code> argument were added. The <code>ip</code> and <code>phone</code> keywords were added.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

The `identity profile` command and `default`, `dot1x`, or `eapoudp` keywords must be entered in global configuration mode before the `device` command can be used.

**Examples**

The following configuration example defines an identity profile for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) to statically authorize host 192.168.1.3 with "policyname1" as the associated identity policy:

```
Router(config)# identity profile eapoudp
Router(config-identity-prof)# device authorize ip-address 192.168.1.3 policy policyname1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>identity profile eapoudp</td>
<td>Creates an identity profile.</td>
</tr>
</tbody>
</table>
device-role

To specify the role of the device attached to the port, use the **device-role** command in neighbor discovery (ND) inspection policy configuration mode or router advertisement (RA) guard policy configuration mode.

```
device-role {host|monitor|router}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Sets the role of the device to host.</td>
</tr>
<tr>
<td>monitor</td>
<td>Sets the role of the device to monitor.</td>
</tr>
<tr>
<td>router</td>
<td>Sets the role of the device to router.</td>
</tr>
</tbody>
</table>

### Command Default

The device role is host.

### Command Modes

- ND inspection policy configuration (config-nd-inspection)
- RA guard policy configuration (config-ra-guard)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
<tr>
<td>15.0(2)SE</td>
<td>This command was integrated into Cisco IOS Release 15.0(2)SE.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is host, and therefore all the inbound router advertisement and redirect messages are blocked. If the device role is enabled using the **router** keyword, all messages (router solicitation [RS], router advertisement [RA], or redirect) are allowed on this port.

When the **router** or **monitor** keyword is used, the multicast RS messages are bridged on the port, regardless of whether limited broadcast is enabled. However, the **monitor** keyword does not allow inbound RA or redirect messages. When the **monitor** keyword is used, devices that need these messages will receive them.

### Note

With the introduction of Cisco IOS Release 15.2(4)S1, the trusted port has precedence over the device role for accepting RAs over a port to the router. Prior to this release, the device role router had precedence over the trusted port. The device role of the router still needs to be configured in order for the RS to be sent over the port.

### Examples

The following example defines a Neighbor Discovery Protocol (NDP) policy name as policy1, places the device in ND inspection policy configuration mode, and configures the device as the host:
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# device-role host

The following example defines an RA guard policy name as raguard1, places the device in RA guard policy configuration mode, and configures the device as the host:

Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# device-role host

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ipv6 nd inspection policy</td>
<td>Defines the ND inspection policy name and enters ND inspection policy configuration mode.</td>
</tr>
<tr>
<td></td>
<td>ipv6 nd raguard policy</td>
<td>Defines the RA guard policy name and enters RA guard policy configuration mode.</td>
</tr>
</tbody>
</table>
**device-sensor accounting**

To add device sensor protocol data to accounting records and to generate accounting events when new sensor data is detected, use the `device-sensor accounting` command in global configuration mode. To disable adding device sensor protocol data to accounting records and to disable generating accounting events, use the `no` form of this command.

```
device-sensor accounting
no device-sensor accounting
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The device sensor protocol data is added to the accounting records and accounting events are generated when new sensor data is detected.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)SE1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(1)SG</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)SG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The device sensor is used to glean endpoint information from Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), and DHCP messages and make this information available to registered clients in the context of an access session. You can use the `device-sensor accounting` command to include the data gleaned by the device sensor in RADIUS accounting messages.

**Examples**

The following example shows how to add the device sensor protocol data to accounting records:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor accounting
Device(config)# end
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug device-sensor</code></td>
<td>Enables debugging for the device sensor.</td>
</tr>
<tr>
<td><code>show device-sensor cache</code></td>
<td>Displays device sensor cache entries.</td>
</tr>
</tbody>
</table>
device-sensor filter-list cdp

To create a Cisco Discovery Protocol filter containing a list of Type-Length-Value (TLV) fields that can be included or excluded in the device sensor output, use the `device-sensor filter-list cdp` command in global configuration mode. To remove the Cisco Discovery Protocol filter containing the list of TLV fields, use the `no` form of this command.

```
device-sensor filter-list cdp list cdp-list
do device-sensor filter-list cdp list cdp-list
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>Specifies a Cisco Discovery Protocol TLV filter list.</td>
</tr>
<tr>
<td><code>tlv-list-name</code></td>
<td>Cisco Discovery Protocol TLV filter list name.</td>
</tr>
</tbody>
</table>

**Command Default**
Cisco Discovery Protocol TLV filter list is not available.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)SE1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(1)SG</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)SG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `device-sensor filter-list cdp list tlv-list-name` command to configure the name of the Cisco Discovery Protocol TLV filter list and enter Cisco Discovery Protocol sensor configuration mode. You can configure the list of TLVs in Cisco Discovery Protocol sensor configuration mode using the `tlv {name tlv-name | number tlv-number}` command. Use the `name tlv-name` keyword-argument pair to specify the name of the TLV. Enter `?` for querying the available TLV names. Use the `number tlv-name` keyword-argument pair to specify the TLV number to be added to the Cisco Discovery Protocol TLV filter list.

Use the `no tlv {name tlv-name | number tlv-number}` command to remove individual TLVs from the Cisco Discovery Protocol TLV filter list.

Use the `no device-sensor filter-list cdp list tlv-list-name` command to remove the entire TLV list containing all the TLVs.

**Examples**

The following example shows how to create a Cisco Discovery Protocol filter containing a list of TLVs:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor filter-list cdp list cdp-list
Device(config-sensor-cdplist)# tlv name address-type
Device(config-sensor-cdplist)# tlv name device-name
Device(config-sensor-cdplist)# tlv number 34
Device(config-sensor-cdplist)# end
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug device-sensor</td>
<td>Enables debugging for the device sensor.</td>
</tr>
<tr>
<td>device-sensor accounting</td>
<td>Adds the device sensor protocol data to accounting records and generates</td>
</tr>
<tr>
<td></td>
<td>additional accounting events when new sensor data is detected.</td>
</tr>
<tr>
<td>device-sensor filter-list dhcp</td>
<td>Creates a DHCP filter containing a list of options that can be included or</td>
</tr>
<tr>
<td></td>
<td>excluded in the device sensor output.</td>
</tr>
<tr>
<td>device-sensor filter-list lldp</td>
<td>Creates an LLDP filter containing a list of TLV fields that can be included</td>
</tr>
<tr>
<td></td>
<td>or excluded in the device sensor output.</td>
</tr>
<tr>
<td>show device-sensor cache</td>
<td>Displays device sensor cache entries.</td>
</tr>
</tbody>
</table>
device-sensor filter-list dhcp

To create a DHCP filter containing a list of options that can be included or excluded in the device sensor output, use the `device-sensor filter-list dhcp` command in global configuration mode. To remove the DHCP filter containing the list of options, use the `no` form of this command.

```
device-sensor filter-list dhcp list  option-list-name
no device-sensor filter-list dhcp list  option-list-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>Specifies a DHCP options filter list.</td>
</tr>
<tr>
<td>option-list-name</td>
<td>Name of DHCP options filter list.</td>
</tr>
</tbody>
</table>

**Command Default**

DHCP options filter list is not available.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)SE1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(1)SG</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)SG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `device-sensor filter-list dhcp list option-list-name` command to configure the name of the DHCP options filter list and enter into DHCP sensor configuration mode. You can configure the list of options in DHCP sensor configuration mode using the `option { name option-name | number option-number }` command. Use the `name option-name` keyword-argument pair to specify the name of the TLV. Enter `?` for querying the available TLV names. Use the `number option-name` keyword-argument pair to specify the TLV number to be added to the DHCP options filter list.

Use the `no option { name option-name | number option-number }` command to remove individual options from the DHCP options filter list.

Use the `no device-sensor filter-list dhcp list option-list-name` command to remove the entire TLV list containing all the TLVs.

**Examples**

The following example shows how to create a DHCP filter containing a list of options:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor filter-list dhcp list dhcp-list
Device(config-sensor-dhcplist)# option name address-type
Device(config-sensor-dhcplist)# option name device-name
Device(config-sensor-dhcplist)# option number 34
Device(config-sensor-dhcplist)# end
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug device-sensor</td>
<td>Enables debugging for the device sensor.</td>
</tr>
<tr>
<td>device-sensor accounting</td>
<td>Adds the device sensor protocol data to accounting records and generates additional accounting events when new sensor data is detected.</td>
</tr>
<tr>
<td>device-sensor filter-list cdp</td>
<td>Creates a Cisco Discovery Protocol filter containing a list of TLV fields that can be included or excluded in the device sensor output.</td>
</tr>
<tr>
<td>device-sensor filter-list lldp</td>
<td>Creates an LLDP filter containing a list of TLV fields that can be included or excluded in the device sensor output.</td>
</tr>
<tr>
<td>show device-sensor cache</td>
<td>Displays device sensor cache entries.</td>
</tr>
</tbody>
</table>
device-sensor filter-list lldp

To create a Link Layer Discovery Protocol (LLDP) filter containing a list of Type-Length-Value (TLV) fields that can be included or excluded in the device sensor output, use the `device-sensor filter-list lldp` command in global configuration mode. To remove the LLDP filter containing the list of TLV fields, use the `no` form of this command.

```
device-sensor filter-list lldp list  tlv-list-name
no device-sensor filter-list lldp list  tlv-list-name
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>Specifies an LLDP TLV filter list.</td>
</tr>
<tr>
<td>tlv-list-name</td>
<td>Name of the LLDP TLV filter list.</td>
</tr>
</tbody>
</table>

**Command Default**

LLDP TLV filter list is not available.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)SE1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(1)SG</td>
<td>This command was integrated into Cisco IOS Release 15.1(SG).</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `device-sensor filter-list lldp list tlv-list-name` command to configure the name of the LLDP TLV filter list and enter LLDP sensor configuration mode. You can configure the list of TLVs in LLDP sensor configuration mode using the `tlv {name tlv-name | number tlv-number}` command. Use the `name tlv-name` keyword-argument pair to specify the name of the TLV. Enter `?` for querying the available TLV names. Use the `number tlv-name` keyword-argument pair to specify the TLV number to be added to the LLDP TLV filter list.

Use the `no tlv {name tlv-name | number tlv-number}` command to remove individual TLVs from the LLDP TLV filter list.

Use the `no device-sensor filter-list lldp list tlv-list-name` command to remove the entire TLV list containing all the TLVs.

**Examples**

The following example shows how to create an LLDP filter containing a list of TLVs:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor filter-list lldp list lldp-list
Device(config-sensor-lldplist)# tlv name address-type
Device(config-sensor-lldplist)# tlv name device-name
Device(config-sensor-lldplist)# tlv number 34
Device(config-sensor-lldplist)# end
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug device-sensor</code></td>
<td>Enables debugging for the device sensor.</td>
</tr>
<tr>
<td><code>device-sensor accounting</code></td>
<td>Adds the device sensor protocol data to accounting records and generates additional accounting events when new sensor data is detected.</td>
</tr>
<tr>
<td><code>device-sensor filter-list cdp</code></td>
<td>Creates a Cisco Discovery Protocol filter containing a list of TLV fields that can be included or excluded in the device sensor output.</td>
</tr>
<tr>
<td><code>device-sensor filter-list dhcp</code></td>
<td>Creates a DHCP filter containing a list of options that can be included or excluded in the device sensor output.</td>
</tr>
<tr>
<td><code>show device-sensor cache</code></td>
<td>Displays device sensor cache entries.</td>
</tr>
</tbody>
</table>
device-sensor filter-spec

To apply a specific protocol filter containing a list of Type-Length-Value (TLV) fields to the device sensor output, use the device-sensor filter-spec command in global configuration mode. To remove the protocol filter list from the device sensor output, use the no form of this command.

```
device-sensor filter-spec { cdp | dhcp | lldp } { exclude { all | list list-name } | include list list-name }
no device-sensor filter-spec { cdp | dhcp | lldp } { exclude { all | list list-name } | include list list-name }
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdp</td>
<td>Applies a Cisco Discovery Protocol TLV filter list to the device sensor output.</td>
</tr>
<tr>
<td>dhcp</td>
<td>Applies a DHCP TLV filter list to the device sensor output.</td>
</tr>
<tr>
<td>lldp</td>
<td>Applies a Link Layer Discovery Protocol (LLDP) TLV filter list to the device sensor output.</td>
</tr>
<tr>
<td>exclude</td>
<td>Specifies the TLVs that should be excluded from the device sensor output.</td>
</tr>
<tr>
<td>all</td>
<td>Disables all notifications for the associated protocol.</td>
</tr>
<tr>
<td>list list-name</td>
<td>Specifies the name of the protocol TLV filter list.</td>
</tr>
<tr>
<td>include</td>
<td>Specifies the TLVs that should be included in the device sensor output.</td>
</tr>
</tbody>
</table>

Command Default
All TLVs are included in notifications and will trigger notifications.

Command Modes
Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)SE1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(1)SG</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)SG.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the device-sensor filter-spec command to specify the TLVs that must be included in all sensor outputs (session notifications sent to internal sensor clients and accounting requests).

Certain TLVs and message types such as DISCOVER, OFFER, REQUEST, ACK, and IP addresses are excluded because they are used as transport for higher layer protocols and will change frequently without conveying any useful information about the endpoint.

OFFER messages will also be ignored as they may be received from multiple servers and will not convey any useful endpoint data.

Examples

The following example shows how to apply a Cisco Discovery Protocol TLV filter list to the device sensor output:

```
Device> enable
```
Device# **configure terminal**
Device(config)# **device-sensor filter-spec cdp include list cdp-list1**
Device(config)# **end**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>debug device-sensor</strong></td>
<td>Enables debugging for device sensor.</td>
</tr>
<tr>
<td><strong>device-sensor accounting</strong></td>
<td>Adds the device sensor protocol data to accounting records and generates</td>
</tr>
<tr>
<td></td>
<td>additional accounting events when new sensor data is detected.</td>
</tr>
<tr>
<td><strong>device-sensor filter-list cdp</strong></td>
<td>Creates a Cisco Discovery Protocol filter containing a list of options that can be included or excluded in the device sensor output.</td>
</tr>
<tr>
<td><strong>device-sensor filter-list dhcp</strong></td>
<td>Creates a DHCP filter containing a list of options that can be included or excluded in the device sensor output.</td>
</tr>
<tr>
<td><strong>device-sensor filter-list lldp</strong></td>
<td>Creates an LLDP filter containing a list of TLV fields that can be included or excluded in the device sensor output.</td>
</tr>
<tr>
<td><strong>show device-sensor cache</strong></td>
<td>Displays device sensor cache entries.</td>
</tr>
</tbody>
</table>
device-sensor filter-spec http

To apply a device sensor filter specification to HTTP type, length, value (TLV) fields, use the `device-sensor filter-spec http` command in global configuration mode. To remove the device sensor filter specification from HTTP TLV fields, use the `no` form of this command.

device-sensor filter-spec http exclude all
no device-sensor filter-spec http

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exclude</code></td>
<td>Specifies the TLVs that should be excluded from the device sensor output.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Disables all notifications for the associated protocol.</td>
</tr>
</tbody>
</table>

**Command Default**
The device sensor processes HTTP TLVs.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(2)E</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `device-sensor filter-spec http` command to specify that HTTP TLVs must be included in all sensor output (session notifications sent to internal sensor clients and accounting requests).

**Examples**
The following example shows how to apply a device sensor filter specification to HTTP TLVs:

Device> enable
Device# configure terminal
Device(config)# device-sensor filter-spec http exclude all
Device(config)# end

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug device-sensor</td>
<td>Enables debugging for a device sensor.</td>
</tr>
<tr>
<td>device-sensor accounting</td>
<td>Adds device sensor protocol data to accounting records and generates additional accounting events when new sensor data is detected.</td>
</tr>
<tr>
<td>device-sensor filter-spec</td>
<td>Applies a specific protocol filter containing a list of TLV fields to the device sensor output.</td>
</tr>
<tr>
<td>device-sensor filter-list cdp</td>
<td>Creates a Cisco Discovery Protocol filter containing a list of options that can be included or excluded in the device sensor output.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>device-sensor filter-list dhcp</code></td>
<td>Creates a DHCP filter containing a list of options that can be included or excluded in the device sensor output.</td>
</tr>
<tr>
<td><code>device-sensor filter-list lldp</code></td>
<td>Creates an LLDP filter containing a list of TLV fields that can be included or excluded in the device sensor output.</td>
</tr>
<tr>
<td><code>show device-sensor cache</code></td>
<td>Displays device sensor cache entries.</td>
</tr>
</tbody>
</table>
device-sensor notify

To enable client notifications and accounting events for Type-Length-Value (TLV) changes, use the device-sensor notify command in global configuration mode. To disable client notifications and accounting events for TLV changes, use the no form of this command.

```
device-sensor notify { all-changes | new-tlvs }
no device-sensor notify { all-changes | new-tlvs }
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-changes</td>
<td>Enables client notifications and accounting events for all TLV changes.</td>
</tr>
<tr>
<td>new-tlvs</td>
<td>Enables client notifications and accounting events for only new TLV changes.</td>
</tr>
</tbody>
</table>

### Command Default

Client notifications and accounting events are generated only for new TLVs.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(SE)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(SG)</td>
<td>This command was integrated into Cisco IOS Release 15.1(SG).</td>
</tr>
</tbody>
</table>

### Usage Guidelines

By default, for each supported peer protocol, client notifications and accounting events will be generated only when an incoming packet includes a TLV that was not previously received in the context of a given session.

To enable client notifications and accounting events for all TLV changes, where either a new TLV has been received or a previously received TLV was received with a different value, use the device-sensor notify all-changes command.

To return to the default behavior, use the device-sensor notify new-tlvs or the default device-sensor notify command.

### Examples

The following example shows how to enable client notifications and accounting events for all TLV changes:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor notify all-changes
Device(config)# end
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug device-sensor</td>
<td>Enables debugging for device sensor.</td>
</tr>
<tr>
<td>device-sensor accounting</td>
<td>Adds the device sensor protocol data to accounting records and generates additional accounting events when new sensor data is detected.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>device-sensor filter-list cdp</code></td>
<td>Creates a Cisco Discovery Protocol filter containing a list of options that can be included or excluded in the device sensor output.</td>
</tr>
<tr>
<td><code>device-sensor filter-list dhcp</code></td>
<td>Creates a DHCP filter containing a list of options that can be included or excluded in the device sensor output.</td>
</tr>
<tr>
<td><code>device-sensor filter-list lldp</code></td>
<td>Creates an LLDP filter containing a list of TLV fields that can be included or excluded in the device sensor output.</td>
</tr>
<tr>
<td><code>show device-sensor cache</code></td>
<td>Displays device sensor cache entries.</td>
</tr>
</tbody>
</table>
dhcp (IKEv2)

To assign an IP address to the remote access client using a DHCP server, use the `dhcp` command in IKEv2 authorization policy configuration mode. To remove the assigned IP address, use the `no` form of this command.

```
dhcp {giaddr ip-address|server {ip-address hostname}|timeout seconds}
no dhcp {giaddr|server|timeout}
```

**Syntax Description**
- `giaddr ip-address`: Specifies the gateway IP address (giaddr).
- `server {ip-address hostname}`: Specifies addresses for the DHCP server.
- `ip-address`: IP address of the DHCP server.
- `hostname`: Hostname of the DHCP server. The hostname is resolved during configuration.
- `timeout seconds`: Specifies the wait time in seconds before the next DHCP server in the list is tried.

**Command Default**
An IP address is not assigned by a DHCP server.

**Command Modes**
IKEv2 client group configuration (config-ikev2-author-policy)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(3)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
If this command is not configured, an IP address is assigned to a remote device using either a local pool that is configured on a device or a framed IP address attribute that is defined in RADIUS.

**Note**
You can specify only one DHCP server. It is assumed that the DHCP server can be reached via the global routing table, and therefore, the DHCP packets are forwarded to the global routing table.

**Examples**
The following example shows that the IP address of the DHCP server is 192.0.2.1 and that the time to wait until the next DHCP server on the list is tried is 6 seconds:

```
Device(config)# crypto ikev2 client configuration group home
Device(config-ikev2-client-config-group)# key abcd
Device(config-ikev2-client-config-group)# dhcp server 192.0.2.1
Device(config-ikev2-client-config-group)# dhcp timeout 6
```

**Related Commands**
- `crypto ikev2 authorization policy`: Specifies an IKEv2 authorization policy group.
**dhcp server (isakmp)**

To assign an IP address or hostname using a DHCP server, use the `dhcp server` command in crypto ISAKMP group configuration mode. To remove the assigned IP address or hostname, use the `no` form of this command.

```
dhcp server {ip-address hostname}
no dhcp server {ip-address hostname}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Address of the DHCP server.</td>
</tr>
<tr>
<td>hostname</td>
<td>Hostname of the DHCP server.</td>
</tr>
</tbody>
</table>

### Command Default

IP address is not assigned by a DHCP server.

### Command Modes

Crypto ISAKMP group configuration (config-isakmp-group)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If this command is not configured, an IP address is assigned to a remote device using either a local pool that is configured on a router or a framed IP address attribute that is defined in RADIUS.

Note: Up to five DHCP servers can be configured one at a time.

Note: The DHCP proxy feature does not include functionality for the DHCP server to "push" the DNS, WINS server, or domain name to the remote client.

### Examples

The following example shows that the IP address of the DHCP server is 10.2.3.4 and that the time to wait until the next DHCP server on the list is tried is 6 seconds:

```
Router (config)# crypto isakmp client configuration group home
Router (config-isakmp-group)# key abcd
Router (config-isakmp-group)# dhcp server 10.2.3.4
Router (config-isakmp-group)# dhcp timeout 6
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto isakmp client configuration group</td>
<td>Specifies to which group a policy profile will be defined.</td>
</tr>
</tbody>
</table>
**dhcp timeout**

To set the wait time before the next DHCP server on the list is tried, use the `dhcp timeout` command in crypto ISAKMP group configuration mode. To remove the wait time that was set, use the `no` form of this command.

```
 dhcp timeout time
 no dhcp timeout time
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>time</code></td>
<td>Response time in seconds. Value = 4 through 30.</td>
</tr>
</tbody>
</table>

**Command Modes**

Crypto ISAKMP group configuration (config-isakmp-group)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows that the IP address of the DHCP server is 10.2.3.4 and that the time to wait until the next DHCP server on the list is tried is 6 seconds:

```
Router (config)# crypto isakmp client configuration group home
Router (config-isakmp-group)# dhcp server 10.2.3.4
Router (config-isakmp-group)# key abcd
Router (config-isakmp-group)# dhcp timeout 6
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto isakmp client configuration group</td>
<td>Specifies to which group a policy profile will be defined.</td>
</tr>
</tbody>
</table>
dialer aaa

To allow a dialer to access the authentication, authorization, and accounting (AAA) server for dialing information, use the dialer aaa command in interface configuration mode. To disable this function, use the no form of this command.

`dialer aaa [ { password string | suffix string } ]`

`no dialer aaa [ { password string | suffix string } ]`

**Syntax Description**

| password string | (Optional) Defines a nondefault password for authentication. The password string can be a maximum of 128 characters. |
| suffix string | (Optional) Defines a suffix for authentication. The suffix string can be a maximum of 64 characters. |

**Command Default**

This feature is not enabled by default.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(3)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(5)T</td>
<td>The password and <strong>suffix</strong> keywords were added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is required for large scale dial-out and Layer 2 Tunneling Protocol (L2TP) dial-out functionality. With this command, you can specify a suffix, a password, or both. If you do not specify a password, the default password will be “cisco.”

**Note**

Only IP addresses can be specified as usernames for the **dialer aaa suffix** command.

**Examples**

This example shows a user sending out packets from interface Dialer1 with a destination IP address of 10.1.1.1. The username in the access-request message is “10.1.1.1@ciscoDoD” and the password is “cisco.”

```bash
interface dialer1
dialer aaa
dialer aaa suffix @ciscoDoD password cisco
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>accept dialout</td>
<td>Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup.</td>
</tr>
<tr>
<td></td>
<td>dialer congestion-threshold</td>
<td>Specifies congestion threshold in connected links.</td>
</tr>
<tr>
<td></td>
<td>dialer vpdn</td>
<td>Enables a Dialer Profile or DDR dialer to use L2TP dial-out.</td>
</tr>
</tbody>
</table>
diameter origin host

To configure the fully qualified domain name (FQDN) of the host of a Diameter node, use the `diameter origin host` command in global configuration mode. To disable the configured FQDN, use the `no` form of this command.

```
diameter origin host string
no diameter origin host string
```

**Syntax Description**

| String | Character string that describes the FQDN for a specific Diameter node. |

**Command Default**

No realm is configured.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Because there is no host configured by default, it is mandatory to configure this information. The origin host information is sent in requests to a Diameter peer. Global Diameter protocol parameters are used if Diameter parameters have not been defined at a Diameter peer level.

**Examples**

The following example shows how to configure a Diameter origin host:

```
Router(config)# diameter origin host
host1.example.com.
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diameter origin realm</td>
<td>Configures origin realm information for a Diameter node.</td>
</tr>
<tr>
<td>diameter peer</td>
<td>Defines a Diameter peer and enters Diameter peer configuration mode.</td>
</tr>
</tbody>
</table>
diameter origin realm

To configure origin realm information for a Diameter node, use the `diameter origin realm` command in global configuration mode. To disable the configured realm information, use the `no` form of this command.

```
diameter origin realm string
no diameter origin realm string
```

**Syntax Description**
- `string`: Character string that describes the realm information for a specific Diameter node.

**Command Default**
No realm is configured.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Because there is no realm configured by default, it is mandatory to configure this information. Origin realm information is sent in requests to a Diameter peer.

**Examples**
The following example shows how to configure a Diameter origin realm:

```
Router (config)# diameter origin realm example.com
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diameter origin host</td>
<td>Configures the FQDN of the host of a Diameter node.</td>
</tr>
<tr>
<td>diameter peer</td>
<td>Defines a Diameter peer and enters Diameter peer configuration mode.</td>
</tr>
</tbody>
</table>
**diameter peer**

To configure a device as a Diameter Protocol peer and enter the Diameter peer configuration submode, use the *diameter peer* command in global configuration mode. To disable Diameter Protocol configuration for a peer, use the *no* form of this command.

```
diameter peer name
no diameter peer name
```

**Syntax Description**

- *name*  
  Character string used to name the peer node to be configured for the Diameter Credit Control Application (DCCA).

**Command Default**

No Diameter peer is configured.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command enables the Diameter peer configuration submode. From the submode, you can configure other DCCA parameters. The configuration is applied when you exit the submode.

**Examples**

The following example shows how to configure a Diameter peer:

```
Router (config)# diameter peer
  dia_peer_1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address ipv4</td>
<td>Defines a route to the host of the Diameter peer using IPv4.</td>
</tr>
<tr>
<td>destination host</td>
<td>Configures the FQDN of a Diameter peer.</td>
</tr>
<tr>
<td>destination realm</td>
<td>Configures the destination realm in which a Diameter peer is located.</td>
</tr>
<tr>
<td>ip vrf forwarding</td>
<td>Associates a VRF with a Diameter peer.</td>
</tr>
<tr>
<td>security ipsec</td>
<td>Configures IPSec as the security protocol for the Diameter peer-to-peer connection.</td>
</tr>
<tr>
<td>show diameter peer</td>
<td>Displays the Diameter peer configuration.</td>
</tr>
<tr>
<td>source interface</td>
<td>Configures the interface to connect to the Diameter peer.</td>
</tr>
<tr>
<td>timer</td>
<td>Configures Diameter base protocol timers for peer-to-peer communication.</td>
</tr>
<tr>
<td>transport {tcp} port</td>
<td>Configures the transport protocol for connections to the Diameter peer.</td>
</tr>
</tbody>
</table>
**diameter redundancy**

To enable the Diameter node to be a Cisco IOS Redundancy Facility (RF) client and track session states, use the `diameter redundancy` command in global configuration mode. To disable this feature, use the `no` form of this command.

```
diameter redundancy
no diameter redundancy
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Diameter redundancy is not configured.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you configure Diameter redundancy on a device, that device will not initiate any TCP connection while it is a standby node. Upon transition to active status, the device initiates a TCP connection to the Diameter peer.

**Note**

This command is required for service-aware Packet Data Protocol (PDP) session redundancy. For more information about service-aware PDP session redundancy, see the “GTP-Session Redundancy for Service-Aware PDPs Overview” section of the *Cisco GGSN Release 5.2 Configuration Guide*.

**Examples**

The following example shows how to configure Diameter redundancy:

```
Router (config)# diameter redundancy
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>diameter origin host</code></td>
<td>Configures the FQDN of the host of this Diameter node.</td>
</tr>
<tr>
<td><code>diameter origin realm</code></td>
<td>Configures the realm of origin in which this Diameter node is located.</td>
</tr>
<tr>
<td><code>diameter timer</code></td>
<td>Configures Diameter base protocol timers to use if none have been configured at the Diameter peer level.</td>
</tr>
<tr>
<td><code>diameter vendor support</code></td>
<td>Configures a Diameter node to advertise the vendor AVPs it supports in capability exchange messages with Diameter peers.</td>
</tr>
</tbody>
</table>
**diameter timer**

To set either the frequency of transport connection attempts or the interval for sending watchdog messages, use the `diameter timer` command in global configuration mode. To return to the default values, use the `no` form of this command.

```
diameter timer {connection|transaction|watch-dog} value
no diameter timer {connection|transaction|watch-dog} value
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connection</td>
<td>Maximum interval, in seconds, for the Gateway General Packet Radio Service (GPRS) Support Node (GGSN) to attempt reconnection to a Diameter peer after being disconnected due to a transport failure. The range is from 1 to 1000. The default is 30. A value of 0 configures the GGSN not to attempt reconnection.</td>
</tr>
<tr>
<td>transaction</td>
<td>Maximum interval, in seconds, the GGSN waits for a Diameter peer to respond before trying another peer. The range is from 1 to 1000. The default is 30.</td>
</tr>
<tr>
<td>watch-dog</td>
<td>Maximum interval, in seconds, the GGSN waits for a Diameter peer response to a watchdog packet. The range is from 1 to 1000. The default is 30. <strong>Note</strong> When the watchdog timer expires, a device watchdog request (DWR) is sent to the Diameter peer and the watchdog timer is reset. If a device watchdog answer (DWA) is not received before the next expiration of the watchdog timer, a transport failure to the Diameter peer has occurred.</td>
</tr>
<tr>
<td>value</td>
<td>The valid range, in seconds, from 1 to 1000. The default is 30.</td>
</tr>
</tbody>
</table>

**Command Default**

The default value for each timer is 30 seconds.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When configuring timers, the value for the transaction timer should be larger than the transmission-timeout value, and, on the Serving GPRS Support Node (SGSN), the values configured for the number of GPRS Tunneling Protocol (GTP) N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, Diameter Credit Control Application (DCCA), and Cisco Content Services Gateway (CSG)). Specifically, the SGSN N3*T3 must be greater than 2 x RADIUS timeout + N x DCCA timeout + CSG timeout where:

- The factor 2 is for both authentication and accounting.
- The value N is for the number of Diameter servers configured in the server group.

**Examples**

The following examples show how to configure the Diameter timers:
Router config# diameter timer connection 20
Router config# diameter timer watch-dog 25

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa group server diameter</td>
<td>Defines a Diameter AAA server group.</td>
</tr>
<tr>
<td></td>
<td>diameter peer</td>
<td>Configures a Diameter peer and enters Diameter peer configuration submode.</td>
</tr>
<tr>
<td></td>
<td>timer</td>
<td>Configures the Diameter base protocol timers for a Diameter peer.</td>
</tr>
</tbody>
</table>
diameter vendor supported

To configure a Diameter node to advertise the vendor-specific attribute value pairs (AVPs) it recognizes, use the `diameter vendor supported` command in global configuration mode. To remove the supported vendor configuration, use the `no` form of this command.

```
diameter vendor supported {Cisco|3gpp|Vodafone}
no diameter vendor supported {Cisco|3gpp|Vodafone}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Cisco</th>
<th>Configures the Diameter node to advertise support for the Cisco-specific AVPs.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3gpp</td>
<td>Configures the Diameter node to advertise support for the AVPs that support the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Third-Generation Partnership Project (3GPP).</td>
</tr>
<tr>
<td></td>
<td>Vodafone</td>
<td>Configures the Diameter node to advertise support for the Vodafone-specific AVPs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>No vendor identifier is configured.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Global configuration</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

| Usage Guidelines   | Individual vendors can define AVPs specific to their implementation of the Diameter Credit Control Application (DCCA), or for individual applications. You can configure multiple instances of this command, as long as each instance has a different vendor identifier. |

<table>
<thead>
<tr>
<th>Examples</th>
<th>The following example shows how to configure DCCA to advertise support for a the Cisco-specific AVPs:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Router (config)# diameter vendor supported Cisco</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>diameter origin host</td>
<td>Configures the FQDN of the host of this Diameter node.</td>
</tr>
<tr>
<td></td>
<td>diameter origin realm</td>
<td>Configures the realm of origin in which this Diameter node is located.</td>
</tr>
<tr>
<td></td>
<td>diameter redundancy</td>
<td>Enables the Diameter node to be a Cisco IOS RF client and track session states.</td>
</tr>
<tr>
<td></td>
<td>diameter timer</td>
<td>Configures Diameter base protocol timers to use if none have been configured at the Diameter peer level.</td>
</tr>
</tbody>
</table>
disable open-media-channel

To prevent the creation of Real-time Transport Protocol (RTP) or RTP Control (RTCP) media channels when a Session Initiation Protocol (SIP) class map is used for SIP inspection, use the `disable open-media-channel` command in parameter-map type configuration mode. To enable the creation of RTP or RTCP media channels, use the `no` form of this command or remove this parameter map from the inspect action.

```
disable open-media-channel
no disable open-media-channel
```

### Syntax Description
This command has no arguments or keywords.

### Command Default
RTP and RTCP media channels are opened by the SIP inspection process.

### Command Modes
Parameter-map type configuration (config-profile)

### Command History
- **Release** 15.0(1)M
  - This command was introduced.

### Usage Guidelines
Cisco IOS Firewall Trust Relay Point (TRP) support enables Cisco IOS Firewall to process Simple Traversal of User Datagram Protocol (UDP) (STUN) messages. The STUN messages open ports (pinholes) for secondary channels (RTP and RTCP), which are necessary for implementation of TRPs in voice networks.

Cisco IOS Firewall supports partial SIP inspection that allows the SIP Application-level Gateway (ALG) to parse the SIP message in a packet to check for protocol conformance.

To configure partial SIP inspection in voice networks, you must use the `disable open-media-channel` command to configure SIP ALG so that it does not open pinholes for media information found in the SDP message.

When Cisco IOS TRP is used in voice network for firewall traversal, Partial SIP-ALG (enabled when this parameter map is attached to the inspect action) provides security for SIP control channel and STUN with Cisco Flow data (CFD) provides security for the RTP and RTCP channels. If Partial SIP-ALG is not used, the normal SIP-ALG will open RTP and RTCP channels by itself.

### Examples
The following example shows how to create a parameter map that does not open a media channel when attached to a SIP class map:

```
Router(config)# parameter-map type protocol-info sip pmap-sip
Router(config-profile)# disable open-media-channel
```

### Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>parameter-map type protocol-info</td>
<td>Creates or modifies a protocol-specific parameter map and enters parameter-map type configuration mode.</td>
</tr>
</tbody>
</table>
disconnect ssh

To terminate a Secure Shell (SSH) connection on your router, use the `disconnect ssh` command in privileged EXEC mode.

```
disconnect ssh [vty] session-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vty</td>
<td>(Optional) Virtual terminal for remote console access.</td>
</tr>
<tr>
<td>session-id</td>
<td>The session-id is the number of connection displayed in the <code>show ip ssh</code> command output.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(1)T</td>
<td>This command was integrated into Cisco IOS Release 12.1 T.</td>
</tr>
<tr>
<td>12.2(17a)SX</td>
<td>This command was integrated into Cisco IOS Release 12.2(17a)SX.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `clear line vty n` command, where `n` is the connection number displayed in the `show ip ssh` command output, may be used instead of the `disconnect ssh` command.

When the EXEC connection ends, whether normally or abnormally, the SSH connection also ends.

**Examples**

The following example terminates SSH connection number 1:

```
disconnect ssh 1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear line vty</td>
<td>Returns a terminal line to idle state using the privileged EXEC command.</td>
</tr>
</tbody>
</table>
**dn**

To associate the identity of a router with the distinguished name (DN) in the certificate of the router, use the dn command in crypto identity configuration mode. To remove this command from your configuration, use the no form of this command.

```
dn name=string [, name=string]
no dn name=string [, name=string]
```

**Syntax Description**

- `name string`: Identity used to restrict access to peers with specific certificates. Optionally, you can associate more than one identity.

**Command Default**

If this command is not enabled, the router can communicate with any encrypted interface that is not restricted on its IP address.

**Command Modes**

Crypto identity configuration (crypto-identity)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXD.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the dn command to associate the identity of the router, which is defined in the crypto identity command, with the DN that the peer used to authenticate itself.

**Note**

The name defined in the crypto identity command must match the `string` defined in the dn command. That is, the identity of the peer must be the same as the identity in the exchanged certificate.

This command allows you set restrictions in the router configuration that prevent those peers with specific certificates, especially certificates with particular DNs, from having access to selected encrypted interfaces.

An encrypting peer matches this list if it contains the attributes listed in any one line defined within the `name=string`.

**Examples**

The following example shows how to configure an IPsec crypto map that can be used only by peers that have been authenticated by the DN and if the certificate belongs to “green”:

```
crypto map map-to-green 10 ipsec-isakmp
set peer 172.21.114.196
set transform-set my-transformset
match address 124
identity to-green
```
crypto identity to-green
dn ou=green

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>crypto identity</td>
<td>Configures the identity of the router with a given list of DN in the certificate of the router.</td>
</tr>
<tr>
<td></td>
<td>fqdn</td>
<td>Associates the identity of the router with the hostname that the peer used to authenticate itself.</td>
</tr>
</tbody>
</table>
dn (IKEv2)

To enable and derive an IKEv2 name mangler from identity of type distinguished name (DN), use the `dn` command in IKEv2 name mangler configuration mode. To remove the name derived from DN, use the `no` form of this command.

```
   dn  {common-name|country|domain|locality|organization|organization-unit|state}
   no dn
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>common-name</td>
<td>Derives the name mangler from the common name portion in the DN.</td>
</tr>
<tr>
<td>country</td>
<td>Derives the name mangler from the country portion in the DN.</td>
</tr>
<tr>
<td>domain</td>
<td>Derives the name mangler from the domain portion in the DN.</td>
</tr>
<tr>
<td>locality</td>
<td>Derives the name mangler from the locality portion in the DN.</td>
</tr>
<tr>
<td>organization</td>
<td>Derives the name mangler from the organization portion in the DN.</td>
</tr>
<tr>
<td>organization-unit</td>
<td>Derives the name mangler from the organization-unit portion in the DN.</td>
</tr>
<tr>
<td>state</td>
<td>Derives the name mangler from the state portion in the DN.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

IKEv2 name mangler configuration (config-ikev2-name-mangler)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(3)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to derive the name mangler from any field in the remote identity of type DN.

**Examples**

The following example shows how to derive a name for the name mangler from the country field of the DN:

```
Router(config)# crypto ikev2 name-mangler mangler2
Router(config-ikev2-name-mangler)# dn country
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2 name mangler</td>
<td>Defines a name mangler.</td>
</tr>
</tbody>
</table>
**dnis (AAA preauthentication)**

To preauthenticate calls on the basis of the Dialed Number Identification Service (DNIS) number, use the `dnis` command in AAA preauthentication configuration mode. To remove the `dnis` command from your configuration, use the `no` form of this command.

```
dnis [ { if-avail | required } ] [ accept-stop ] [ password string ]
no dnis [ { if-avail | required } ] [ accept-stop ] [ password string ]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>if-avail</code></td>
<td>(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.</td>
</tr>
<tr>
<td><code>required</code></td>
<td>(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.</td>
</tr>
<tr>
<td><code>accept-stop</code></td>
<td>(Optional) Prevents subsequent preauthentication elements from being tried once preauthentication has succeeded for a call element.</td>
</tr>
<tr>
<td><code>password string</code></td>
<td>(Optional) Password to use in the Access-Request packet. The default is <code>cisco</code>.</td>
</tr>
</tbody>
</table>

**Command Default**

The `if-avail` and `required` keywords are mutually exclusive. If the `if-avail` keyword is not configured, the preauthentication setting defaults to `required`.

The default password string is `cisco`.

**Command Modes**

AAA preauthentication configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You may configure more than one of the AAA preauthentication commands (`clid`, `ctype`, `dnis`) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure `dnis`, then `clid`, then `ctype`, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

**Examples**

The following example enables DNIS preauthentication using a RADIUS server and the password Ascend-DNIS:

```
aaa preauth
group radius
dnis password Ascend-DNIS
```
The following example specifies that incoming calls be preauthenticated on the basis of the DNIS number:

```
aaa preauth
group radius
dnis required
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa preauth</td>
<td>Enters AAA preauthentication mode.</td>
</tr>
<tr>
<td>clid</td>
<td>Preauthenticates calls on the basis of the CLID number.</td>
</tr>
<tr>
<td>ctype</td>
<td>Preauthenticates calls on the basis of the call type.</td>
</tr>
<tr>
<td>dnis bypass (AAA preauthentication configuration)</td>
<td>Specifies a group of DNIS numbers that will be bypassed for preauthentication.</td>
</tr>
<tr>
<td>group (authentication)</td>
<td>Selects the security server to use for AAA preauthentication.</td>
</tr>
<tr>
<td>isdn guard-timer</td>
<td>Sets a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.</td>
</tr>
</tbody>
</table>
**dnis (RADIUS)**

To preauthenticate calls on the basis of the DNIS (Dialed Number Identification Service) number, use the `dnis` command in AAA preauthentication configuration mode. To remove the `dnis` command from your configuration, use the `no` form of this command.

```
dnis [if-avail|required] [accept-stop] [password  password]
no dnis [if-avail|required] [accept-stop] [password  password]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>if-avail</td>
<td>(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.</td>
</tr>
<tr>
<td>required</td>
<td>(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.</td>
</tr>
<tr>
<td>accept-stop</td>
<td>(Optional) Prevents subsequent preauthentication elements such as clid or ctype from being tried once preauthentication has succeeded for a call element.</td>
</tr>
<tr>
<td>password password</td>
<td>(Optional) Defines the password for the preauthentication element.</td>
</tr>
</tbody>
</table>

**Command Default**

The `if-avail` and `required` keywords are mutually exclusive. If the `if-avail` keyword is not configured, the preauthentication setting defaults to `required`.

The default password string is cisco.

**Command Modes**

AAA preauthentication configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You may configure more than one of the authentication, authorization, and accounting (AAA) preauthentication commands (`clid`, `ctype`, `dnis`) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure `dnis`, then `clid`, then `ctype`, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.
Examples

The following example specifies that incoming calls be preauthenticated on the basis of the DNIS number:

aaa preauth
group radius
dnis required

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clid</td>
<td>Preauthenticates calls on the basis of the CLID number.</td>
</tr>
<tr>
<td>ctype</td>
<td>Preauthenticates calls on the basis of the call type.</td>
</tr>
<tr>
<td>dnis bypass (AAA preauthentication configuration)</td>
<td>Specifies a group of DNIS numbers that will be bypassed for preauthentication.</td>
</tr>
<tr>
<td>group (RADIUS)</td>
<td>Specifies the AAA RADIUS server group to use for preauthentication.</td>
</tr>
</tbody>
</table>
**dnis bypass (AAA preauthentication configuration)**

To specify a group of DNIS (Dialed Number Identification Service) numbers that will be bypassed for preauthentication, use the `dnis bypass` command in AAA preauthentication configuration mode. To remove the `dnis bypass` command from your configuration, use the `no` form of this command.

```
dnis bypass dnis-group-name
no dnis bypass dnis-group-name
```

**Syntax Description**

| `dnis-group-name` | Name of the defined DNIS group. |

**Command Default**

No DNIS numbers are bypassed for preauthentication.

**Command Modes**

AAA preauthentication configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before using this command, you must first create a DNIS group with the `dialer dnis group` command.

**Examples**

The following example specifies that preauthentication be performed on all DNIS numbers except for two DNIS numbers (12345 and 12346), which have been defined in the DNIS group called hawaii:

```
aaa preauth
group radius
dnis required
dnis bypass hawaii
dialer dnis group hawaii
driver dnis group hawaii
number 12345
number 12346
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dialer dnis group</code></td>
<td>Creates a DNIS group.</td>
</tr>
<tr>
<td><code>dnis (RADIUS)</code></td>
<td>Preauthenticates calls on the basis of the DNIS number.</td>
</tr>
</tbody>
</table>
To specify the primary and secondary Domain Name Service (DNS) servers, use the `dns` command in ISAKMP group configuration mode or IKEv2 authorization policy configuration mode. To remove this command from your configuration, use the `no` form of this command.

```
[[ipv6]] dns primary-server [secondary-server]
no [[ipv6]] dns primary-server [secondary-server]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6</code></td>
<td>(Optional) Specifies an IPv6 address for the DNS server. To specify an IPv4 address, execute the command without this keyword.</td>
</tr>
<tr>
<td><code>primary-server</code></td>
<td>Name of the primary DNS server.</td>
</tr>
<tr>
<td><code>secondary-server</code></td>
<td>(Optional) Name of the secondary DNS server.</td>
</tr>
</tbody>
</table>

**Command Default**

A DNS server is not specified.

**Command Modes**

ISAKMP group configuration (config-isakmp-group)
IKEv2 authorization policy configuration (config-ikev2-author-policy)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
<tr>
<td>15.2(1)T</td>
<td>This command was modified. The <code>ipv6</code> keyword was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `dns` command to specify the primary and secondary DNS servers for the group.

You must enable the following commands before enabling the `dns` command:

- `crypto isakmp client configuration group` -- Specifies the group policy information that has to be defined or changed.
- `crypto ikev2 authorization policy` -- Specifies the local group policy authorization parameters.

**Examples**

The following example shows how to define a primary and secondary DNS server for the default group name:

```
crypto isakmp client configuration group default
  key cisco
dns 10.2.2.2 10.3.2.3
pool dog
acl 199
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl</td>
<td>Configures split tunneling.</td>
</tr>
<tr>
<td>crypto ikev2 authorization policy</td>
<td>Specifies an IKEv2 authorization policy.</td>
</tr>
<tr>
<td>crypto isakmp client configuration group</td>
<td>Specifies the policy profile of the group that will be defined.</td>
</tr>
<tr>
<td>domain (isakmp-group)</td>
<td>Specifies the DNS domain to which a group belongs.</td>
</tr>
</tbody>
</table>
dnsix-dmdp retries through dynamic

- dnsix-dmdp retries, on page 129
- dnsix-nat authorized-redirection, on page 130
- dnsix-nat primary, on page 131
- dnsix-nat secondary, on page 132
- dnsix-nat source, on page 133
- dnsix-nat transmit-count, on page 134
- dns-timeout, on page 135
- domain (AAA), on page 136
- domain (isakmp-group), on page 138
- domain-stripping, on page 139
- dot1x control-direction, on page 141
- dot1x credentials, on page 144
- dot1x critical (global configuration), on page 145
- dot1x critical (interface configuration), on page 146
- dot1x default, on page 147
- dot1x guest-vlan, on page 149
- dot1x guest-vlan supplicant, on page 151
- dot1x host-mode, on page 152
- dot1x initialize, on page 154
- dot1x mac-auth-bypass, on page 155
- dot1x max-reauth-req, on page 157
- dot1x max-req, on page 159
- dot1x max-start, on page 162
- dot1x multi-hosts, on page 164
- dot1x multiple-hosts, on page 165
- dot1x pae, on page 167
- dot1x port-control, on page 169
- dot1x re-authenticate (EtherSwitch), on page 172
- dot1x re-authenticate (privileged EXEC), on page 173
- dot1x reauthentication, on page 175
- dot1x re-authentication (EtherSwitch), on page 178
- dot1x supplicant interface, on page 179
- dot1x system-auth-control, on page 180
• dot1x timeout, on page 182
• dot1x timeout (EtherSwitch), on page 187
• dpd, on page 189
• drop (type access-control), on page 190
• drop (zone-based policy), on page 192
• drop-unsecure, on page 194
• dtls port, on page 195
• dynamic, on page 196
**dnsix-dmdp retries**

To set the retransmit count used by the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) Message Delivery Protocol (DMDP), use the `dnsix-dmdp retries` command in global configuration mode. To restore the default number of retries, use the `no` form of this command.

```
dnsix-dmdp retries count
no dnsix-dmdp retries count
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>count</code></td>
<td>Number of times DMDP will retransmit a message. It can be an integer from 0 to 200. The default is 4 retries, or until acknowledged.</td>
</tr>
</tbody>
</table>

**Command Default**

Retransmits messages up to 4 times, or until acknowledged.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Examples**

The following example sets the number of times DMDP will attempt to retransmit a message to 150:

```
dnsix-dmdp retries 150
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dnsix-nat authorized-redirection</code></td>
<td>Specifies the address of a collection center that is authorized to change the primary and secondary addresses of the host to receive audit messages.</td>
</tr>
<tr>
<td><code>dnsix-nat primary</code></td>
<td>Specifies the IP address of the host to which DNSIX audit messages are sent.</td>
</tr>
<tr>
<td><code>dnsix-nat secondary</code></td>
<td>Specifies an alternate IP address for the host to which DNSIX audit messages are sent.</td>
</tr>
<tr>
<td><code>dnsix-nat source</code></td>
<td>Starts the audit-writing module and defines audit trail source address.</td>
</tr>
<tr>
<td><code>dnsix-nat transmit-count</code></td>
<td>Causes the audit-writing module to collect multiple audit messages in the buffer before sending the messages to a collection center.</td>
</tr>
</tbody>
</table>
**dnsix-nat authorized-redirection**

To specify the address of a collection center that is authorized to change the primary and secondary addresses of the host to receive audit messages, use the `dnsix-nat authorized-redirection` command in global configuration mode. To delete an address, use the `no` form of this command.

```
dnsix-nat authorized-redirection ip-address
no dnsix-nat authorized-redirection ip-address
```

**Syntax Description**

| `ip-address` | IP address of the host from which redirection requests are permitted. |

**Command Default**

An empty list of addresses.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use multiple `dnsix-nat authorized-redirection` commands to specify a set of hosts that are authorized to change the destination for audit messages. Redirection requests are checked against the configured list, and if the address is not authorized the request is rejected and an audit message is generated. If no address is specified, no redirection messages are accepted.

**Examples**

The following example specifies that the address of the collection center that is authorized to change the primary and secondary addresses is 192.168.1.1:

```
dnsix-nat authorization-redirection 192.168.1.1
```
To specify the IP address of the host to which Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit messages are sent, use the `dnsix-nat primary` command in global configuration mode. To delete an entry, use the `no` form of this command.

```
dnsix-nat primary ip-address
no dnsix-nat primary ip-address
```

**Syntax Description**
- `[ip-address]` IP address for the primary collection center.

**Command Default**
Messages are not sent.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
An IP address must be configured before audit messages can be sent.

**Examples**
The following example configures an IP address as the address of the host to which DNSIX audit messages are sent:

```
dnsix-nat primary 172.16.1.1
```
To specify an alternate IP address for the host to which Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit messages are sent, use the `dnsix-nat secondary` command in global configuration mode. To delete an entry, use the `no` form of this command.

```
dnsix-nat secondary ip-address
no dnsix-nat secondary ip-address
```

**Syntax Description**

| `ip-address` | IP address for the secondary collection center. |

**Command Default**

No alternate IP address is known.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the primary collection center is unreachable, audit messages are sent to the secondary collection center instead.

**Examples**

The following example configures an IP address as the address of an alternate host to which DNSIX audit messages are sent:

```
dnsix-nat secondary 192.168.1.1
```
**dnsix-nat source**

To start the audit-writing module and to define the audit trail source address, use the `dnsix-nat source` command in global configuration mode. To disable the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit trail writing module, use the `no` form of this command.

```
dnsix-nat source ip-address
no dnsix-nat source ip-address
```

**Syntax Description**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-address</strong></td>
<td>Source IP address for DNSIX audit messages.</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must issue the `dnsix-nat source` command before any of the other `dnsix-nat` commands. The configured IP address is used as the source IP address for DMDP protocol packets sent to any of the collection centers.

**Examples**

The following example enables the audit trail writing module, and specifies that the source IP address for any generated audit messages should be the same as the primary IP address of Ethernet interface 0:

```
dnsix-nat source 192.168.2.5
interface ethernet 0
  ip address 192.168.2.5 255.255.255.0
```
**dnsix-nat transmit-count**

To have the audit writing module collect multiple audit messages in the buffer before sending the messages to a collection center, use the `dnsix-nat transmit-count` command in global configuration mode. To revert to the default audit message count, use the `no` form of this command.

```
dnsix-nat transmit-count count
no dnsix-nat transmit-count count
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>count</code></td>
<td>Number of audit messages to buffer before transmitting to the server. It can be an integer from 1 to 200.</td>
</tr>
</tbody>
</table>

**Command Default**

One message is sent at a time.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An audit message is sent as soon as the message is generated by the IP packet-processing code. The audit writing module can, instead, buffer up to several audit messages before transmitting to a collection center.

**Examples**

The following example configures the system to buffer five audit messages before transmitting them to a collection center:

```
dnsix-nat transmit-count 5
```
dns-timeout

To specify the Domain Name System (DNS) idle timeout (the length of time for which a DNS lookup session will continue to be managed while there is no activity), use the `dns-timeout` command in parameter-map type inspect configuration mode. To disable the timeout, use the `no` form of this command.

```
dns-timeout  seconds
no dns-timeout  seconds
```

**Syntax Description**

| seconds | Length of time, in seconds, for which a DNS name lookup session will still be managed while there is no activity. The default is 5. |

**Command Default**
The DNS idle timeout is disabled.

**Command Modes**
Parameter-map type inspect configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can use the `dns-timeout` subcommand when you are creating an inspect type parameter map. You can enter the `dns-timeout` subcommand after you enter the `parameter-map type inspect` command.

Use the `dns-timeout` command if you have DNS inspection configured and want to control the timeout of DNS sessions.

If DNS inspection is not configured, but you enter the `dns-timeout` command, the command does not take effect (that is, it is not applied to a DNS session).

For more detailed information about creating a parameter map, see the `parameter-map type inspect` command.

**Examples**

The following example specifies that if there is no activity, a DNS lookup session will continue to be managed for 25 seconds:

```
parameter-map type inspect insp-params
dns-timeout 25
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip inspect dns-timeout</code></td>
<td>Specifies the DNS idle timeout (the length of time during which a DNS name lookup session will still be managed while there is no activity).</td>
</tr>
<tr>
<td><code>parameter-map type inspect</code></td>
<td>Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect action.</td>
</tr>
</tbody>
</table>
domain (AAA)

To configure username domain options for the RADIUS application, use the `domain` command in dynamic authorization local server configuration mode. To disable the username domain options configured, use the `no` form of this command.

```
domain {delimiter character|stripping [right-to-left]}
no domain {delimiter character|stripping [right-to-left]}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>delimiter character</code></td>
<td>Specifies the domain delimiter. One of the following options can be specified: @, /, $, %, , # or -</td>
</tr>
<tr>
<td><code>stripping</code></td>
<td>Compares the incoming username with the names oriented to the left of the @ domain delimiter.</td>
</tr>
<tr>
<td><code>right-to-left</code></td>
<td>Terminates the string at the first delimiter going from right to left.</td>
</tr>
</tbody>
</table>

**Command Default**

No username domain options are configured.

**Command Modes**

Dynamic authorization local server configuration (config-locsvr-da-radius)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(31)SB14</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRC5</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRC5.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.3</td>
<td>This command was modified. This command was implemented on ASR 1000 series routers.</td>
</tr>
<tr>
<td>15.1(2)T</td>
<td>This command was integrated into Cisco IOS Release 15.1(2)T. This command was also modified. The <code>right-to-left</code> keyword was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If domain stripping is not configured, the full username provided in the authentication, authorization, and accounting (AAA) packet of disconnect (POD) messages is compared with the online subscribers. Configuring domain stripping allows you to send disconnect messages with only the username present before the @ domain delimiter. The network access server (NAS) compares and matches this username with any online subscriber with a potential domain.

For instance, when domain stripping is configured and you send a POD message with the username “test,” a comparison between the POD message and online subscribers takes place, and subscribers with the username “test@cisco.com” or “test” match the specified username “test.”

**Examples**

The following configuration example is used to match a username from right to left. If the username is user1@cisco.com@test.com, then the username to be matched by the POD message is user1@cisco.com.

```
Router# configure terminal
```
Router(config)# aaa server radius dynamic-author
Router(config-locsvr-da-radius)# domain stripping right-to-left
Router(config-locsvr-da-radius)# domain delimiter @
Router(config-locsvr-da-radius)# end

The following configuration example is used to match a username from left to right. If the username is user1@cisco.com@test.com, then the username to be matched by the POD message is user1.

Router# configure terminal
Router(config)# aaa server radius dynamic-author
Router(config-locsvr-da-radius)# domain stripping
Router(config-locsvr-da-radius)# domain delimiter @
Router(config-locsvr-da-radius)# end

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa server radius dynamic-author</td>
<td>Configures a device as a AAA server to facilitate interaction with an external policy server.</td>
</tr>
</tbody>
</table>
domain (isakmp-group)

To specify the Domain Name Service (DNS) domain to which a group belongs, use the `domain` command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove this command from your configuration, use the `no` form of this command.

```
domain name
no domain name
```

**Syntax Description**
- `name`: Name of the DNS domain.

**Command Default**
A DNS domain is not specified.

**Command Modes**
ISAKMP group configuration (config-isakmp-group)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `domain` command to specify group domain membership.

You must enable the `crypto isakmp configuration group` command, which specifies group policy information that has to be defined or changed, before enabling the `domain` command.

**Examples**
The following example shows that members of the group “cisco” also belong to the domain “cisco.com”:

```
crypto isakmp client configuration group cisco
    key cisco
    dns 10.2.2.2 10.3.2.3
    pool dog
    acl 199
    domain cisco.com
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl</td>
<td>Configures split tunneling.</td>
</tr>
<tr>
<td>crypto isakmp client configuration group</td>
<td>Specifies the DNS domain to which a group belongs.</td>
</tr>
<tr>
<td>crypto isakmp keepalive</td>
<td>Specifies the primary and secondary DNS servers.</td>
</tr>
</tbody>
</table>
domain-stripping

To configure domain stripping at the server group level, use the `domain-stripping` command in server group RADIUS configuration mode. To disable the configuration, use the `no` form of this command.

```
domain-stripping [strip-suffix word] [right-to-left] [prefix-delimiter word] [delimiter word]
no domain-stripping [strip-suffix word] [right-to-left] [prefix-delimiter word] [delimiter word]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>strip-suffix</th>
<th>(Optional) Configures the suffix, which needs to be stripped.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>word</td>
<td>(Optional) Suffix that needs to be stripped.</td>
</tr>
<tr>
<td></td>
<td>right-to-left</td>
<td>(Optional) Terminates the string at the first delimiter going from right to left.</td>
</tr>
<tr>
<td></td>
<td>prefix-delimiter</td>
<td>(Optional) Configures a set of prefix delimiters.</td>
</tr>
<tr>
<td></td>
<td>delimiter</td>
<td>(Optional) Configures a set of suffix delimiters.</td>
</tr>
</tbody>
</table>

**Command Default**
Stripping is disabled. The entire username (including the domain name) is sent to the RADIUS server.

**Command Modes**
Server group RADIUS configuration (config-sg-radius)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.4S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(3)T</td>
<td>This command was integrated into Cisco IOS Release 15.2(3)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `radius-server domain-stripping` command to remove the domain name from the username received at the global level. All authentication, authorization, and accounting (AAA) requests with “user@example.com” will go to the remote RADIUS server with the reformatted username “user.” The domain name is removed from the request.

Use the `domain-stripping` command to configure domain stripping at the server group level. Per-server group configuration will override the global configuration. That is, if domain stripping is not enabled globally but enabled in the server group, it is enabled only for that server group. Also, if virtual routing and forwarding (VRF)-specific domain stripping is configured globally and in the server group for a different VRF, domain stripping is enabled in both the VRFs. After domain stripping and broadcast accounting are configured, you can create separate accounting records as per the configurations.

**Examples**

The following example shows how to configure domain stripping at the server group level:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius rad1
Device(config-sg-radius)# domain-stripping right-to-left delimiter @$/
Device(config-sg-radius)# end
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>aaa group server radius</strong></td>
<td>Adds the RADIUS server group.</td>
</tr>
</tbody>
</table>
dot1x control-direction

Note
Effective with Cisco IOS Release 12.2(33)SXI, the dot1x control-direction command is replaced by the authentication control-direction command. See the authentication control-direction command for more information.

To change an IEEE 802.1X controlled port to unidirectional or bidirectional, use the dot1x control-direction command in interface configuration mode. To return to the default setting, use the no form of this command.

dot1x control-direction {both|in}

no dot1x control-direction

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>both</td>
<td>Enables bidirectional control on the port.</td>
</tr>
<tr>
<td>in</td>
<td>Enables unidirectional control on the port.</td>
</tr>
</tbody>
</table>

Command Default
The port is set to bidirectional mode.

Command Modes
Interface configuration (config-if)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(25)SEC</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(6)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(6)T.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td>This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Switches (ISRs) only.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was replaced by the authentication control-direction command.</td>
</tr>
</tbody>
</table>

Usage Guidelines
The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

Unidirectional State

When you configure a port as unidirectional with the dot1x control-direction in interface configuration command, the port changes to the spanning-tree forwarding state.
When Unidirectional Control Port is enabled, the connected host is in the sleeping mode or power-down state. The host does not exchange traffic with other devices in the network. The host connected to the unidirectional port cannot send traffic to the network, the host can only receive traffic from other devices in the network.

**Bidirectional State**

When you configure a port as bidirectional with the `dot1x control-direction both` interface configuration command, the port is access-controlled in both directions. In this state, the switch port receives or sends only EAPOL packets; all other packets are dropped.

Using the `both` keyword or using the `no` form of this command changes the port to its bidirectional default setting.

**Catalyst 6500 Series Switch**

Setting the port as bidirectional enables 802.1X authentication with wake-on-LAN (WoL).

**Cisco IOS Release 12.4(4)XC**

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

**Examples**

The following example shows how to enable unidirectional control:

```
Switch(config-if)# dot1x control-direction in
```

The following examples show how to enable bidirectional control:

```
Switch(config-if)# dot1x control-direction both
```

or

```
Switch(config-if)# no dot1x control-direction
```

You can verify your settings by entering the show dot1x all privileged EXEC command. The show dot1x all command output is the same for all devices except for the port names and the state of the port. If a host is attached to the port but is not yet authenticated, a display similar to the following appears:

```
Supplicant MAC  0002.b39a.9275
AuthSM State = CONNECTING
BendSM State = IDLE
PortStatus = UNAUTHORIZED
```

If you enter the `dot1x control-direction` command to enable unidirectional control, the following appears in the show dot1x all command output:

```
ControlDirection = In
```

If you enter the `dot1x control-direction` command and the port cannot support this mode because of a configuration conflict, the following appears in the show dot1x all command output:

```
ControlDirection = In (Disabled due to port settings):
```

The following example shows how to reset the global 802.1X parameters:
Switch(config)# dot1x default

**Catalyst 6500 Series Switch**

The following example shows how to enable 802.1X authentication with WoL and set the port as bidirectional:

Switch(config)# interface gigabitethernet 5/1
Switch(config-if)# dot1x control-direction both

**802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)X**

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```plaintext
interface FastEthernet0
description  switchport connect to a client
!
interface FastEthernet1
description  switchport connect to a client
!
interface FastEthernet2
description  switchport connect to a client
!
interface FastEthernet3
description  switchport connect to a client
!
interface FastEthernet4
description  Connect to the public network
!
interface Vlan1
description  Apply 802.1x functionality on SVI
dot1x pae authenticator
dot1x port-control auto
dot1x reauthentication
dot1x control-direction in
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show dot1x</td>
<td>Displays details for an identity profile.</td>
</tr>
</tbody>
</table>
dot1x credentials

To specify which 802.1X credential profile to use when configuring a supplicant (client) or to apply a credentials structure to an interface and to enter dot1x credentials configuration mode, use the `dot1x credentials` command in global configuration or interface configuration mode. To remove the credential profile, use the `no` form of this command.

```
dot1x credentials name
no dot1x credentials
```

**Syntax Description**
- `name`: Name of the credentials profile.

**Command Default**
A credentials profile is not specified.

**Command Modes**
- Global configuration
- Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
An 802.1X credential structure is necessary when configuring a supplicant. This credentials structure may contain a username, password, and description.

**Examples**
The following example shows which credentials profile should be used when configuring a supplicant:

```
dot1x credentials basic-user
  username router
  password secret
  description This credentials profile should be used for most configured ports
```

The credentials structure can be applied to an interface, along with the `dot1x pae supplicant` command and keyword, to enable supplicant functionality on that interface.

```
interface fastethernet 0/1
  dot1x credentials basic-user
  dot1x pae supplicant
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>anonymous-id (dot1x credential)</code></td>
<td>Specifies the anonymous identity that is associated with a credentials profile.</td>
</tr>
<tr>
<td><code>description (dot1x credential)</code></td>
<td>Specifies the description for an 802.1X credentials profile.</td>
</tr>
<tr>
<td><code>password (dot1x credential)</code></td>
<td>Specifies the password for an 802.1X credentials profile.</td>
</tr>
<tr>
<td><code>username (dot1x credential)</code></td>
<td>Specifies the username for an 802.1X credentials profile.</td>
</tr>
</tbody>
</table>
**dot1x critical (global configuration)**

To configure the IEEE 802.1X critical authentication parameters, use the **dot1x critical** command in global configuration mode.

```text
dot1x critical {eapol|recovery delay milliseconds}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eapol</td>
<td>Specifies that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port.</td>
</tr>
<tr>
<td>recovery delay</td>
<td>Specifies the recovery delay period that the switch waits to reinitialize a critical port when an unavailable RADIUS server becomes available; valid values are from 1 to 10000, in milliseconds.</td>
</tr>
<tr>
<td>milliseconds</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

The default settings are as follows:

- **eapol** -- Disabled
- **milliseconds** -- 1000 milliseconds

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXH</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>The <code>recovery delay</code> keyword was replaced by the <code>authentication critical recovery delay</code> command.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to specify that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port:

```text
Switch(config)# dot1x critical eapol
```

This example shows how to set the recovery delay period that the switch waits to reinitialize a critical port when an unavailable RADIUS server becomes available:

```text
Switch(config)# dot1x critical recovery delay 1500
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>dot1x critical (interface configuration)</strong></td>
<td>Enables 802.1X critical authentication on an interface.</td>
</tr>
</tbody>
</table>
**dot1x critical (interface configuration)**

To enable 802.1X critical authentication, and optionally, 802.1X critical authentication recovery and authentication, on an interface, use the `dot1x critical` command in interface configuration mode. To disable 802.1X critical authentication, and optionally, 802.1X critical authentication recovery and authentication, use the `no` form of this command.

```
set1x critical [recovery action reinitialize]
no dot1x critical [recovery action reinitialize]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>recovery action reinitialize</td>
<td>(Optional) Enables 802.1X critical authentication recovery and specifies that the port is authenticated when an authentication server is available.</td>
</tr>
</tbody>
</table>

**Command Default**
The 802.1X critical authentication is enabled on an interface.

**Command Modes**
Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXH</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to enable 802.1X critical authentication on an interface:

```
Router(config-if)# dot1x critical
```

This example shows how to enable 802.1X critical authentication recovery and authenticate the port when an authentication server is available:

```
Router(config-if)# dot1x critical recovery action reinitialize
```

This example shows how to disable 802.1X critical authentication on an interface:

```
Router(config-if)# no
dot1x critical
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x critical (global configuration)</code></td>
<td>Configures the 802.1X critical authentication parameters.</td>
</tr>
</tbody>
</table>
**dot1x default**

To reset the global 802.1X authentication parameters to their default values as specified in the latest IEEE 802.1X standard, use the `dot1x default` command in global configuration or interface configuration mode.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The default values are as follows:

- The per-interface 802.1X protocol enable state is disabled (force-authorized).
- The number of seconds between reauthentication attempts is 3600 seconds.
- The quiet period is 60 seconds.
- The retransmission time is 30 seconds.
- The maximum retransmission number is 2 times.
- The multiple host support is disabled.
- The client timeout period is 30 seconds.
- The authentication server timeout period is 30 seconds.

**Command Modes**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(6)EA2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)ZJ</td>
<td>This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was implemented on the Supervisor Engine 720 in Cisco IOS Release 12.2(14)SX.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>This command was implemented on the Supervisor Engine 2 in Cisco IOS Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.4(6)T</td>
<td>Interface configuration was added as a configuration mode for this command.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td>This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

Use the `show dot1x` command to verify your current 802.1X settings.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows how to reset the global 802.1X parameters:

```
Router(config)# dot1x default
```

The following example show how to reset the global 802.1X parameters on FastEthernet interface 0:

```
Router(config)# interface FastEthernet0
Router(config-if)# dot1x default
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x critical (global configuration)</code></td>
<td>Configures the 802.1X critical authentication parameters.</td>
</tr>
<tr>
<td><code>dot1x critical (interface configuration)</code></td>
<td>Enables 802.1X critical authentication on an interface.</td>
</tr>
<tr>
<td><code>dot1x max-req</code></td>
<td>Sets the maximum number of times that the device sends an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.</td>
</tr>
<tr>
<td><code>dot1x re-authentication (EtherSwitch)</code></td>
<td>Enables periodic reauthentication of the client for the Ethernet switch network module.</td>
</tr>
<tr>
<td><code>dot1x timeout (EtherSwitch)</code></td>
<td>Sets retry timeouts for the Ethernet switch network module.</td>
</tr>
<tr>
<td><code>show dot1x</code></td>
<td>Displays 802.1X information.</td>
</tr>
<tr>
<td><code>show dot1x (EtherSwitch)</code></td>
<td>Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.</td>
</tr>
</tbody>
</table>
**dot1x guest-vlan**

To specify an active VLAN as an IEEE 802.1x guest VLAN, use the `dot1x guest-vlan` command in interface configuration mode. To return to the default setting, use the `no` form of this command.

```
dot1x guest-vlan vlan-id
no dot1x guest-vlan
```

**Syntax Description**

- `vlan-id`: Specify an active VLAN as an IEEE 802.1x guest VLAN. The range is 1 to 4094.

**Command Default**

No guest VLAN is configured.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(14)EA1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)SE</td>
<td>This command was modified to change the default guest VLAN behavior.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(11)T.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>15.3(1)S</td>
<td>This command was integrated into Cisco IOS Release 15.3(1)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can configure a guest VLAN on a static-access port.

For each IEEE 802.1x port, you can configure a guest VLAN to provide limited services to clients (a device or workstation connected to the switch) not running IEEE 802.1x authentication. These users might be upgrading their systems for IEEE 802.1x authentication, and some hosts, such as Windows 98 systems, might not be IEEE 802.1x capable.

When you enable a guest VLAN on an IEEE 802.1x port, the software assigns clients to a guest VLAN when it does not receive a response to its Extensible Authentication Protocol over LAN (EAPOL) request/identity frame or when EAPOL packets are not sent by the client.

With Cisco IOS Release 12.4(11)T and later, the switch port maintains the EAPOL packet history. If another EAPOL packet is detected on the interface during the lifetime of the link, the guest VLAN feature is disabled. If the port is already in the guest VLAN state, the port returns to the unauthorized state, and authentication restarts. The EAPOL history is reset upon loss of link.

Any number of non-IEEE 802.1x-capable clients are allowed access when the switch port is moved to the guest VLAN. If an IEEE 802.1x-capable client joins the same port on which the guest VLAN is configured, the port is put into the unauthorized state in the RADIUS-configured or user-configured access VLAN, and authentication is restarted.

Guest VLANs are supported on IEEE 802.1x switch ports in single-host or multi-host mode.
You can configure any active VLAN except a Remote Switched Port Analyzer (RSPAN) VLAN or a voice VLAN as an IEEE 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

After you configure a guest VLAN for an IEEE 802.1x port to which a DHCP client is connected, you might need to get a host IP address from a DHCP server. You can change the settings for restarting the IEEE 802.1x authentication process on the switch before the DHCP process on the client times out and tries to get a host IP address from the DHCP server. You should decrease the settings for the IEEE 802.1x authentication process using the `dot1x max-reauth-req` and `dot1x timeout tx-period` interface configuration commands. The amount of decrease depends on the connected IEEE 802.1x client type.

**Examples**

This example shows how to specify VLAN 5 as an IEEE 802.1x guest VLAN:

```
Switch(config-if)# dot1x guest-vlan 5
```

This example shows how to set 3 as the quiet time on the switch, to set 15 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request, and to enable VLAN 2 as an IEEE 802.1x guest VLAN when an IEEE 802.1x port is connected to a DHCP client:

```
Switch(config-if)# dot1x timeout max-reauth-req 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

You can display the IEEE 802.1x administrative and operational status for the device or for the specified interface by entering the `show dot1x interface interface-id` privileged EXEC command.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x max-reauth-req</code></td>
<td>Specifies the number of times that the switch retransmits an EAP-request/identity frame to the client before restarting the authentication process.</td>
</tr>
<tr>
<td><code>dot1x timeout</code></td>
<td>Sets authentication retry timeouts.</td>
</tr>
<tr>
<td><code>show dot1x</code></td>
<td>Displays details for an identity profile.</td>
</tr>
</tbody>
</table>
dot1x guest-vlan supplicant

To allow the 802.1x-capable supplicants to enter the guest VLAN, use the `dot1x guest-vlan supplicant` command in global configuration mode. To prevent the 802.1x-capable supplicants from entering the guest VLAN, use the `no` form of this command.

```
dot1x guest-vlan supplicant
no dot1x guest-vlan supplicant
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
The 802.1x-capable supplicants are prevented from entering the guest VLAN.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXH</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to allow the 802.1x-capable supplicants to enter the guest VLAN:

```
Router(config) # dot1x guest-vlan supplicant
```

This example shows how to prevent the 802.1x-capable supplicants from entering the guest VLAN:

```
Router(config) # no dot1x guest-vlan supplicant
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x critical (global configuration)</code></td>
<td>Configures the 802.1X critical authentication parameters.</td>
</tr>
<tr>
<td><code>dot1x critical (interface configuration)</code></td>
<td>Enables 802.1X critical authentication on an interface.</td>
</tr>
</tbody>
</table>
**dot1x host-mode**

**Note**
Effective with Cisco IOS Release 12.2(33)SXI, the `dot1x host-mode` command is replaced by the `authentication host-mode` command. See the `authentication host-mode` command for more information.

To allow hosts on an IEEE 802.1X-authorized port, use the `dot1x host-mode` command in interface configuration mode. To return to the default setting, use the `no` form of this command.

```
   dot1x host-mode {multi-auth|multi-host|single-host}
   no dot1x host-mode {multi-auth|multi-host|single-host}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>multi-auth</code></td>
<td>Specifies that all clients are authenticated individually on the port. The multi-auth mode is not supported on switch ports and is the default mode for switch ports.</td>
</tr>
<tr>
<td><code>multi-host</code></td>
<td>Ensures that the first client and all subsequent clients are allowed access to the port if the first client is successfully authenticated.</td>
</tr>
<tr>
<td><code>single-host</code></td>
<td>Ensures that only the first client is authenticated. All other clients are ignored and may cause a violation. The single-host mode is the default mode for switch ports.</td>
</tr>
</tbody>
</table>

**Command Default**
Hosts are not allowed on an 802.1X-authorized port.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(14)EA1</td>
<td>This command was introduced for switches. It replaced the <code>dot1x multiple-hosts</code> command.</td>
</tr>
<tr>
<td>12.4(6)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(6)T.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td>This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Switches (ISRs) only.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was replaced by the <code>authentication host-mode</code> command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before you use this command, use the `dot1x port-control auto` command to enables IEEE 802.1X port-based authentication, and cause the port to begin in the unauthorized state.

The `multi-auth` mode authenticates each new client separately.

In `multi-host` mode, only one of the attached hosts has to be successfully authorized for all hosts to be granted network access (the `multi-host` mode authenticates one client, but after the client is authenticated, traffic is allowed from all other MAC addresses.). If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL] logoff message is received), all attached clients are denied access to the network.
The single-host mode allows only one client per port; that is, one MAC address is authenticated, and all others are blocked.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISR s only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows how to enable IEEE 802.1X globally, to enable IEEE 802.1x on a port, and to enable multiple-hosts mode:

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host:
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
description switchport connect to a client
!
interface FastEthernet1
description switchport connect to a client
!
interface FastEthernet2
description switchport connect to a client
!
interface FastEthernet3
description switchport connect to a client
!
interface FastEthernet4
description Connect to the public network
!
interface Vlan1
description Apply 802.1x functionality on SVI
dot1x pae authenticator
dot1x port-control auto
dot1x reauthentication
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dot1x port-control</td>
<td>Enables 802.1X port-based authentication.</td>
</tr>
<tr>
<td></td>
<td>show dot1x</td>
<td>Displays details for an identity profile.</td>
</tr>
</tbody>
</table>
dot1x initialize

**Note**

Effective with Cisco IOS Release 12.2(33)SXI, the `dot1x initialize` command is replaced by the `clear authentication session` command. See the `clear authentication session` command for more information.

To initialize 802.1X clients on all 802.1X-enabled interfaces, use the `dot1x initialize` command in privileged EXEC mode. This command does not have a **no** form.

```
dot1x initialize [interface interface-name]
```

**Syntax Description**

| interface interface-name | (Optional) Specifies an interface to be initialized. If this keyword is not entered, all interfaces are initialized. |

**Command Default**

State machines are not enabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(14)E6A1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(2)XA</td>
<td>This command was integrated into Cisco IOS Release 12.3(2)XA.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to initialize the 802.1X state machines and to set up a fresh environment for authentication. After you enter this command, the port status becomes unauthorized.

**Examples**

The following example shows how to manually initialize a port:

```
Router# dot1x initialize interface gigabitethernet2/0/2
```

You can verify the unauthorized port status by entering the `show dot1x [interface interface-name]` command.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Displays details for an identity profile.</td>
</tr>
</tbody>
</table>
**dot1x mac-auth-bypass**

To enable a switch to authorize clients based on the client MAC address, use the `dot1x mac-auth-bypass` command in interface configuration mode. To disable MAC authentication bypass, use the `no` form of this command.

```
dot1x mac-auth-bypass [eap]
no dot1x mac-auth-bypass
```

**Syntax Description**

- `eap` (Optional) Configures the switch to use Extensible Authentication Protocol (EAP) for authorization.

**Command Default**

MAC authentication bypass is disabled.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXH</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(4)M</td>
<td>This command was integrated into Cisco IOS Release 15.1(4)M.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use MAC authentication bypass on a routed port, ensure that MAC address learning is enabled on the port.

When the MAC authentication bypass feature is enabled on an 802.1X port, the switch uses the MAC address as the client identity. The authentication server has a database of client MAC addresses that are allowed network access. If authorization fails, the switch assigns the port to the guest VLAN if a VLAN is configured.

**Examples**

This example shows how to enable MAC authentication bypass:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x mac-auth-bypass
```

This example shows how to configure the switch to use EAP for authorization:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x mac-auth-bypass eap
```

This example shows how to disable MAC authentication bypass:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# no dot1x mac-auth-bypass
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><em>dot1x critical (global configuration)</em></td>
<td>Configures the 802.1X critical authentication parameters.</td>
</tr>
<tr>
<td></td>
<td><em>dot1x critical (interface configuration)</em></td>
<td>Enables 802.1X critical authentication on an interface.</td>
</tr>
</tbody>
</table>
**dot1x max-reauth-req**

To set the maximum number of times the authenticator sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client, use the `dot1x max-reauth-req` command in interface configuration mode. To set the maximum number of times to the default setting of 2, use the `no` form of this command.

```
dot1x max-reauth-req number
no dot1x max-reauth-req
```

**Syntax Description**

| number | Maximum number of times. The range is 1 through 10. The default is 2. |

**Command Default**

The command default is 2.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)SE</td>
<td>The <code>number</code> argument was added.</td>
</tr>
<tr>
<td>12.4(6)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(6)T.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td>This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

**Cisco IOS Release 12.4(4)XC**

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

**Verifying Settings**

You can verify your settings by entering the `show dot1x [interface interface-id]` command.

**Examples**

The following example shows how to set 4 as the number of times that the authentication process is restarted before changing to the unauthorized state:

```
Router(config-if)# dot1x max-reauth-req 4
```

**802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC**
The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```plaintext
interface FastEthernet0
  description switchport connect to a client
!
interface FastEthernet1
  description switchport connect to a client
!
interface FastEthernet2
  description switchport connect to a client
!
interface FastEthernet3
  description switchport connect to a client
!
interface FastEthernet4
  description Connect to the public network
!
interface Vlan1
  description Apply 802.1x functionality on SVI
  dot1x pae authenticator
dot1x port-control auto
  dot1x reauthentication
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x max-req</code></td>
<td>Sets the maximum number of times that a device can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.</td>
</tr>
<tr>
<td><code>dot1x timeout tx-period</code></td>
<td>Sets the number of seconds that the switch waits for a response to an EAP request or identity frame from the client before resending the request.</td>
</tr>
<tr>
<td><code>show dot1x</code></td>
<td>Displays IEEE 802.1X status for the specified port.</td>
</tr>
</tbody>
</table>
**dot1x max-req**

To set the maximum number of times that a networking device or Ethernet switch network module can send an Extensible Authentication Protocol (EAP) request/identity frame to a client (assuming that a response is not received) before restarting the authentication process, use the `dot1x max-req` command in interface configuration or global configuration mode. To set the number of times to the default setting of 2, use the `no` form of this command.

```
dot1x max-req retry-number
no dot1x max-req
```

**Syntax Description**

| retry-number | Maximum number of retries. The value is from 1 through 10. The default value is 2. The value is applicable to all EAP packets except for Request ID. |

**Command Default**

The default number of retries is 2.

**Command Modes**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(6)EA2</td>
<td>This command was introduced on the Cisco Ethernet switch network module.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was implemented on the Supervisor Engine 720 in Cisco IOS Release 12.2(14)SX.</td>
</tr>
<tr>
<td>12.2(15)ZJ</td>
<td>This command was implemented on the Cisco Ethernet switch network module on the following platforms in Cisco IOS Release 12.2(15)ZJ: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.</td>
</tr>
<tr>
<td>12.1(11)AX</td>
<td>This command was integrated into Cisco IOS Release 12.1(11)AX.</td>
</tr>
<tr>
<td>12.1(14)EA1</td>
<td>This command was integrated into Cisco IOS Release 12.1(14)EA1 and the configuration mode was changed to interface configuration mode except on the EtherSwitch network module.</td>
</tr>
<tr>
<td>12.3(2)XA</td>
<td>This command was integrated into Cisco IOS Release 12.3(2)XA and implemented on the following router platforms: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T and implemented on the following router platforms: Cisco 1751, Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>This command was implemented on the Supervisor Engine 2 in Cisco IOS Release 12.2(17d)SXB.</td>
</tr>
</tbody>
</table>
Modification

Release | Modification
--- | ---
12.4(4)XC | This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.
12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

Note

You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows that the maximum number of times that the networking device will send an EAP request or identity message to the client PC is 6:

```
Router(config) configure terminal
Router(config)# interface ethernet 0
Router(config-if)# dot1x max-req 6
```

The following example shows how to set the number of times that a switch sends an EAP request or identity frame to 5 before restarting the authentication process:

```
Router(config-if)# dot1x max-req 5
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x port-control</code></td>
<td>Enables manual control of the authorization state of a controlled port.</td>
</tr>
<tr>
<td><code>dot1x re-authentication</code></td>
<td>Globally enables periodic reauthentication of the client PCs on the 802.1X interface.</td>
</tr>
<tr>
<td><code>dot1x reauthentication (EtherSwitch)</code></td>
<td>Enables periodic reauthentication of the Ethernet switch network module client on the 802.1X interface.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>dot1x timeout</td>
<td>Sets retry timeouts.</td>
</tr>
<tr>
<td>dot1x timeout (EtherSwitch)</td>
<td>Sets retry timeouts for the Ethernet switch network module.</td>
</tr>
<tr>
<td>show dot1x</td>
<td>Displays details for an identity profile.</td>
</tr>
<tr>
<td>show dot1x (EtherSwitch)</td>
<td>Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.</td>
</tr>
</tbody>
</table>
**dot1x max-start**

To set the maximum number of Extensible Authentication Protocol (EAP) start frames that a supplicant sends (assuming that no response is received) to the client before concluding that the other end is 802.1X unaware, use the `dot1x max-start` command in global configuration or interface configuration mode. To remove the maximum number-of-times setting, use the `no` form of this command.

```
dot1x max-start number
no dot1x max-start
```

**Syntax Description**

| number | Maximum number of times that the router sends an EAP start frame. The value is from 1 to 65535. The default is 3. |

**Command Default**

The default maximum number setting is 3.

**Command Modes**

Global configuration

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(11)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(6)T</td>
<td>Global configuration mode was added for this command.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td>This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

**Examples**

The following example shows that the maximum number of EAP over LAN- (EAPOL-) Start requests has been set to 5:

```
Router (config)# interface Ethernet1
Router (config-if)# dot1x pae supplicant
Router (config-if)# dot1x max-start 5
```

**802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC**

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):
interface FastEthernet0
description switchport connect to a client
!
interface FastEthernet1
description switchport connect to a client
!
interface FastEthernet2
description switchport connect to a client
!
interface FastEthernet3
description switchport connect to a client
!
interface FastEthernet4
description Connect to the public network
!
interface Vlan1
description Apply 802.1x functionality on SVI
dot1x pae authenticator
dot1x port-control auto

dot1x reauthentication

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x pae</td>
<td>Sets the PAE type during 802.1X authentication.</td>
</tr>
<tr>
<td>interface</td>
<td>Configures an interface type.</td>
</tr>
</tbody>
</table>
dot1x multi-hosts

To allow multiple hosts (clients) on an 802.1X-authorized port in interface configuration command mode, use the dot1x multi-hosts command. Use the no form of this command to disallow multiple hosts.

```
dot1x multi-hosts
no dot1x multi-hosts
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before entering this command, ensure that the `dot1x port-control` command is set to `auto` for the specified interface.

**Examples**

This example shows how to allow multiple hosts:

```
Router(config-if)# dot1x multi-hosts
Router(config-if)#
```

This example shows how to disallow multiple hosts:

```
Router(config-if)# no dot1x multi-hosts
Router(config-if)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x port-control</td>
<td>Sets the port control value.</td>
</tr>
<tr>
<td>show dot1x</td>
<td>Displays 802.1X information.</td>
</tr>
</tbody>
</table>
**dot1x multiple-hosts**

This command was replaced by the `dot1x host-mode` command effective with Cisco IOS Release 12.1(14)EA1 and Release 12.4(6)T.

To allow multiple hosts (clients) on an 802.1X-authorized switch port that has the `dot1x port-control` interface configuration command set to `auto`, use the `dot1x multiple-hosts` command in interface configuration mode. To return to the default setting, use the `no` form of this command.

```
```
dot1x multiple-hosts
no dot1x multiple-hosts
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Multiple hosts are disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(6)EA2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)ZJ</td>
<td>This command was implemented on the following platforms: Cisco 2600 series,</td>
</tr>
<tr>
<td></td>
<td>Cisco 3600 series, and Cisco 3700 series routers.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T on the following</td>
</tr>
<tr>
<td></td>
<td>platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series</td>
</tr>
<tr>
<td></td>
<td>routers.</td>
</tr>
<tr>
<td>12.1(14)EA1</td>
<td>This command was replaced by the <code>dot1x host-mode</code> command in Cisco IOS</td>
</tr>
<tr>
<td></td>
<td>Release 12.1(14)EA1.</td>
</tr>
<tr>
<td>12.4(6)T</td>
<td>This command was replaced by the <code>dot1x host-mode</code> command on the T-train.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is supported only on switch ports.

This command enables you to attach multiple clients to a single 802.1X-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL]-logoff message is received), all attached clients are denied access to the network.

Use the `show dot1x` (EtherSwitch)privileged EXEC command with the `interface` keyword to verify your current 802.1X multiple host settings.

**Examples**

The following example shows how to enable 802.1X on Fast Ethernet interface 0/1 and to allow multiple hosts:

```
Router(config)# interface fastethernet0/1
```
Router(config-if)# dot1x port-control auto
Router(config-if)# dot1x multiple-hosts

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dot1x default</td>
<td>Enables manual control of the authorization state of the port.</td>
</tr>
<tr>
<td></td>
<td>show dot1x (EtherSwitch)</td>
<td>Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.</td>
</tr>
</tbody>
</table>
**dot1x pae**

To set the Port Access Entity (PAE) type, use the `dot1x pae` command in interface configuration mode. To disable the PAE type that was set, use the `no` form of this command.

```
dot1x pae [{supplicant|authenticator|both}]
no dot1x pae [{supplicant|authenticator|both}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>supplicant</code></td>
<td>(Optional) The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.</td>
</tr>
<tr>
<td><code>authenticator</code></td>
<td>(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.</td>
</tr>
<tr>
<td><code>both</code></td>
<td>(Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages.</td>
</tr>
</tbody>
</table>

**Command Default**

PAE type is not set.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(11)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td>This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the `dot1x system-auth-control` command has not been configured, the `supplicant` keyword will be the only keyword available for use with this command. (That is, if the `dot1x system-auth-control` command has not been configured, you cannot configure the interface as an authenticator.)

**Cisco IOS Release 12.4(4)XC**

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

**Examples**

The following example shows that the interface has been set to act as a supplicant:

```
Router (config)# interface Ethernet1
Router (config-if)# dot1x pae supplicant
```
**802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC**

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```plaintext
interface FastEthernet0
  description switchport connect to a client

interface FastEthernet1
  description switchport connect to a client

interface FastEthernet2
  description switchport connect to a client

interface FastEthernet3
  description switchport connect to a client

interface FastEthernet4
  description Connect to the public network

interface Vlan1
  description Apply 802.1x functionality on SVI
dot1x pae authenticator
dot1x port-control auto
dot1x reauthentication
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x system-auth-control</code></td>
<td>Enables 802.1X SystemAuthControl (port-based authentication).</td>
</tr>
<tr>
<td><code>interface</code></td>
<td>Configures an interface type.</td>
</tr>
</tbody>
</table>
**dot1x port-control**

*Note* Effective with Cisco IOS Release 12.2(33)SX1, the `dot1x port-control` command is replaced by the `authentication port-control` command. See the `authentication port-control` command for more information.

To enable manual control of the authorization state of a controlled port, use the `dot1x port-control` command in interface configuration mode. To disable the port-control value, use the `no` form of this command.

```plaintext
dot1x port-control {auto|force-authorized|force-unauthorized}
no dot1x port-control
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.</td>
</tr>
<tr>
<td>force-authorized</td>
<td>Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The <code>force-authorized</code> keyword is the default.</td>
</tr>
<tr>
<td>force-unauthorized</td>
<td>Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.</td>
</tr>
</tbody>
</table>

**Command Default**

The default is force-authorized.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(6)EA2</td>
<td>This command was introduced for the Cisco Ethernet switch network module.</td>
</tr>
<tr>
<td>12.1(11)AX</td>
<td>This command was integrated into Cisco IOS Release 12.1(11)AX.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(15)ZJ</td>
<td>This command was implemented on the following platforms for the Cisco Ethernet switch network module: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.</td>
</tr>
<tr>
<td>12.3(2)XA</td>
<td>This command was introduced on the following Cisco Switches: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T. Switch support was added for the following platforms: Cisco 1751, Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.</td>
</tr>
</tbody>
</table>
Modification
Support for this command on the Supervisor Engine 2 was added for Cisco IOS Release 12.2(17d)SXB.

12.4(4)XC
This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Switchs (ISRs) only.

12.2(33)SRA
This command was integrated into Cisco IOS Release 12.2(33)SRA.

12.2(33)SXI
This command was replaced by the **authentication** **port-control** command.

### Usage Guidelines

**For Ethernet Switch Network Modules**

The following guidelines apply to Ethernet switch network modules:

- The 802.1X protocol is supported on Layer 2 static-access ports.
- You can use the **auto** keyword only if the port is not configured as one of these types:
  - Trunk port—If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
  - EtherChannel port—Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel or on an active port in an EtherChannel, an error appears, and 802.1X is not enabled. If you enable 802.1X on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.
  - Switch Port Analyzer (SPAN) destination port—You can enable 802.1X on a port that is a SPAN destination port; however, 802.1X is disabled until the port is removed as a SPAN destination. You can enable 802.1X on a SPAN source port.

To globally disable 802.1X on the device, you must disable it on each port. There is no global configuration command for this task.

**For Cisco IOS Release 12.4(4)XC**

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

**Verifying Settings**

You can verify your settings by entering the **show dot1x** command and checking the Status column in the 802.1X Port Summary section of the display. An enabled status means that the port-control value is set to **auto** or to **force-unauthorized**.

**Examples**

The following example shows that the authentication status of the client PC will be determined by the authentication process:

```
Switch(config)# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# dot1x port-control auto
```
802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
  description switchport connect to a client
!
interface FastEthernet1
  description switchport connect to a client
!
interface FastEthernet2
  description switchport connect to a client
!
interface FastEthernet3
  description switchport connect to a client
!
interface FastEthernet4
  description Connect to the public network
!
interface Vlan1
  description Apply 802.1x functionality on SVI
  dot1x pae authenticator
  dot1x port-control auto

dot1x reauthentication
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>.dot1x max-req</code></td>
<td>Sets the maximum number of times that a switch or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.</td>
</tr>
<tr>
<td><code>.dot1x re-authentication</code></td>
<td>Globally enables periodic reauthentication of the client on the 802.1X interface.</td>
</tr>
<tr>
<td><code>.dot1x reauthentication (EtherSwitch)</code></td>
<td>Enables periodic reauthentication of the client on the 802.1X interface.</td>
</tr>
<tr>
<td><code>.dot1x timeout</code></td>
<td>Sets retry timeouts.</td>
</tr>
<tr>
<td><code>.dot1x timeout (EtherSwitch)</code></td>
<td>Sets retry timeouts for the Ethernet switch network module.</td>
</tr>
<tr>
<td><code>.show dot1x</code></td>
<td>Displays details for an identity profile.</td>
</tr>
<tr>
<td><code>.show dot1x (EtherSwitch)</code></td>
<td>Displays the 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.</td>
</tr>
</tbody>
</table>
**dot1x re-authenticate (EtherSwitch)**

To manually initiate a reauthentication of all 802.1X-enabled ports or the specified 802.1X-enabled port on a router with an Ethernet switch network module installed, use the `dot1x re-authenticate` command in privileged EXEC mode.

```
dot1x re-authenticate [interface interface-type interface-number]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface interface-type interface-number</td>
<td>(Optional) Specifies the slot and port number of the interface to reauthenticate.</td>
</tr>
</tbody>
</table>

**Command Default**

There is no default setting.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(6)EA2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)ZJ</td>
<td>This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can use this command to reauthenticate a client without waiting for the configured number of seconds between reauthentication attempts (reauthperiod) and automatic reauthentication.

**Examples**

The following example shows how to manually reauthenticate the device connected to Fast Ethernet interface 0/1:

```
Router# dot1x re-authenticate interface fastethernet 0/1
Starting reauthentication on FastEthernet0/1.
```
dot1x re-authenticate (privileged EXEC)

Note

Effective with Cisco IOS Release 12.2(33)SX1, the dot1x re-authenticate command is replaced by the clear authentication session command. See the clear authentication session command for more information.

To manually initiate a reauthentication of the specified 802.1X-enabled ports, use the dot1x re-authenticate command in privileged EXEC mode.

dot1x re-authenticate [interface interface-name interface-number]

Syntax Description

| interface interface-name interface-number | (Optional) Interface on which reauthentication is to be initiated. |

Command Default

There is no default setting.

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(11)AX</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(2)XA</td>
<td>This command was integrated into Cisco IOS Release 12.3(2)XA.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td>This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You can use this command to reauthenticate a client without having to wait for the configured number of seconds between reauthentication attempts (re-authperiod) and automatic reauthentication.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows how to manually reauthenticate the device that is connected to a port:

```
Router# dot1x re-authenticate interface gigabitethernet2/0/1
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):
interface FastEthernet0
  description switchport connect to a client
!
interface FastEthernet1
  description switchport connect to a client
!
interface FastEthernet2
  description switchport connect to a client
!
interface FastEthernet3
  description switchport connect to a client
!
interface FastEthernet4
  description Connect to the public network
!
interface Vlan1
  description Apply 802.1x functionality on SVI
dot1x pae authenticator
dot1x port-control auto

dot1x reauthentication

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x reauthentication</td>
<td>Globally enables periodic reauthentication of the client PCs on the 802.1X interface.</td>
</tr>
<tr>
<td>dot1x timeout</td>
<td>Sets retry timeouts.</td>
</tr>
</tbody>
</table>
dot1x reauthentication

**Note**
Effective with Cisco IOS Release 12.2(33)SXI, the `dot1x reauthentication` command is replaced by the `authentication periodic` command. See the `authentication periodic` command for more information.

To enable periodic reauthentication of the client PCs on the 802.1X interface, use the `dot1x reauthentication` command in interface configuration mode. To disable periodic reauthentication, use the `no` form of this command.

```
  dot1x reauthentication
  no dot1x reauthentication
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Periodic reauthentication is not set.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>This command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.3(2)XA</td>
<td>This command was integrated into Cisco IOS Release 12.3(2)XA.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>This command was implemented on the Supervisor Engine 2 in Cisco IOS Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td>This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was replaced by the <code>authentication periodic</code> command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The reauthentication period can be set using the `dot1x timeout` command.

**Cisco IOS Release 12.4(4)XC**
For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

**Examples**
The following example shows that reauthentication has been enabled and the reauthentication period as been set for 1800 seconds:
Router(config)# configure terminal
Router(config)# interface ethernet 0
Router(config-if)# dot1x reauthentication
Router(config-if)# dot1x timeout reauth-period 1800

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)X

The following example shows Layer 3 802.1X support on a switched virtual interface using a Cisco 870 ISR:

interface FastEthernet0
  description switchport connect to a client
!
interface FastEthernet1
  description switchport connect to a client
!
interface FastEthernet2
  description switchport connect to a client
!
interface FastEthernet3
  description switchport connect to a client
!
interface FastEthernet4
  description Connect to the public network
!
interface Vlan1
  description Apply 802.1x functionality on SVI
dot1x pae authenticator
dot1x port-control auto
dot1x reauthentication

Cisco 7600 Series

The following example shows how to enable periodic reauthentication of the client:

Router(config-if)# dot1x reauthentication
Router(config-if)#

The following example shows how to disable periodic reauthentication of the client:

Router(config-if)# no dot1x reauthentication
Router(config-if)#

<table>
<thead>
<tr>
<th>Related Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>dot1x max-req</td>
</tr>
<tr>
<td>dot1x port-control</td>
</tr>
<tr>
<td>dot1x timeout</td>
</tr>
<tr>
<td>Command</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>show dot1x</td>
</tr>
</tbody>
</table>
**dot1x re-authentication (EtherSwitch)**

To enable periodic reauthentication of the client for an Ethernet switch network module, use the `dot1x re-authentication` command in global configuration mode. To disable periodic reauthentication, use the `no` form of this command.

```
dot1x re-authentication
no dot1x re-authentication
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Periodic reauthentication is disabled.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(6)EA2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)ZJ</td>
<td>This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You configure the amount of time between periodic reauthentication attempts by using the `dot1x timeout re-authperiod` global configuration command.

**Examples**

The following example shows how to disable periodic reauthentication of the client:

```
Router(config)# no dot1x re-authentication
```

The following example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000 seconds:

```
Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x timeout (EtherSwitch)</code></td>
<td>Sets retry timeouts for the Ethernet switch network module.</td>
</tr>
<tr>
<td><code>show dot1x (EtherSwitch)</code></td>
<td>Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.</td>
</tr>
</tbody>
</table>
dot1x supplicant interface

To configure the dot1x supplicant for a given interface, use the `dot1x supplicant interface` command in privileged EXEC mode. To disable the configuration, use the `no` form of this command.

```
dot1x supplicant {start|stop} profile-name interface type number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>start</code></td>
<td>Starts the supplicant for a given interface.</td>
</tr>
<tr>
<td><code>stop</code></td>
<td>Stops the supplicant for a given interface.</td>
</tr>
<tr>
<td><code>profile-name</code></td>
<td>Profile name.</td>
</tr>
<tr>
<td><code>type number</code></td>
<td>Interface type and number.</td>
</tr>
</tbody>
</table>

**Command Default**
The dot1x supplicant interface is not configured.

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to configure the dot1x supplicant for a Gigabit Ethernet interface:

```
Router# dot1x supplicant start nl interface GigabitEthernet 0/0/1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x default</code></td>
<td>Resets the global 802.1X authentication parameters to their default values as specified in the latest IEEE 802.1X standard.</td>
</tr>
</tbody>
</table>
**dot1x system-auth-control**

To globally enable 802.1X SystemAuthControl (port-based authentication), use the `dot1x system-auth-control` command in global configuration mode. To disable SystemAuthControl, use the `no` form of this command.

```
dot1x system-auth-control
no dot1x system-auth-control
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

System authentication is disabled by default. If this command is disabled, all ports behave as if they are force authorized.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)XA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>This command was implemented on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXB.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

The `no` form of the command removes any 802.1X-related configurations.

**Catalyst 6500 Series Switch and Cisco 7600 Series**

You must enable Authentication, Authorization, and Accounting (AAA) and specify the authentication method list before enabling 802.1X. A method list describes the sequence and authentication methods to be queried to authenticate a user.

**Examples**

The following example shows how to enable SystemAuthControl:
Router(config)# dot1x system-auth-control

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa authentication dot1x</td>
<td>Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.</td>
</tr>
<tr>
<td>aaa new-model</td>
<td>Enables the AAA access-control model.</td>
</tr>
<tr>
<td>debug dot1x</td>
<td>Displays 802.1X debugging information.</td>
</tr>
<tr>
<td>description</td>
<td>Specifies a description for an 802.1X profile.</td>
</tr>
<tr>
<td>device</td>
<td>Statically authorizes or rejects individual devices.</td>
</tr>
<tr>
<td>dot1x initialize</td>
<td>Initializes 802.1X state machines on all 802.1X-enabled interfaces.</td>
</tr>
<tr>
<td>dot1x max-req</td>
<td>Sets the maximum number of times that a router or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.</td>
</tr>
<tr>
<td>dot1x port-control</td>
<td>Enables manual control of the authorized state of a controlled port.</td>
</tr>
<tr>
<td>dot1x re-authenticate</td>
<td>Manually initiates a reauthentication of the specified 802.1X-enabled ports.</td>
</tr>
<tr>
<td>dot1x reauthentication</td>
<td>Globally enables periodic reauthentication of the client PCs on the 802.1X interface.</td>
</tr>
<tr>
<td>dot1x timeout</td>
<td>Sets retry timeouts.</td>
</tr>
<tr>
<td>identity profile</td>
<td>Creates an identity profile and enters identity profile configuration mode.</td>
</tr>
<tr>
<td>show dot1x</td>
<td>Displays details and statistics for an identity profile.</td>
</tr>
<tr>
<td>template</td>
<td>Specifies a virtual template from which commands may be cloned.</td>
</tr>
</tbody>
</table>
### dot1x timeout

To configure the value for retry timeouts, use the `dot1x timeout` command in global configuration or interface configuration mode. To return to the default value for retry timeouts to, use the `no` form of this command.

#### All Platforms Except the Cisco 7600 Series Switch

```
dot1x timeout {auth-period seconds|held-period seconds|quiet-period seconds|ratelimit-period seconds|reauth-period {seconds|server}|server-timeout seconds|start-period seconds|supp-timeout seconds|tx-period seconds}
no dot1x timeout {auth-period seconds|held-period seconds|quiet-period seconds|ratelimit-period seconds|reauth-period {seconds|server}|server-timeout seconds|start-period seconds|supp-timeout seconds|tx-period seconds}
```

#### Cisco 7600 Series Switch

```
dot1x timeout {reauth-period seconds|quiet-period seconds|tx-period seconds|supp-timeout seconds|server-timeout seconds}
no dot1x timeout {reauth-period|quiet-period|tx-period|supp-timeout|server-timeout}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>auth-period seconds</strong></td>
<td>Configures the time, in seconds, the supplicant (client) waits for a response from an authenticator (for packets other than Extensible Authentication Protocol over LAN [EAPOL]-Start) before timing out.</td>
</tr>
<tr>
<td></td>
<td>• The range is from 1 to 65535. The default is 30.</td>
</tr>
<tr>
<td><strong>held-period seconds</strong></td>
<td>Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt).</td>
</tr>
<tr>
<td></td>
<td>• The range is from 1 to 65535. The default is 60.</td>
</tr>
<tr>
<td><strong>quiet-period seconds</strong></td>
<td>Configures the time, in seconds, that the authenticator (server) remains quiet (in the HELD state) following a failed authentication exchange before trying to reauthenticate the client.</td>
</tr>
<tr>
<td></td>
<td>• For all platforms except the Cisco 7600 series Switch, the range is from 1 to 65535. The default is 120.</td>
</tr>
<tr>
<td></td>
<td>• For the Cisco 7600 series Switch, the range is from 0 to 65535. The default is 60.</td>
</tr>
<tr>
<td><strong>ratelimit-period seconds</strong></td>
<td>Throttles the EAP-START packets that are sent from misbehaving client PCs (for example, PCs that send EAP-START packets that result in the wasting of switch processing power).</td>
</tr>
<tr>
<td></td>
<td>• The authenticator ignores EAPOL-Start packets from clients that have successfully authenticated for the rate-limit period duration.</td>
</tr>
<tr>
<td></td>
<td>• The range is from 1 to 65535. By default, rate limiting is disabled.</td>
</tr>
</tbody>
</table>
Configure the time, in seconds, after which an automatic reauthentication should be initiated.

- The **server** keyword indicates that the reauthentication period value for the client should be obtained from the authentication, authorization, and accounting (AAA) server as the Session-Timeout (RADIUS Attribute 27) value. If the **server** keyword is used, the action upon reauthentication is also decided by the server and sent as the Termination-Action (RADIUS Attribute 29) value. The termination action could be either "terminate" or "reauthenticate." If the **server** keyword is not used, the termination action is always "reauthenticate."

- For all platforms except the Cisco 7600 series switch, the range is from 1 to 65535. The default is 3600.

- For the Cisco 7600 series switch, the range is from 1 to 4294967295. The default is 3600. See the "Usage Guidelines" section for additional information.

**Note** Effective with Cisco IOS Release 12.2(33)SXI, this phrase is replaced by the **authentication timer reauthenticate** command. See the **authentication timer reauthenticate** command for more information.

---

### server-timeout

```
seconds
```

Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted.

- For all platforms except the Cisco 7600 series switch, the range is from 1 to 65535. The default is 30.

- For the Cisco 7600 series switch, the range is from 30 to 65535. The default is 30.

If the server does not send a response to an 802.1X packet within the specified period, the packet is sent again.

---

### start-period

```
seconds
```

Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted.

- The value is from 1 to 65535. The default is 30.

---

### supp-timeout

```
seconds
```

Sets the authenticator-to-supplicant retransmission time for all EAP messages other than EAP Request ID.

- For all platforms except the Cisco 7600 series Switch, the range is from 1 to 65535. The default is 30.

- For the Cisco 7600 series Switch, the range is from 30 to 65535. The default is 30.
Configure the number of seconds between retransmission of EAP request ID packets (assuming that no response is received) to the client.

- For all platforms except the Cisco 7600 series switch, the range is from 1 to 65535. The default is 30.
- For the Cisco 7600 series switch, the range is from 30 to 65535. The default is 30.
- If an 802.1X packet is sent to the supplicant and the supplicant does not send a response after the retry period, the packet will be sent again.

**Command Default**

Periodic reauthentication and periodic rate-limiting are not done.

**Command Modes**

Global configuration
Interface configuration

**Cisco 7600 Switch**

Interface configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>This command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.3(2)XA</td>
<td>This command was integrated into Cisco IOS Release 12.3(2)XA.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>12.2(18)SE</td>
<td>Ranges for the server-timeout, supp-timeout, and tx-period keywords were changed.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was added for Cisco IOS Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.3(11)T</td>
<td>The auth-period, held-period, and start-period keywords were added.</td>
</tr>
<tr>
<td>12.2(25)SEC</td>
<td>The range for the tx-period keyword was changed, and the reauth-period and server-timeout keywords were added.</td>
</tr>
<tr>
<td>12.1(11)AX</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(14)EA1</td>
<td>The supp-timeout and server-timeout keywords were added. The configuration mode for the command was changed to interface configuration mode.</td>
</tr>
<tr>
<td>12.4(6)T</td>
<td>The supp-timeout keyword was added, and this command was integrated into Cisco IOS Release 12.4(6)T.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td>This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Switches (ISRs) only.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Modification
---
Release | Modification
--- | ---
12.2(33)SXI | The `reauth-period` keyword was replaced by the `authentication timer` `reauthenticate` command.

Usage Guidelines
For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Cisco 7600 Switch
You must enable periodic reauthentication before you enter the `dot1x timeout reauth-period` command. Enter the `dot1x reauthentication` command to enable periodic reauthentication. The `dot1x timeout reauth-period` command affects the behavior of the system only if periodic reauthentication is enabled.

Examples
The following example shows that various 802.1X retransmission and timeout periods have been set:

```
Switch(config)# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout auth-period 2000
Switch(config-if)# dot1x timeout held-period 2400
Switch(config-if)# dot1x timeout reauth-period 1800
Switch(config-if)# dot1x timeout quiet-period 600
Switch(config-if)# dot1x timeout start-period 90
Switch(config-if)# dot1x timeout supp-timeout 300
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x timeout server-timeout 60
```

The following example shows how to return to the default reauthorization period:

```
Switch(config-if)# no dot1x timeout reauth-period
```

Cisco 7600 Switch
The following example shows how to set 802.1X retransmission and timeout periods on the Cisco 7600 Switch:

```
Switch(config-if)# dot1x timeout reauth-period 4000
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x timeout supp-timeout 25
Switch(config-if)# dot1x timeout server-timeout 25
```

802.1X Support on a Cisco 870 ISR for Cisco IOS Release 12.4(4)XC
The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
  description  switchport connect to a client
```
interface FastEthernet1
description switchport connect to a client
!
interface FastEthernet2
description switchport connect to a client
!
interface FastEthernet3
description switchport connect to a client
!
interface FastEthernet4
description Connect to the public network
!
interface Vlan1
description Apply 802.1x functionality on SVI
dot1x pae authenticator
dot1x port-control auto

dot1x reauthentication

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x max-req</td>
<td>Sets the maximum number of times that a switch or Ethernet switch module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.</td>
</tr>
<tr>
<td>dot1x port-control</td>
<td>Sets an 802.1X port control value.</td>
</tr>
<tr>
<td>dot1x re-authentication</td>
<td>Globally enables periodic reauthentication of the client PCs on the 802.1X interface.</td>
</tr>
<tr>
<td>show dot1x</td>
<td>Displays 802.1X information.</td>
</tr>
</tbody>
</table>
dot1x timeout (EtherSwitch)

To set the number of retry seconds between 802.1X authentication exchanges when an Ethernet switch network module is installed in the router, use the `dot1x timeout` command in global configuration mode. To return to the default setting, use the `no` form of this command.

```
dot1x timeout {quiet-period seconds|re-authperiod seconds|tx-period seconds}
nodot1x timeout {quiet-period seconds|re-authperiod seconds|tx-period seconds}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>quiet-period seconds</td>
<td>Specifies the time in seconds that the Ethernet switch network module remains in the quiet state following a failed authentication exchange with the client. The range is from 0 to 65535 seconds. The default is 60 seconds.</td>
</tr>
<tr>
<td>re-authperiod seconds</td>
<td>Specifies the number of seconds between reauthentication attempts. The range is from 1 to 4294967295. The default is 3660 seconds.</td>
</tr>
<tr>
<td>tx-period seconds</td>
<td>Time in seconds that the switch should wait for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is from 1 to 65535 seconds. The default is 30 seconds.</td>
</tr>
</tbody>
</table>

**Command Default**

<table>
<thead>
<tr>
<th>Command Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>quiet-period : 60 seconds</td>
</tr>
<tr>
<td>re-authperiod: 3660 seconds</td>
</tr>
<tr>
<td>tx-period: 30 seconds</td>
</tr>
</tbody>
</table>

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(6)EA2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)ZJ</td>
<td>This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You should change the default values of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients or authentication servers.

**quiet-period Keyword**

During the quiet period, the Ethernet switch network module does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a smaller number than the default.

**re-authperiod Keyword**

The `re-authperiod` keyword affects the behavior of the Ethernet switch network module only if you have enabled periodic reauthentication by using the `dot1x re-authentication` global configuration command.

**Examples**

The following example shows how to set the quiet time on the switch to 30 seconds:
Router(config)# dot1x timeout quiet-period 30

The following example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000 seconds:

Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000

The following example shows how to set 60 seconds as the amount of time that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request:

Router(config)# dot1x timeout tx-period 60

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x max-req</td>
<td>Sets the maximum number of times that the device sends an EAP-request/identity frame before restarting the authentication process.</td>
</tr>
<tr>
<td>dot1x re-authentication</td>
<td>Enables periodic reauthentication of the client for the Ethernet switch network module.</td>
</tr>
<tr>
<td>(EtherSwitch)</td>
<td></td>
</tr>
<tr>
<td>show dot1x (EtherSwitch)</td>
<td>Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.</td>
</tr>
</tbody>
</table>
To configure Dead Peer Detection (DPD), use the `dpd` command in IKEv2 profile configuration mode. To delete DPD, use the `no` form of this command.

```
dpd  interval retry-interval {on-demand|periodic}
no  dpd
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interval</code></td>
<td>Specifies the keepalive interval in seconds. The range is 10 to 3600.</td>
</tr>
<tr>
<td><code>retry-interval</code></td>
<td>Specifies the retry interval in seconds when there is no reply from the peer.</td>
</tr>
<tr>
<td><code>on-demand</code></td>
<td>Specifies the on-demand mode to send the keepalive only in the absence of any incoming data traffic, to check the liveness of the peer before sending any data.</td>
</tr>
<tr>
<td><code>periodic</code></td>
<td>Specifies the periodic mode to send keepalives regularly at a specified interval.</td>
</tr>
</tbody>
</table>

**Command Default**

DPD is disabled by default.

**Command Modes**

IKEv2 profile configuration (config-ikev2-profile)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to configure DPD globally for peers matching a profile. The DPD configuration in an Internet Key Exchange Version 2 (IKEv2) profile overrides the global DPD configuration.

**Examples**

The following example shows how to configure the periodic mode for DPD:

```
Router(config)# crypto ikev2 profile prf1
Router(config-ikev2-profile)# dpd 1000 250 periodic
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2 dpd</td>
<td>Defines DPD globally for all peers.</td>
</tr>
<tr>
<td>crypto ikev2 profile</td>
<td>Defines IKEv2 profile.</td>
</tr>
</tbody>
</table>
drop (type access-control)

Effective with Cisco IOS Release 15.2(4)M, the drop command is not available in Cisco IOS software.

To configure a traffic class to discard packets belonging to a specific class, use the drop command in policy-map class configuration mode. To disable the packet discarding action in a traffic class, use the no form of this command.

```
drop [all]
no drop [all]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>(Optional) Discards the entire stream of packets belonging to the traffic class.</td>
</tr>
</tbody>
</table>

**Command Default**
The packet discarding action in a traffic class is disabled.

**Command Modes**
Policy-map class configuration (config-pmap-c)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(3)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(4)M</td>
<td>This command was removed from the Cisco IOS software.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Once the match criteria are applied to packets belonging to the specific traffic class using the match class session command in a class map, these packets can be discarded by configuring the drop command with the all keyword in a policy map. Packets match only on the packet session (flow) entry of the Flexible Packet Matching (FPM) access control list (ACL) pattern matching tool, and skip user-configured classification filters. When the drop command is specified with the all keyword, this command can only be associated with a class map that was created with the class-map command and type access-control keyword and used in a policy map that can be attached to one or more interfaces to specify a service policy that is created with the policy-map command and type access-control keyword.

**Examples**
The following example shows how to create and configure a traffic class called class1 for use in a policy map called policy1. The policy map (service policy) is attached to output serial interface 2/0. All packets that match access group 101 are placed in class1. Packets that belong to this class are discarded.

```
Router(config)# class-map class1
Router(config-cmap)# match access-group 101
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial2/0
```
The following example shows how to configure a class map and policy map to specify the protocol stack class, the match criteria and action to take, and a combination of classes using session-based (flow-based) and nonsession-based actions. The **drop all** command is associated with the action to be taken on the policy.

```
Router(config)# class-map type access-control match-all my-HTTP
Router(config-cm)# match field tcp destport eq 8080
Router(config-cm)# match start tcp payload-start offset 20 size 10 regex "GET"
Router(config)# class-map type access-control match-all my-FTP
Router(config-cm)# match field tcp destport eq 21
Router(config)# class-map type access-control match all class1
Router(config-cm)# match class my-HTTP session
Router(config-cm)# match start tcp payload-start offset 40 size 20 regex "abc.*def"
Router(config)# policy-map type access-control my_http_policy
Router(config-pmap)# class class1
Router(config-pmap-c)# drop all
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input my_http_policy
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class</td>
<td>Specifies the name of a predefined traffic class, which was configured with the <strong>class-map</strong> command. The class command also classifies traffic to the traffic policy and enters policy-map class configuration mode.</td>
</tr>
<tr>
<td>class-map type access-control</td>
<td>Creates a class map to be used for matching packets to a specified class and enters class-map configuration mode for determining the exact pattern to look for in the protocol stack of interest.</td>
</tr>
<tr>
<td>log</td>
<td>Generates log messages for a predefined traffic class.</td>
</tr>
<tr>
<td>match class session</td>
<td>Configures match criteria for a class map used to identify a session (flow) containing packets of interest, which is then applied to all packets transmitted during the session.</td>
</tr>
<tr>
<td>policy-map type access-control</td>
<td>Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy, and enters policy-map configuration mode.</td>
</tr>
<tr>
<td>show class-map</td>
<td>Displays all class maps and their matching criteria.</td>
</tr>
<tr>
<td>show policy-map</td>
<td>Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.</td>
</tr>
<tr>
<td>show policy-map interface</td>
<td>Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.</td>
</tr>
</tbody>
</table>
drop (zone-based policy)

To drop packets that are sent to a device, use the drop command in policy-map class configuration mode. To stop the dropping of traffic packets, use the no form of this command.

```
drop [log]
no drop
```

### Syntax Description

- **log** (Optional) Displays logging messages about dropped packets.

### Command Default

Packets are not dropped.

### Command Modes

Policy-map class configuration (config-pmap-c)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(1)S</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)S.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.12S</td>
<td>This command was integrated into Cisco IOS XE Release 3.12S.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Before you configure the drop command, you must configure the policy-map type inspect and class type inspect commands.

In Cisco IOS Release 15.1(2)T and earlier releases, if you use the drop command to configure a zone-based firewall with IP multicast traffic, all multicast updates are dropped by the zone-based firewall.

In Cisco IOS Release 15.1(3)T and later releases, all multicast updates are passed by the zone-based firewall even if you explicitly configure the drop command for a zone-based firewall with IP multicast traffic.

### Examples

The following example shows how to create a policy map that drops all traffic:

```
Device(config)# policy-map type inspect p1
Device(config-pmap)# class type inspect c1
Device(config-pmap-c)# drop
```

The following example shows how to create a policy map that drops HTTP traffic:

```
Device(config)# access-list 101 permit ip 192.168.1 0.0.0.255 any
Device(config-ext-nacl)# exit
Device(config)# class-map type inspect match-all c1
Device(config-cmap)# match access-group 101
Device(config-cmap)# match protocol http
Device(config-cmap)# exit
Device(config)# policy-map type inspect p1
Device(config-pmap)# class type inspect c1
Device(config-pmap-c)# drop
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class type inspect</td>
<td>Specifies the traffic class on which an action is to be performed.</td>
</tr>
<tr>
<td>policy-map type inspect</td>
<td>Creates Layer 3 and Layer 4 inspect type policy maps.</td>
</tr>
</tbody>
</table>
**drop-unsecure**

To drop messages with no or invalid options or an invalid signature, use the `drop-unsecure` command in neighbor discovery (ND) inspection policy configuration mode or or router advertisement (RA) guard policy configuration mode. To disable this function, use the `no` form of this command.

```
drop-unsecure
no drop-unsecure
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No ND inspection policies are configured.

**Command Modes**

ND inspection policy configuration (config-nd-inspection)

RA guard policy configuration (config-ra-guard)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(2)SE</td>
<td>This command was integrated into Cisco IOS Release 15.0(2)SE.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `drop-unsecure` command drops messages with no or invalid Cryptographically Generated Address (CGA) options or Rivest, Shamir, and Adleman (RSA) signature as per RFC 3971, Secure Discovery (SeND). However, note that messages with an RSA signature or CGA options that do not conform with or are not verified per RFC 3972, Cryptographically Generated Addresses (CGA), are dropped.

Use the `drop-unsecure` command after enabling ND inspection policy configuration mode using the `ipv6 nd inspection policy` command.

**Examples**

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and enables the router to drop messages with invalid CGA options or an invalid RSA signature:

```
Router(config)# ipv6 nd-inspection policy policy1
Router(config-nd-inspection)# drop-unsecure
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 nd inspection policy</code></td>
<td>Defines the ND inspection policy name and enters ND inspection policy configuration mode.</td>
</tr>
<tr>
<td><code>ipv6 nd raguard policy</code></td>
<td>Defines the RA guard policy name and enters RA guard policy configuration mode.</td>
</tr>
</tbody>
</table>
**dtls port**

To configure a desired port for the Datagram Transport Layer Security (DTLS) to listen, use the `dtls port` command in WebVPN gateway configuration mode. To disable the port, use the `no` form of this command.

```
dtls port port-number
no dtls port port-number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Port-number</th>
<th>Description</th>
</tr>
</thead>
</table>

**Command Default**

The default DTLS port is 443.

**Command Modes**

WebVPN gateway configuration (config-webvpn-gateway)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

DTLS listens on port 443 by default. You can configure the desired DTLS port using the `dtls port` command.

**Examples**

The following example shows how to configure 1055 as the DTLS port for a WebVPN gateway “gateway1”:

```
Router# configure terminal
Router(config)# webvpn gateway gateway1
Router(config-webvpn-gateway)# dtls port 1055
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>svc dtls</td>
<td>Enables DTLS support on the Cisco IOS SSL VPN.</td>
</tr>
</tbody>
</table>
**dynamic**

To define a named dynamic IP access list, use the `dynamic` command in access-list configuration mode. To remove the access lists, use the `no` form of this command.

```
dynamic dynamic-name [timeout minutes] {deny|permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log] [fragments]
no dynamic dynamic-name
```

**Internet Control Message Protocol (ICMP)**

```
dynamic dynamic-name [timeout minutes] {deny|permit} icmp source source-wildcard destination destination-wildcard [icmp-type [icmp-code]icmp-message] [precedence precedence] [tos tos] [log] [fragments]
```

**Internet Group Management Protocol (IGMP)**

```
dynamic dynamic-name [timeout minutes] {deny|permit} igmp source source-wildcard destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [log] [fragments]
```

**Transmission Control Protocol (TCP)**

```
dynamic dynamic-name [timeout minutes] {deny|permit} tcp source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [established] [precedence precedence] [tos tos] [log] [fragments]
```

**User Datagram Protocol (UDP)**

```
dynamic dynamic-name [timeout minutes] {deny|permit} udp source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [precedence precedence] [tos tos] [log] [fragments]
```

### Syntax Description

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>dynamic-name</strong></td>
<td>Identifies this access list as a dynamic access list. Refer to lock-and-key access documented in the “Configuring Lock-and-Key Security (Dynamic Access Lists)” chapter in the <em>Cisco IOS Security Configuration Guide</em>.</td>
</tr>
<tr>
<td><strong>timeout minutes</strong></td>
<td>(Optional) Specifies the absolute length of time (in minutes) that a temporary access-list entry can remain in a dynamic access list. The default is an infinite length of time and allows an entry to remain permanently. Refer to lock-and-key access documented in the “Configuring Lock-and-Key Security (Dynamic Access Lists)” chapter in the <em>Cisco IOS Security Configuration Guide</em>.</td>
</tr>
<tr>
<td><strong>deny</strong></td>
<td>Denies access if the conditions are matched.</td>
</tr>
<tr>
<td><strong>permit</strong></td>
<td>Permits access if the conditions are matched.</td>
</tr>
<tr>
<td><strong>protocol</strong></td>
<td>Name or number of an Internet protocol. It can be one of the keywords <code>eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, or udp</code>, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the <code>ip</code> keyword. Some protocols allow further qualifiers described later.</td>
</tr>
</tbody>
</table>
| **source** | Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:
| | • Use a 32-bit quantity in four-part, dotted decimal format.  
| | • Use the `any` keyword as an abbreviation for a `source` and `source-wildcard` of `0.0.0.0` `255.255.255.255`.  
| | • Use `host source` as an abbreviation for a `source` and `source-wildcard` of `source 0.0.0.0`. |
| **source-wildcard** | Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard:
| | • Use a 32-bit quantity in four-part, dotted decimal format. Place 1s in the bit positions you want to ignore.  
| | • Use the `any` keyword as an abbreviation for a `source` and `source-wildcard` of `0.0.0.0` `255.255.255.255`.  
| | • Use `host source` as an abbreviation for a `source` and `source-wildcard` of `source 0.0.0.0`. |
| **destination** | Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination:
| | • Use a 32-bit quantity in four-part, dotted decimal format.  
| | • Use the `any` keyword as an abbreviation for the `destination` and `destination-wildcard` of `0.0.0.0` `255.255.255.255`.  
| | • Use `host destination` as an abbreviation for a `destination` and `destination-wildcard` of `destination 0.0.0.0`. |
| **destination-wildcard** | Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:
| | • Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore.  
| | • Use the `any` keyword as an abbreviation for a `destination` and `destination-wildcard` of `0.0.0.0` `255.255.255.255`.  
| | • Use `host destination` as an abbreviation for a `destination` and `destination-wildcard` of `destination 0.0.0.0`. |
| **precedence** | (Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7, or by name as listed in the section “Usage Guidelines.” |
| **tos** | (Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by name as listed in the section “Usage Guidelines.” |
log  (Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the logging console command.)

The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.

The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

fragments  (Optional) The access-list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the fragments keyword, see the “Access List Processing of Fragments” and “Fragments and Policy Routing” sections in the “Usage Guidelines” section.

icmp-type  (Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.

icmp-code  (Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.

icmp-message  (Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the section “Usage Guidelines.”

igmp-type  (Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section “Usage Guidelines.”

operator  (Optional) Compares source or destination ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).

If the operator is positioned after the source and source-wildcard, it must match the source port.

If the operator is positioned after the destination and destination-wildcard, it must match the destination port.

The range operator requires two port numbers. All other operators require one port number.

port  (Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the section “Usage Guidelines” of the access-list(IP extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.

established  (Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
**Command Default**

An extended access list defaults to a list that denies everything. An extended access list is terminated by an implicit deny statement.

**Command Modes**

Access-list configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(11)</td>
<td>The <code>fragments</code> keyword was added.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>The <code>igrp</code> keyword was removed because the IGRP protocol is no longer available in Cisco IOS software.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can use named access lists to control the transmission of packets on an interface and restrict contents of routing updates. The Cisco IOS software stops checking the extended access list after a match occurs. Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list. Extended access lists used to control vty access or restrict the contents of routing updates must not match against the TCP source port, the ToS value, or the precedence of the packet.

**Note**

Named IP access lists will not be recognized by any software release prior to Cisco IOS Release 11.2.

**Note**

After an access list is created, any subsequent additions (possibly entered from the terminal) are placed at the end of the list. In other words, you cannot selectively add or remove access list command lines from a specific access list.

The following is a list of precedence names:

- `critical`
- `flash`
- `flash-override`
- `immediate`
- `internet`
- `network`
- `priority`
- `routine`
The following is a list of ToS names:

- max-reliability
- max-throughput
- min-delay
- min-monetary-cost
- normal

The following is a list of ICMP message type and code names:

- administratively-prohibited
- alternate-address
- conversion-error
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
• no-room-for-option
• option-missing
• packet-too-big
• parameter-problem
• port-unreachable
• precedence-unreachable
• protocol-unreachable
• reassembly-timeout
• redirect
• router-advertisement
• router-solicitation
• source-quench
• source-route-failed
• time-exceeded
• timestamp-reply
• timestamp-request
• traceroute
• ttl-exceeded
• unreachable

The following is a list of IGMP message names:
• dvmrp
• host-query
• host-report
• pim
• trace

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a ? in the place of a port number.
• bgp
• chargen
• daytime
• discard
The following is a list of UDP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a ? in the place of a port number.

- biff
- bootpc
- bootps
- discard
- dns
- dnsix
- echo
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- ntp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs-ds
- talk
- tftp
- time
- who
- xdmcp

**Access List Processing of Fragments**

The behavior of access-list entries regarding the use or lack of the `fragments` keyword can be summarized as follows:
If the Access-List Entry has... | Then...
---|---
...no `fragments` keyword (the default behavior), and assuming all of the access-list entry information matches, | For an access-list entry containing only Layer 3 information:
  - The entry is applied to nonfragmented packets, initial fragments and noninitial fragments.

For an access-list entry containing Layer 3 and Layer 4 information:
  - The entry is applied to nonfragmented packets and initial fragments.
    - If the entry is a `permit` statement, the packet or fragment is permitted.
    - If the entry is a `deny` statement, the packet or fragment is denied.
  - The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and
    - If the entry is a `permit` statement, the noninitial fragment is permitted.
    - If the entry is a `deny` statement, the next access-list entry is processed.

**Note**
The `deny` statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.

...the `fragments` keyword, and assuming all of the access-list entry information matches, | The access-list entry is applied only to noninitial fragments. The `fragments` keyword cannot be configured for an access-list entry that contains any Layer 4 information.

---

Be aware that you should not simply add the `fragments` keyword to every access-list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list `permit` or `deny` entry that contains the `fragments` keyword, the packet is compared to the next access-list entry, and so on, until it is either permitted or denied by an access-list entry that does not contain the `fragments` keyword. Therefore, you may need two access-list entries for every `deny` entry. The first `deny` entry of the pair will not include the `fragments` keyword, and applies to the initial fragment. The second `deny` entry of the pair will include the `fragments` keyword and applies to the subsequent fragments. In the cases where there are multiple `deny` access-list entries for the same host but with different Layer 4 ports, a single `deny` access-list entry with the `fragments` keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

**Note**
The `fragments` keyword cannot solve all cases involving access lists and IP fragments.

**Fragments and Policy Routing**
Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the `match ip address` command and the access list had entries that match on Layer 4 through 7 information. It
is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the `fragments` keyword in access-list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

### Examples

The following example defines a dynamic access list named abclist:

```plaintext
ip access-group abclist in
!
ip access-list extended abclist
dynamic testlist timeout 5
permit ip any any
permit tcp any host 10.302.21.2 eq 23
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear access-template</td>
<td>Clears a temporary access-list entry from a dynamic access list manually.</td>
</tr>
<tr>
<td>distribute-list in (IP)</td>
<td>Filters networks received in updates.</td>
</tr>
<tr>
<td>distribute-list out (IP)</td>
<td>Suppresses networks from being advertised in updates.</td>
</tr>
<tr>
<td>ip access-group</td>
<td>Controls access to an interface.</td>
</tr>
<tr>
<td>ip access-list</td>
<td>Defines an IP access list by name.</td>
</tr>
<tr>
<td>logging console</td>
<td>Limits messages logged to the console based on severity.</td>
</tr>
<tr>
<td>show access-lists</td>
<td>Displays the contents of current IP and rate-limit access lists.</td>
</tr>
<tr>
<td>show ip access-list</td>
<td>Displays the contents of all current IP access lists.</td>
</tr>
</tbody>
</table>
E

• eap, on page 209
• eap (IKEv2 profile), on page 210
• eckeypair, on page 212
• eku (cs-server), on page 213
• eku request, on page 215
• email (IKEv2 profile), on page 217
• enable, on page 218
• enable algorithm-type, on page 221
• enable password, on page 223
• enable secret, on page 225
• enabled (IPS), on page 229
• encryption (IKE policy), on page 230
• encryption (IKEv2 proposal), on page 232
• enforce-checksum, on page 234
• engine (IPS), on page 235
• enrollment, on page 236
• enrollment command, on page 239
• enrollment credential, on page 240
• enrollment http-proxy, on page 242
• enrollment mode ra, on page 243
• enrollment profile, on page 244
• enrollment retry count, on page 245
• enrollment retry period, on page 246
• enrollment selfsigned, on page 247
• enrollment terminal (ca-profile-enroll), on page 248
• enrollment terminal (ca-trustpoint), on page 249
• enrollment url (ca-identity), on page 251
• enrollment url (ca-profile-enroll), on page 252
• enrollment url (ca-trustpoint), on page 254
• eou allow, on page 258
• eou clientless, on page 259
• eou default, on page 260
• eou initialize, on page 261
- eou logging, on page 262
- eou max-retry, on page 263
- eou port, on page 264
- eou rate-limit, on page 265
- eou revalidate, on page 266
- eou timeout, on page 268
- error-msg, on page 269
- error-url, on page 270
- evaluate, on page 271
- evaluate (IPv6), on page 273
- event-action, on page 275
- exception access-group, on page 277
- exclusive-domain, on page 279
This command is removed effective with Cisco IOS Release 12.4(6)T.

To specify Extensible Authentication Protocol- (EAP-) specific parameters, use the `eap` command in identity profile configuration mode. To disable the parameters that were set, use the `no` form of this command.

```
eap {username name|password password}
no eap {username name|password password}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username name</td>
<td>Username that will be sent to Request-Id packets.</td>
</tr>
<tr>
<td>password password</td>
<td>Password that should be used when replying to an Message Digest 5 (MD5) challenge.</td>
</tr>
</tbody>
</table>

**Command Default**

EAP parameters are not set.

**Command Modes**

Identity profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(11)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(6)T</td>
<td>This command was removed.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.33SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command if your router is configured as a supplicant. This command provides the means for configuring the identity and the EAP MD5 password that will be used by 802.1X to authenticate.

**Examples**

The following example shows that the EAP username “user1” has been configured:

```
Router (config)# identity profile dot1x
Router (config-identity-prof)# eap username user1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>identity profile</td>
<td>Creates an identity profile.</td>
</tr>
</tbody>
</table>
eap (IKEv2 profile)

To derive the name mangler from the remote identity of type Extensible Authentication Protocol (EAP), use the `eap` command in IKEv2 name mangler configuration mode. To remove the name derived from EAP, use the `no` form of this command.

```plaintext
eap { all | dn { country | domain | locality | organization | organization-unit | state } { prefix | suffix } { delimiter { . | @ | \ } } }
no eap
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>Derives the name mangler from the entire EAP identity.</td>
</tr>
<tr>
<td><code>dn</code></td>
<td>Derives the name from identities of type DN in EAP.</td>
</tr>
<tr>
<td><code>country</code></td>
<td>Derives the name from the country name specified in the DN.</td>
</tr>
<tr>
<td><code>domain</code></td>
<td>Derives the name from the domain name specified in the DN.</td>
</tr>
<tr>
<td><code>locality</code></td>
<td>Derives the name from the locality specified in the DN.</td>
</tr>
<tr>
<td><code>organization</code></td>
<td>Derives the name from the organization specified in the DN.</td>
</tr>
<tr>
<td><code>organization-unit</code></td>
<td>Derives the name from the organization-unit specified in the DN.</td>
</tr>
<tr>
<td><code>state</code></td>
<td>Derives the name from the state name specified in the DN.</td>
</tr>
<tr>
<td><code>prefix</code></td>
<td>Derives the name from the prefix in EAP.</td>
</tr>
<tr>
<td><code>suffix</code></td>
<td>Derives the name from the suffix in EAP.</td>
</tr>
<tr>
<td><code>delimiter</code></td>
<td>Refers to the specified delimiter in the prefix or suffix.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

IKEv2 name mangler configuration (config-ikev2-name-mangler)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(3)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to derive the name mangler from any field in the remote identity of type EAP.

### Examples

The following example shows how to derive a name for the name mangler from a specific delimiter in EAP prefix:

```plaintext
Cisco IOS Security Command Reference: Commands D to L
```
Router(config)# crypto ikev2 name-mangler mangler2
Router(config-ikev2-name-mangler)# eap prefix delimiter @

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>crypto ikev2 name mangler</td>
<td>Defines a name mangler.</td>
</tr>
</tbody>
</table>
eckeypair

To configure the trustpoint to use an Elliptic Curve (EC) key on which certificate requests are generated using ECDSA signatures, use the `eckeypair` command in ca-trustpoint configuration mode. To remove the encryption key, use the `no` form of this command.

```
eckeypair label
no eckeypair label
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>label</code></td>
<td>Specifies the EC key label that is configured using the <code>crypto key generate rsa</code> or <code>crypto key generate ec keysizes</code> command in global configuration mode. See the Configuring Internet Key Exchange for IPsec VPNs feature module for more information.</td>
</tr>
</tbody>
</table>

**Command Default**

The trustpoint is not configured with an EC key.

**Command Modes**

Ca-trustpoint configuration mode (ca-trustpoint)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(2)T</td>
<td>This command was introduced in Cisco IOS Release 15.1(2)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If an ECDSA signed certificate is imported without a trustpoint configuration, then the label defaults to the FQDN value.

**Examples**

The following example configures the EC key label in a certificate enrollment in a PKI:

```
Router(config)#
crypto pki trustpoint mytp
Router(ca-trustpoint)# eckeypair Router_1_Key
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crypto key generate ec keysizes</code></td>
<td>Generates EC keys.</td>
</tr>
<tr>
<td><code>crypto key generate rsa</code></td>
<td>Generates RSA keys.</td>
</tr>
<tr>
<td><code>crypto pki trustpoint</code></td>
<td>Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.</td>
</tr>
</tbody>
</table>
eku (cs-server)

To configure the extended key usage (EKU) parameters, use the `eku` command in certificate server configuration mode. To remove the EKU parameters, use the `no` form of this command.

```
eku  attribute

no  ek u  attribute
```

### Syntax Description

| `attribute` | The `attribute` argument can be one of the following:
| --- | --- |
| • client-auth
| • code-signing
| • email-protection
| • ipsec-end-system
| • ipsec-tunnel
| • ipsec-user
| • ocsp-signing
| • server-auth
| • ssh-client
| • ssh-server
| • time-stamping

### Command Default

EKU attributes are not set by the certificate server in a requested certificate.

### Command Modes

Certificate server configuration (cs-server)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS 15.2(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `crypto pki server` command in global configuration mode to enable a Cisco IOS certificate server (CS) and to enter certificate server configuration mode (cs-server). The `eku` command allows the certificate server to enforce EKU attributes in a requested certificate.

### Example

The following example shows how to configure the EKU attribute “ssh-client” in the certificate server:

```
Device> enable
Device# configure terminal
Device(config)# crypto pki server mycertserver
Device(cs-server)# eku ssh-client
Device(cs-server)# end

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto pki server</td>
<td>Enables a Cisco IOS certificate server (CS) or immediately generates shadow certification authority (CA) credentials.</td>
</tr>
</tbody>
</table>
**eku request**

To configure the request to include a specific extended key usage (EKU) attribute in the certificate, use the `eku request` command in certification authority (CA) trustpoint configuration mode. To remove the configuration request, use the `no` form of this command.

```
    eku request attribute
    no eku request attribute
```

**Syntax Description**

<table>
<thead>
<tr>
<th>attribute</th>
<th>The attribute argument can be one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• client-auth</td>
</tr>
<tr>
<td></td>
<td>• code-signing</td>
</tr>
<tr>
<td></td>
<td>• email-protection</td>
</tr>
<tr>
<td></td>
<td>• ipsec-end-system</td>
</tr>
<tr>
<td></td>
<td>• ipsec-tunnel</td>
</tr>
<tr>
<td></td>
<td>• ipsec-user</td>
</tr>
<tr>
<td></td>
<td>• ocsp-signing</td>
</tr>
<tr>
<td></td>
<td>• server-auth</td>
</tr>
<tr>
<td></td>
<td>• ssh-client</td>
</tr>
<tr>
<td></td>
<td>• ssh-server</td>
</tr>
<tr>
<td></td>
<td>• time-stamping</td>
</tr>
</tbody>
</table>

**Command Default**

The EKU attributes are not requested during certificate enrollment.

**Command Modes**

Certification authority trustpoint configuration (ca-trustpoint)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS 15.2(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `crypto pki trustpoint` command in global configuration mode to declare the trustpoint and a given name and to enter CA-trustpoint configuration mode.

The `eku request` command under the public key infrastructure (PKI) trust point allows the PKI client to request the listed EKU attributes in the certificates during enrollment. This request, when configured on the PKI client, is sent to the CA server during enrollment.
**Example**

The following example shows how to configure the request to include the EKU attribute “ssh-client” in the certificate:

```
Device> enable
Device# configure terminal
Device(config)# crypto pki trustpoint msca
Device(ca-trustpoint)# eku request ssh-client
Device(ca-trustpoint)# end
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto pki trustpoint</td>
<td>Declares the trustpoint and a given name.</td>
</tr>
<tr>
<td>match eku</td>
<td>Allows a PKI client to validate a peer certificate only if the specified attribute is present in the certificate.</td>
</tr>
</tbody>
</table>
email (IKEv2 profile)

To derive the name mangler from the remote identity of type e-mail, use the `email` command in IKEv2 name mangler configuration mode. To remove the name derived from the e-mail, use the `no` form of this command.

```
email {all|domain|username}
no email
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Derives the name mangler from the entire FQDN.</td>
</tr>
<tr>
<td>domain</td>
<td>Derives the name mangler from the domain name in e-mail.</td>
</tr>
<tr>
<td>hostname</td>
<td>Derives the name mangler from the username in e-mail.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

IKEv2 name mangler configuration (config-ikev2-name-mangler)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(3)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to derive the name mangler from any field in the remote identity of type e-mail.

### Examples

The following example shows how to derive a name for the name mangler from the username in e-mail:

```
Router(config)# crypto ikev2 name-mangler mangler2
Router(config-ikev2-name-mangler)# email username
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2 name mangler</td>
<td>Defines a name mangler.</td>
</tr>
</tbody>
</table>
enable

To change the privilege level for a CLI session or to use a CLI view for a CLI session, use the `enable` command in either user EXEC, privileged EXEC, or diagnostic mode.

```
enable [privilege-level] [view [view-name]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>privilege-level</code></td>
<td>(Optional) Privilege level at which to log in.</td>
</tr>
<tr>
<td><code>view</code></td>
<td>(Optional) Enters into root view, which enables users to configure CLI views.</td>
</tr>
<tr>
<td><code>view-name</code></td>
<td>(Optional) Enters or exits a specified command-line interface (CLI) view. This keyword can be used to switch from one CLI view to another CLI view.</td>
</tr>
<tr>
<td><code>Note</code></td>
<td>This keyword is required if you want to configure a CLI view.</td>
</tr>
</tbody>
</table>

**Command Default**

Privilege-level 15 (privileged EXEC)

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

Diagnostic Mode (diag)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>The <code>view</code> keyword and <code>view-name</code> argument were added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>The <code>view</code> keyword and <code>view-name</code> argument were integrated into Cisco IOS</td>
</tr>
<tr>
<td></td>
<td>Release 12.2(33)SRB.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in</td>
</tr>
<tr>
<td></td>
<td>a specific 12.2SX release of this train depends on your feature set, platform,</td>
</tr>
<tr>
<td></td>
<td>and platform hardware.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(22)SB.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command became available on the ASR 1000 Series Routers, and became</td>
</tr>
<tr>
<td></td>
<td>available in diagnostic mode for the first time.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, using the `enable` command without the `privilege-level` argument in user EXEC mode causes the router to enter privileged EXEC mode (privilege-level 15).

Entering privileged EXEC mode enables the use of privileged commands. Because many of the privileged commands set operating parameters, privileged access should be password-protected to prevent unauthorized use. If the system administrator has set a password with the `enable password` global configuration command,
you are prompted to enter the password before being allowed access to privileged EXEC mode. The password is case sensitive.

If an enable password has not been set, only enable mode can be accessed through the console connection.

Security levels can be set by an administrator using the enable password and privilege level commands. Up to 16 privilege levels can be specified, using the numbers 0 through 15. Using these privilege levels, the administrator can allow or deny access to specific commands. Privilege level 0 is associated with user EXEC mode, and privilege level 15 is associated with privileged EXEC mode.

For more information on defined privilege levels, see the Cisco IOS Security Configuration Guide and the Cisco IOS Security Command Reference publications.

If a level is not specified when entering the enable command, the user will enter the default mode of privileged EXEC (level 15).

Accessing a CLI View

CLI views restrict user access to specified CLI and configuration information. To configure and access CLI views, users must first enter into root view, which is accomplished via the enable view command (without the view-name argument). Thereafter, users are prompted for a password, which is the same password as the privilege level 15 password.

The view-name argument is used to switch from one view to another view.

To prevent dictionary attacks, a user is prompted for a password even if an incorrect view name is given. The user is denied access only after an incorrect view name and password are given.

Examples

In the following example, the user enters privileged EXEC mode (changes to privilege-level 15) by using the enable command without a privilege-level argument. The system prompts the user for a password before allowing access to the privileged EXEC mode. The password is not printed to the screen. The user then exits back to user EXEC mode using the disable command. Note that the prompt for user EXEC mode is the greater than symbol (>), and the prompt for privileged EXEC mode is the number sign (#).

Router> enable
Password: <letmein>
Router# disable
Router>

The following example shows which commands are available inside the CLI view “first” after the user has logged into this view:

Router# enable view first
Password: 
00:28:23:PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
Router# ?
Exec commands:
  configure Enter configuration mode
  enable Turn on privileged commands
  exit Exit from the EXEC
  show Show running system information
Router# show ?
  ip IP information
  parser Display parser information
  version System hardware and software status
Router# show ip ?
The following example shows how to use the `enable view` command to switch from the root view to the CLI view “first”:

```
Router# enable view
Router# show parser view
Current view is 'root'
! Enable the show parser view command from the root view
Router# show parser view all
Views Present in System:
View Name: first
View Name: second
! Switch to the CLI view “first.”
Router# enable view first
Router# show parser view
Current view is 'first'
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Exits from privileged EXEC mode to user EXEC mode, or, if privilege levels are set, to the specified privilege level.</td>
</tr>
<tr>
<td>enable password</td>
<td>Sets a local password to control access to various privilege levels.</td>
</tr>
<tr>
<td>privilege level (global)</td>
<td>Sets a privilege level for a command.</td>
</tr>
<tr>
<td>privilege level (line)</td>
<td>Sets a privilege level for a command for a specific line.</td>
</tr>
</tbody>
</table>
enable algorithm-type

To set the algorithm type to hash a user password configured using the enable secret command, use the enable algorithm-type command in global configuration mode. To remove the algorithm type, use the no form of this command.

enable algorithm-type {md5 | scrypt | sha256}
no enable algorithm-type {md5 | scrypt | sha256}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable algorithm-type {md5</td>
<td>scrypt</td>
</tr>
<tr>
<td>enable algorithm-type {md5</td>
<td>scrypt</td>
</tr>
<tr>
<td>enable algorithm-type {md5</td>
<td>scrypt</td>
</tr>
</tbody>
</table>

Command Default

No algorithm type is defined.

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3(3)M3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.5(1)S</td>
<td>This command was integrated into the Cisco IOS Release 15.5(1)S.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You must configure the password using the enable secret command before hashing the password with the enable algorithm-type command.

Use the enable algorithm-type command to generate the following types of passwords:

<table>
<thead>
<tr>
<th>Command keyword</th>
<th>Type of password</th>
</tr>
</thead>
<tbody>
<tr>
<td>md5</td>
<td>Type 5</td>
</tr>
<tr>
<td>sha256</td>
<td>Type 8</td>
</tr>
<tr>
<td>scrypt</td>
<td>Type 9</td>
</tr>
</tbody>
</table>

Note

Type 5, 8, and 9 passwords are not reversible.

If you configure type 8 or type 9 passwords and then downgrade to a release that does not support type 8 and type 9 passwords, you must configure the type 5 passwords before downgrading. If not, you are locked out of the device and a password recovery is required.
If you are using an external AAA server to manage privilege levels, you are not locked out of the device.

Note

Examples

The following example shows how to generate a type 8 (PBKDF2 with SHA-256) or a type 9 (SCRYPT) password:

Device# configure terminal
Device(config)# username demo8 algorithm-type sha256 secret cisco
Device(config)# username demo9 algorithm-type scrypt secret cisco
Device(config)# end
Device# show running-config | inc username

username demo8 secret 8 $8$dsYGNam3K1S1JO$7nv/35M/qr6t.dVc7UY9zrJDWRYqncHub1PE9U1MQFs
username demo9 secret 9 $9$nhEmQVczB7dqs0Sx.HsgL6x1il0Rxk0SSVvyqWyucySc7qFm4v7pqCxkKM

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Exits privileged EXEC mode and returns to user EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>enable password</td>
<td>Sets a local password to control access to various privilege levels.</td>
</tr>
<tr>
<td>enable secret</td>
<td>Specifies an additional layer of security over the enable password command.</td>
</tr>
<tr>
<td>username algorithm-type</td>
<td>Sets the algorithm type to hash a user password configured using the username secret command.</td>
</tr>
</tbody>
</table>
enable password

To set a local password to control access to various privilege levels, use the enable password command in global configuration mode. To remove the password requirement, use the no form of this command.

```
enable password [level level] {password[encryption-type] encrypted-password}
no enable password [level level]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>level</strong> <strong>level</strong></td>
<td>(Optional) Level for which the password applies. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified in the command or the no form of the command, the privilege level defaults to 15 (traditional enable privileges).</td>
</tr>
<tr>
<td><strong>password</strong></td>
<td>Password users type to enter enable mode.</td>
</tr>
<tr>
<td><strong>encryption-type</strong></td>
<td>(Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available is 5. If you specify encryption-type, the next argument you supply must be an encrypted password (a password already encrypted by a Cisco router).</td>
</tr>
<tr>
<td><strong>encrypted-password</strong></td>
<td>Encrypted password you enter, copied from another router configuration.</td>
</tr>
</tbody>
</table>

### Command Default

No password is defined. The default is level 15.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- **Caution**: If neither the enable password command nor the enable secret command is configured, and if there is a line password configured for the console, the console line password will serve as the enable password for all VTY (Telnet and Secure Shell [SSH]) sessions.

- Use this command with the **level** option to define a password for a specific privilege level. After you specify the level and the password, give the password to the users who need to access this level. Use the **privilege level** configuration command to specify commands accessible at various levels.

- You will not ordinarily enter an encryption type. Typically you enter an encryption type only if you copy and paste into this command a password that has already been encrypted by a Cisco router.
If you specify an encryption type and then enter a clear text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

If the service password-encryption command is set, the encrypted form of the password you create with the enable password command is displayed when a more nvram:startup-config command is entered.

You can enable or disable password encryption with the service password-encryption command.

An enable password is defined as follows:

- Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password abc?123, do the following:
  - Enter abc.
  - Type Ctrl-v.
  - Enter ?123.

When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter abc?123 at the password prompt.

**Examples**

The following example enables the password “pswd2” for privilege level 2:

```plaintext
enable password level 2 pswd2
```

The following example sets the encrypted password “$1$i5Rkls3LoyxzS8t9”, which has been copied from a router configuration file, for privilege level 2 using encryption type 7:

```plaintext
enable password level 2 5 $1$i5Rkls3LoyxzS8t9
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Exits privileged EXEC mode and returns to user EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>enable secret</td>
<td>Specifies an additional layer of security over the enable password command.</td>
</tr>
<tr>
<td>privilege</td>
<td>Configures a new privilege level for users and associate commands with that privilege level.</td>
</tr>
<tr>
<td>service password-encryption</td>
<td>Encrypts passwords.</td>
</tr>
<tr>
<td>show privilege</td>
<td>Displays your current level of privilege.</td>
</tr>
</tbody>
</table>
enable secret

To specify an additional layer of security over the enable password command, use the enable secret command in global configuration mode. To turn off the enable secret function, use the no form of this command.

```
enable secret [level level] [0] {unencrypted-password|encryption-type encrypted-password}
no enable secret [level level] [encryption-type encrypted-password]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>level level</strong></td>
<td>(Optional) Specifies the level for which the password applies. You can specify up to 15 privilege levels, using numerals 1 through 15. Level 1 is normal EXEC-mode user privileges. If the level argument is not specified in the command or in the no form of the command, the privilege level defaults to 15 (traditional enable privileges).</td>
</tr>
<tr>
<td><strong>0</strong></td>
<td>(Optional) Specifies an unencrypted clear-text password. The password is converted to a Secure Hash Algorithm (SHA) 256 secret and gets stored in the router.</td>
</tr>
<tr>
<td><strong>unencrypted-password</strong></td>
<td>Password for users to enter enable mode. This password should be different from the password created with the enable password command.</td>
</tr>
<tr>
<td><strong>encryption-type</strong></td>
<td>Cisco-proprietary algorithm used to hash the password. The algorithm types available for this command are 4 and 5.</td>
</tr>
<tr>
<td>• 4—Specifies an SHA-256 encrypted secret string. The SHA256 secret string is copied from the router configuration.</td>
<td></td>
</tr>
<tr>
<td>• 5—Specifies a message digest algorithm 5 (MD5) encrypted secret.</td>
<td></td>
</tr>
<tr>
<td>• 8—Specifies a Password-Based Key Derivation Function 2 (PBKDF2) with SHA-256 hashed secret.</td>
<td></td>
</tr>
<tr>
<td>• 9—Specifies a scrypt hashed secret.</td>
<td></td>
</tr>
<tr>
<td><strong>encrypted-password</strong></td>
<td>Hashed password that is copied from another router configuration.</td>
</tr>
</tbody>
</table>

**Command Default**

No password is defined.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>15.0(1)S</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)S. Support for the type 4 algorithm was added.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.1S</td>
<td>This command was integrated into Cisco IOS XE Release 3.1S. Support for the type 4 algorithm was added.</td>
</tr>
<tr>
<td>15.1(4)M</td>
<td>This command was modified. Support for the type 4 algorithm was added.</td>
</tr>
<tr>
<td>Cisco IOS Release 3.3SG</td>
<td>This command was modified. Support for the encryption type 5 was removed.</td>
</tr>
<tr>
<td>15.1(1)SY</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)SY.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.8S</td>
<td>This command was modified. The warning message for removal of support for the type 5 algorithm was modified.</td>
</tr>
<tr>
<td>15.3(3)M</td>
<td>This command was modified.</td>
</tr>
<tr>
<td></td>
<td>• The 4 keyword was deprecated and support for type 8 and type 9 algorithms were added.</td>
</tr>
<tr>
<td></td>
<td>• The warning message for the type 5 algorithm was removed.</td>
</tr>
<tr>
<td></td>
<td>• The warning message for removal of support for the type 4 algorithm was added.</td>
</tr>
<tr>
<td>15.3(3)S</td>
<td>The command modifications were integrated into Cisco IOS Release 15.3(3)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Caution**

If neither the `enable password` command or the `enable secret` command is configured, and if a line password is configured for the console, the console line password will serve as the enable password for all vty (Telnet and Secure Shell [SSH]) sessions.

Use the `enable secret` command to provide an additional layer of security over the `enable password`. The `enable secret` command provides better security by storing the enable secret password using a nonreversible cryptographic function. The added layer of security encryption provides is useful in environments where the password crosses the network or is stored on a TFTP server.

Typically you enter an encryption type only when you paste an encrypted password that you copied from a router configuration file into this command.

**Caution**

If you specify an encryption type and then enter a clear-text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

If you use the same password for the `enable password` and `enable secret` commands, you receive an error message warning that this practice is not recommended, but the password will be accepted. By using the same password, however, you undermine the additional security the `enable secret` command provides.
After you set a password using the `enable secret` command, a password set using the `enable password` command works only if the `enable secret` is disabled or an older version of Cisco IOS software is being used, such as when running an older rxboot image. Additionally, you cannot recover a lost password that has been encrypted by any method.

If the `service password-encryption` command is set, the encrypted form of the password you create is displayed when the `more nvram:startup-config` command is entered.

You can enable or disable password encryption with the `service password-encryption` command.

An enable password is defined as follows:

- Must contain 1 to 25 alphanumeric characters, both uppercase and lowercase.
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password `abc?123`, do the following:
  - Enter `abc`.
  - Press Ctrl-v.
  - Enter `?123`.

When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can enter `abc?123` at the password prompt.

During a downgrade from Cisco IOS XE Release 3.3SG to Cisco IOS XE Release 3.2SG, if a SHA256-encrypted enable password is configured, then the SHA256-encrypted password will be lost without any warning, and the secret password will have to be reconfigured.

With CSCue95644, you can use the `enable secret` command to hash the enable secret password with MD5, PBKDF2 with SHA-256, or scrypt hashing algorithms.

If you use type 8 or type 9 passwords and then downgrade to an older version of Cisco IOS software that does not support type 8 and type 9 passwords, you must reconfigure the passwords to use type 5 hashing before downgrading. If not, you are locked out of the device and password recovery is required. If you are using an external AAA server to manage privilege levels, you are not locked out of the device.

The following example shows how to specify the password with the `enable secret` command:

```
Device> enable
Device# configure terminal
Device(config)# enable secret password
```
After specifying a password with the `enable secret` command, users must enter this password to gain access. Any passwords set through `enable password` command will no longer work.

Password: `password`

The following example shows how to enable the encrypted password “$1$FaD0$Xyi5Rkl3LYyxzS8”, which has been copied from a router configuration file, for privilege level 2 using the encryption type 4:

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 4 $1$FaD0$Xyi5Rkl3LYyxzS8
```

The following example shows the sample warning message that is displayed when a user enters the `enable secret 4 encrypted-password` command:

```
Device# configure terminal
Device(config)# enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
WARNING: Command has been added to the configuration but Type 4 passwords have been deprecated.
Migrate to a supported password type
```

```
Device(config)# end
Device# show running-config | inc secret
```

```
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable algorithm-type</code></td>
<td>Sets the algorithm type to hash a user password configured using the <code>enable secret</code> command.</td>
</tr>
<tr>
<td><code>enable password</code></td>
<td>Sets a local password to control access to various privilege levels.</td>
</tr>
<tr>
<td><code>more nvram:startup-config</code></td>
<td>Displays the startup configuration file contained in NVRAM or specified by the <code>CONFIG_FILE</code> environment variable.</td>
</tr>
<tr>
<td><code>service password-encryption</code></td>
<td>Encrypt passwords.</td>
</tr>
</tbody>
</table>
enabled (IPS)

To change the enabled status of a given signature or signature category, use the `enabled` command in signature-definition-status (config-sigdef-status) or IPS-category-action (config-ips-category-action) configuration mode. To return to the default action, use the `no` form of this command.

`enabled [true|false]`
`no enabled`

**Syntax Description**

<table>
<thead>
<tr>
<th>true</th>
<th>Enables a specified signature or all signatures within a specified category.</th>
</tr>
</thead>
<tbody>
<tr>
<td>false</td>
<td>Disables a specified signature or all signatures within a specified category.</td>
</tr>
</tbody>
</table>

**Command Default**

All commands are enabled.

**Command Modes**

Signature-definition-status configuration (config-sigdef-status)
IPS-category-action configuration (config-ips-category-action)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `enabled` command to change the status of a signature or signature category to active (true) or inactive (false).

**Examples**

The following example shows how to change the status of signature 9000:0 to enabled:

```
Router(config)# ip ips signature-definition
Router(config-sig)# signature 9000 0
Router(config-sig-sig)# status
Router(config-sigdef-status)# enabled true
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>category</td>
<td>Specifies a signature category that is to be used for multiple signature actions or conditions.</td>
</tr>
<tr>
<td>signature</td>
<td>Specifies a signature for which the CLI user tunings will be changed.</td>
</tr>
<tr>
<td>status</td>
<td>Changes the enabled or retired status of a given signature or signature category.</td>
</tr>
</tbody>
</table>
To specify the encryption algorithm within an Internet Key Exchange (IKE) policy, use the `encryption` command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the encryption algorithm to the default value, use the `no` form of this command.

```
encryption {des|3des|aes|aes 192|aes 256}
no encryption
```

**Syntax Description**
- `des` 56-bit Data Encryption Standard (DES)-CBC as the encryption algorithm.
- `3des` 168-bit DES (3DES) as the encryption algorithm.
- `aes` 128-bit Advanced Encryption Standard (AES) as the encryption algorithm.
- `aes 192` 192-bit AES as the encryption algorithm.
- `aes 256` 256-bit AES as the encryption algorithm.

**Command History**
The 56-bit DES-CBC encryption algorithm

**Command Modes**
ISAKMP policy configuration

**Usage Guidelines**
Use this command to specify the encryption algorithm to be used in an IKE policy.

If a user enters an IKE encryption method that the hardware does not support, a warning message will be displayed immediately after the `encryption` command is entered.

**Examples**
The following example configures an IKE policy with the 3DES encryption algorithm (all other parameters are set to the defaults):

```
crypto isakmp policy
```
The following example is a sample warning message that is displayed when a user enters an IKE encryption method that the hardware does not support:

```
encryption aes 256
WARNING:encryption hardware does not support the configured encryption method for ISAKMP policy 1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>authentication (IKE policy)</strong></td>
<td>Specifies the authentication method within an IKE policy.</td>
</tr>
<tr>
<td><strong>crypto isakmp policy</strong></td>
<td>Defines an IKE policy.</td>
</tr>
<tr>
<td><strong>group (IKE policy)</strong></td>
<td>Specifies the DH group identifier within an IKE policy.</td>
</tr>
<tr>
<td><strong>hash (IKE policy)</strong></td>
<td>Specifies the hash algorithm within an IKE policy.</td>
</tr>
<tr>
<td><strong>lifetime (IKE policy)</strong></td>
<td>Specifies the lifetime of an IKE SA.</td>
</tr>
<tr>
<td><strong>show crypto isakmp policy</strong></td>
<td>Displays the parameters for each IKE policy.</td>
</tr>
</tbody>
</table>
encryption (IKEv2 proposal)

To specify one or more encryption algorithms for an Internet Key Exchange Version 2 (IKEv2) proposal, use the `encryption` command in IKEv2 proposal configuration mode. To remove the encryption algorithm, use the `no` form of this command.

`encryption encryption-type...`
`no encryption`

**Syntax Description**

`encryption-type...` Specifies the type of encryption algorithm.

**Command Default**
The encryption algorithm is not specified.

**Command Modes**
IKEv2 proposal configuration (config-ikev2-proposal)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
<tr>
<td>15.4(2)T</td>
<td>This command was modified. Support was added for Advanced Encryption Standard (AES) in Galois/Counter Mode (AES-GCM).</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.12S</td>
<td>This command was integrated into Cisco IOS XE Release 3.12S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to specify the encryption algorithm to be used in an IKEv2 proposal. The default encryption algorithm in the default proposal is 128-bit Advanced Encryption Standard-Cipher Block Chaining (AES-CBC) and 3 DES encryption algorithm. The encryption type can be one of the following:

<table>
<thead>
<tr>
<th>Encryption Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3des</td>
<td>Specifies 168-bit DES (3DES) as the encryption algorithm.</td>
</tr>
<tr>
<td>aes-cbc-128</td>
<td>Specifies 128-bit AES-CBC as the encryption algorithm.</td>
</tr>
<tr>
<td>aes-cbc-192</td>
<td>Specifies 192-bit AES-CBC as the encryption algorithm.</td>
</tr>
<tr>
<td>aes-cbc-256</td>
<td>Specifies 256-bit AES-CBC as the encryption algorithm.</td>
</tr>
<tr>
<td>aes-gcm-128</td>
<td>Specifies 128-bit Advanced Encryption Standard (AES) in Galois/Counter Mode (AES-GCM) as the encryption algorithm.</td>
</tr>
</tbody>
</table>
Encryption Type | Description
--- | ---
aes-gcm-256 | Specifies 256-bit AES-GCM as the encryption algorithm.

**Note**
You cannot selectively remove an encryption algorithm when multiple encryption algorithms are configured.

**Examples**
The following example configures an IKE proposal with the 3DES encryption algorithm:

Device(config)# crypto ikev2 proposal proposal1
Device(config-ikev2-proposal)# encryption 3des

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2 proposal</td>
<td>Defines an IKEv2 proposal.</td>
</tr>
<tr>
<td>group (ikev2 proposal)</td>
<td>Specifies the DH group identifier in an IKEv2 proposal.</td>
</tr>
<tr>
<td>integrity (ikev2 proposal)</td>
<td>Specifies the integrity algorithm in an IKEv2 proposal.</td>
</tr>
<tr>
<td>show crypto ikev2 proposal</td>
<td>Displays the parameters for each IKEv2 proposal.</td>
</tr>
</tbody>
</table>
enforce-checksum

To enforce checksum verification for Flexible Packet Matching (FPM), use the `enforce-checksum` command in `fpm package-info` mode. To disable the checksum verification, use the `no` form of this command.

```
enforce-checksum
no enforce-checksum
```

**Syntax Description**

This command has no keywords and arguments.

**Command Default**

enforce checksum is enabled.

**Command Modes**

fpm package-info (config-fpm-pak-info)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `enforce-checksum` command ensures that the FPM verifies the checksum of the package during load and that the package has not been tampered. This command is useful when you want to define your own filters inside the FPM packages by disabling enforce-checksum using `no enforce-checksum` command. However, it is recommended to keep the `enforce-checksum` enabled.

**Examples**

The following example shows how to enable the `enforce-checksum` command:

```
Router# configure terminal
Router(config)# fpm package-info
Router(config)# enforce-checksum
```
**engine (IPS)**

To enter signature-definition-action-engine configuration mode, which allows you to change router actions for a specified signature, use the `engine` command in signature-definition-action configuration mode.

### Syntax Description

This command has no arguments or keywords.

### Command Default

None

### Command Modes

Signature-definition-action configuration (config-sigdef-action)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If you wish to change router actions for a specific signature, you must issue the `engine` command to enter the appropriate configuration mode, which allows you to issue the `event-action` command and specify any supported action.

### Examples

The following example shows how to configure signature 5726 to reset all TCP connections and produce an alert:

```console
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature-definition
Router(config-sigdef)# signature 5726 0
Router(config-sigdef-sig)# engine
Router(config-sigdef-sig-engine)# event-action reset-tcp-connection produce-alert
Router(config-sigdef-sig-engine)# exit
Router(config-sigdef-sig)# exit
Router(config-sigdef)# ^Z
Do you want to accept these changes? [confirm]
Router#*
```

*Nov 9 21:50:55.847: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 12 of 11 engines
*Nov 9 21:50:55.859: %IPS-6-ENGINE_READY: multi-string - build time 12 ms - packets for this engine will be scanned
*Nov 9 21:50:55.859: %SYS-5-CONFIG_I: Configured from console by cisco on console

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>event-action</td>
<td>Changes router actions for a signature or signature category.</td>
</tr>
<tr>
<td>signature</td>
<td>Specifies a signature for which the CLI user tunings will be changed.</td>
</tr>
</tbody>
</table>
enrollment

To specify the enrollment parameters of your certification authority (CA), use the enrollment command in ca-trustpoint configuration mode. To remove any of the configured parameters, use the no form of this command.

```
enrollment { mode ra | retry count number | retry period minutes | url url }
no enrollment { mode ra | retry count number | retry period minutes | url url }
```

**Syntax Description**

<table>
<thead>
<tr>
<th>mode ra</th>
<th>Specifies registration authority (RA) mode as the mode supported by the CA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>retry count number</td>
<td>Specifies the number of times that a router will resend a certificate request when it does not receive a response from the previous request. The range is from 1 to 100. The default is 10.</td>
</tr>
<tr>
<td>retry period minutes</td>
<td>Specifies the wait period between certificate request retries. The range is from 1 to 60.</td>
</tr>
<tr>
<td>url url</td>
<td>Specifies the URL of the CA where your router should send certificate requests.</td>
</tr>
</tbody>
</table>

**Command Default**

RA mode is disabled.

After the router sends the first certificate request to the CA, it waits for 1 minute before sending a second request. After the second request, the interval between requests (the retry period) increases exponentially, with an additional 1 minute interval added at each increment.

The router sends a maximum of ten requests.

Your router does not know the CA URL until you specify it using url url.

**Command Modes**

CA-trustpoint configuration (ca-trustpoint)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>The url url option was enhanced to support TFTP enrollment.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXD.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the mode keyword to specify the mode supported by the CA. This keyword is required if your CA system provides an RA.

Use the retry period minutes option to change the retry period from the default value. After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a period of time (the retry period), the router will send another certificate request. The router will continue to send requests until it receives a valid certificate, until the CA returns an enrollment error, or until the configured number of retries is exceeded.
By default, the router sends a maximum of ten requests; you can change this parameter using the retry count number option. It stops sending requests when it receives a valid certificate, when the CA returns an enrollment error, or when the configured number of requests is reached.

Use the `url` option to specify or change the URL of the CA. You can specify enrollment with the Simple Certificate Enrollment Protocol (SCEP) using a HTTP URL or TFTP (using a TFTP URL).

If you are using (SCEP) for enrollment, `url` must be in the form `http://CA_name`, where `CA_name` is the CA’s host Domain Name System (DNS) name or IP address. If you are using TFTP for enrollment, `url` must be in the form `tftp://certserver/file_specification`.

TFTP enrollment is used to send the enrollment request and retrieve the certificate of the CA and the certificate of the router. If the `file_specification` is included in the URL, the router will append an extension onto the file specification. When the `crypto ca authenticate` command is entered, the router will retrieve the certificate of the CA from the specified TFTP server. As appropriate, the router will append the extension “.ca” to the filename or the fully qualified domain name (FQDN). If the `url` option does not include a file specification, the router’s FQDN will be used.

**Note**

The `crypto ca trustpoint` command replaces the `crypto ca identity` and `crypto ca trusted-root` commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as `ca-trustpoint`.

**Examples**

The following example shows how to declare a CA named ka and how to specify registration authority mode. It also shows how to set a retry count of 8 and a retry period of 2 minutes:

```
Router(config) # crypto ca trustpoint ka
Router(ca-trustpoint) # enrollment mode ra
Router(ca-trustpoint) # enrollment retry count 8
Router(ca-trustpoint) # enrollment retry period 2
```

The following example shows how to declare a CA named ka and how to specify the URL of the CA as `http://example:80`:

```
Router(config) # crypto ca trustpoint ka
Router(ca-trustpoint) # enrollment url http://example:80
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crypto ca authenticate</code></td>
<td>Authenticates the CA (by getting the CA’s certificate).</td>
</tr>
<tr>
<td><code>crypto ca trustpoint</code></td>
<td>Declares the CA that your router should use.</td>
</tr>
<tr>
<td><code>enrollment command</code></td>
<td>Specifies the HTTP command that is sent to the CA for enrollment.</td>
</tr>
<tr>
<td><code>enrollment credential</code></td>
<td>Specifies an existing trustpoint from another vendor that is to be enrolled with the Cisco IOS certificate server.</td>
</tr>
<tr>
<td><code>enrollment http-proxy</code></td>
<td>Enables access to the CA by HTTP through the proxy server.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>enrollment profile</td>
<td>Specifies that an enrollment profile can be used for certificate authentication and enrollment.</td>
</tr>
<tr>
<td>enrollment selfsigned</td>
<td>Specifies self-signed enrollment for a trustpoint.</td>
</tr>
<tr>
<td>enrollment terminal</td>
<td>Specifies manual cut-and-paste certificate enrollment.</td>
</tr>
<tr>
<td>enrollment url</td>
<td>Specifies the enrollment parameters of a CA.</td>
</tr>
</tbody>
</table>
enrollment command

To specify the HTTP command that is sent to the certification authority (CA) for enrollment, use the enrollment command command in ca-profile-enroll configuration mode.

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
No default behavior or values

**Command Modes**
Ca-profile-enroll configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13)ZH</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
After enabling this command, you can use the parameter command to specify enrollment parameters for your enrollment profile.

**Examples**
The following example shows how to configure the enrollment profile name “E” for certificate enrollment:

```plaintext
crypto ca trustpoint Entrust
   enrollment profile E
   serial
crypto ca profile enrollment E
   authentication url http://entrust:81
   authentication command GET /certs/cacert.der
   enrollment url http://entrust:81/cda-cgi/clientcgi.exe
   enrollment command POST reference_number=$P2&authcode=$P1
   &retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
   parameter 1 value aaaa-bbbb-cccc
   parameter 2 value 5001
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ca profile enrollment</td>
<td>Defines an enrollment profile.</td>
</tr>
<tr>
<td>parameter</td>
<td>Specifies parameters for an enrollment profile.</td>
</tr>
</tbody>
</table>
enrollment credential

To specify an existing trustpoint from another vendor that is to be enrolled with the Cisco IOS certificate server, use the enrollment credential command in ca-profile-enroll configuration mode.

**enrollment credential label**

**Syntax Description**

| label | Name of the certification authority (CA) trustpoint of another vendor. |

**Command Default**

No default behavior or values.

**Command Modes**

Ca-profile-enroll configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(11)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)SXE</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXE.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To configure a router that is already enrolled with a CA of another vendor that is to be enrolled with a Cisco IOS certificate server, you must configure a certificate enrollment profile (via the crypto pki profile enrollment command). Thereafter, you should issue the enrollment credential command, which specifies the trustpoint of another vendor that has to be enrolled with a Cisco IOS certificate server.

**Examples**

The following example shows how to configure a client router and a Cisco IOS certificate server to exchange enrollment requests via a certificate enrollment profile:

```plaintext
! Define the trustpoint "msca-root" that points to the non-Cisco IOS CA and enroll and authenticate the client with the non-Cisco IOS CA.
crypto pki trustpoint msca-root
  enrollment mode ra
  enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
  ip-address FastEthernet2/0
  revocation-check crl
!
! Configure trustpoint "cs" for Cisco IOS CA.
crypto pki trustpoint cs
  enrollment profile cs1
  revocation-check crl
!
! Define enrollment profile "cs1," which points to Cisco IOS CA and mention (via the enrollment credential command) that "msca-root" is being initially enrolled with the Cisco IOS CA.
crypto pki profile enrollment cs1
  enrollment url http://cs:80
  enrollment credential msca-root!
! Configure the certificate server, and issue and the grant auto trustpoint command to instruct the certificate server to accept enrollment request only from clients
```
who are already enrolled with trustpoint “msca-root.”
crypto pki server cs
database level minimum
database url nvram:
issuer-name CN=cs
grant auto trustpoint msca-root
! crypto pki trustpoint cs
revocation-check crl
rsakeypair cs
!
crypto pki trustpoint msca-root
enrollment mode ra
enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
revocation-check crl

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto pki profile enrollment</td>
<td>Defines an enrollment profile.</td>
</tr>
</tbody>
</table>
enrollment http-proxy

To access the certification authority (CA) by HTTP through the proxy server, use the `enrollment http-proxy` command in ca-trustpoint configuration mode.

```
enrollment http-proxy host-name port-num
```

**Syntax Description**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host-name</td>
<td>Defines the proxy server used to get the CA.</td>
</tr>
<tr>
<td>port-num</td>
<td>Specifies the port number used to access the CA.</td>
</tr>
</tbody>
</table>

**Command Default**

If this command is not enabled, the CA will not be accessed via HTTP.

**Command Modes**

Ca-trustpoint configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXD.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `enrollment http-proxy` command must be used in conjunction with the `enrollment` command, which specifies the enrollment parameters for the CA.

**Examples**

The following example shows how to access the CA named “ka” by HTTP through the bomborra proxy server:

```
crypto ca trustpoint ka
enrollment url http://kahului
enrollment http-proxy bomborra 8080
crl optional
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ca trustpoint</td>
<td>Declares the CA that your router should use.</td>
</tr>
<tr>
<td>enrollment</td>
<td>Specifies the enrollment parameters of your CA.</td>
</tr>
</tbody>
</table>
enrollment mode ra

The enrollment mode ra command is replaced by the enrollment command command. See the enrollment command command for more information.
To specify that an enrollment profile can be used for certificate authentication and enrollment, use the `enrollment profile` command in `ca-trustpoint configuration` mode. To delete an enrollment profile from your configuration, use the `no enrollment profile` form of this command.

```plaintext
enrollment profile label
no enrollment profile label
```

**Syntax Description**
- `label` Creates a name for the enrollment profile.

**Command Default**
Your router does not recognize any enrollment profiles until you declare one using this command.

**Command Modes**
Ca-trustpoint configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13)ZH</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Before you can enable this command, you must enter the `crypto ca trustpoint` command.

The `enrollment profile` command enables your router to accept an enrollment profile, which can be configured via the `crypto ca profile enrollment` command. The enrollment profile, which consists of two templates, can be used to specify different URLs or methods for certificate authentication and enrollment.

**Examples**
The following example shows how to declare the enrollment profile named “E”:

```plaintext
crypto ca trustpoint Entrust
  enrollment profile E
  serial
  crypto ca profile enrollment E
  authentication url http://entrust:81
  authentication command GET /certs/cacert.der
  enrollment url http://entrust:81/cda-cgi/clientcgi.exe
  enrollment command POST reference_number=$P2&authcode=$P1
  retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
  parameter 1 value aaaa-bbbb-cccc
  parameter 2 value 5001
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ca profile enrollment</td>
<td>Defines an enrollment profile.</td>
</tr>
<tr>
<td>crypto ca trustpoint</td>
<td>Declares the CA that your router should use.</td>
</tr>
</tbody>
</table>
enrollment retry count

The enrollment retry count command is replaced by the enrollment command. See the enrollment command for more information.
enrollment retry period

The enrollment retry period command is replaced by the enrollment command. See the enrollment command for more information.
enrollment selfsigned

To specify self-signed enrollment for a trustpoint, use the enrollment selfsigned command in ca-trustpoint configuration mode. To delete self-signed enrollment from a trustpoint, use the no form of this command.

```
enrollment selfsigned
no enrollment selfsigned
```

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

ca-trustpoint configuration (ca-trustpoint)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Before you can use the enrollment selfsigned command, you must enable the crypto pki trustpoint command, which defines the trustpoint and enters ca-trustpoint configuration mode.

If you do not use this command, you should specify another enrollment method for the router by using an enrollment command such as enrollment url or enrollment terminal.

Examples

The following example shows a self-signed certificate being designated for a trustpoint named local:

```
crypto pki trustpoint local
enrollment selfsigned
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto pki trustpoint</td>
<td>Declares the CA that your router should use.</td>
</tr>
</tbody>
</table>
enrollment terminal (ca-profile-enroll)

To specify manual cut-and-paste certificate enrollment, use the enrollment terminal command in ca-profile-enroll configuration mode. To delete a current enrollment request, use the no form of this command.

```
enrollment terminal
no enrollment terminal
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

A certificate enrollment request is not specified.

**Command Modes**

Ca-profile-enroll configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13)ZH</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A user may manually cut-and-paste certificate authentication requests and certificates when a network connection between the router and certification authority (CA) is unavailable. After this command is enabled, the certificate request is printed on the console terminal so that it can be manually copied (cut) by the user.

**Note**

Although most routers accept manual enrollment, the process can be tedious if a large number of routers have to be enrolled.

**Examples**

The following example shows how to configure the enrollment profile named “E” to perform certificate authentication via HTTP and manual certificate enrollment:

```
crypto ca profile enrollment E
  authentication url http://entrust:81
  authentication command GET /certs/cacert.der
  enrollment terminal
  parameter 1 value aaaa-bbbb-cccc
  parameter 2 value 5001
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ca profile enrollment</td>
<td>Defines an enrollment profile.</td>
</tr>
</tbody>
</table>
enrollment terminal (ca-trustpoint)

To specify manual cut-and-paste certificate enrollment, use the `enrollment terminal` command in ca-trustpoint configuration mode. To delete a current enrollment request, use the `no` form of this command.

```
enrollment terminal [pem]
no enrollment terminal [pem]
```

**Syntax Description**

| pem | (Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request. |

**Command Default**

No default behavior or values

**Command Modes**

Ca-trustpoint configuration (ca-trustpoint)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>The <code>pem</code> keyword was added.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXD.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.4(24)T</td>
<td>Support for IPv6 Secure Neighbor Discovery (SeND) was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A user may want to manually cut-and-paste certificate requests and certificates when he or she does not have a network connection between the router and certification authority (CA). When this command is enabled, the router displays the certificate request on the console terminal, allowing the user to enter the issued certificate on the terminal.

**The pem Keyword**

Use the `pem` keyword to issue certificate requests (via the `crypto ca enroll` command) or receive issued certificates (via the `crypto ca import certificate` command) in PEM-formatted files through the console terminal. If the CA server does not support simple certificate enrollment protocol (SCEP), the certificate request can be presented to the CA server manually.

**Note**

When generating certificate requests in PEM format, your router does not have to have the CA certificate, which is obtained via the `crypto ca authenticate` command.

**Examples**

The following example shows how to manually specify certificate enrollment via cut-and-paste. In this example, the CA trustpoint is “MS.”

```
crypto ca trustpoint MS
enrollment terminal
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ca authenticate</td>
<td>Authenticates the CA (by getting the certificate of the CA).</td>
</tr>
<tr>
<td>crypto ca enroll</td>
<td>Obtains the certificates of your router from the certification authority.</td>
</tr>
<tr>
<td>crypto ca import</td>
<td>Imports a certificate manually via TFTP or cut-and-paste at the terminal.</td>
</tr>
<tr>
<td>crypto ca trustpoint</td>
<td>Declares the CA that your router should use.</td>
</tr>
</tbody>
</table>
enrollment url (ca-identity)

The enrollment url (ca-identity) command is replaced by the enrollment url (ca-trustpoint) command. See the enrollment url (ca-trustpoint) command for more information.
enrollment url (ca-profile-enroll)

To specify the URL of the certification authority (CA) server to which to send enrollment requests, use the enrollment url command in ca-profile-enroll configuration mode. To delete the enrollment URL from your enrollment profile, use the no form of this command.

enrollment url url[\{vrf vrf-name\}]
no enrollment url url[\{vrf vrf-name\}]

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td>URL of the CA server to which your router should send certificate requests.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>The VRF name.</td>
</tr>
</tbody>
</table>

Command Default

Your router does not recognize the CA URL until you specify it using this command.

Command Modes

Ca-profile-enroll configuration (ca-profile-enroll)#

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13)ZH</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td>15.1(4)T</td>
<td>This command was modified. The vrf vrf-name keyword-argument pair was added.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command allows the user to specify a different URL or a different method for authenticating a certificate and enrolling a certificate; for example, manual authentication and TFTP enrollment.

Note the following when specifying the url argument:

- If you are using Simple Certificate Enrollment Protocol (SCEP) for enrollment, the value must be in the form http://CA_name, where CA_name is the host Domain Name System (DNS) name or IP address of the CA.
- If you are using TFTP for enrollment, the value must be in the form tftp://certserver/file_specification. (If the URL does not include a file specification, the fully qualified domain name [FQDN] of the router will be used.)

Examples

The following example shows how to enable certificate enrollment via HTTP for the profile name “E”:

crypto pki trustpoint Entrust
   enrollment profile E
   serial

    crypto pki profile enrollment E
    authentication url http://entrust:81
    authentication command GET /certs/cacert.der
    enrollment url http://entrust:81/cda-cgi/clientcgi.exe
    enrollment command POST reference_number=$P2&authcode=$P1&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
    parameter 1 value aaaa-bbbb-cccc
    parameter 2 value 5001
The following example shows how to configure the enrollment and certificate revocation list (CRL) via the same VRF:

crypto pki trustpoint trustpoint1
    enrollment url http://10.10.10.10:80
    vrf vrf1
    revocation-check crl

The following example shows how to configure the enrollment and certificate revocation list (CRL) via different VRF:

crypto pki profile enrollment pki_profile
    enrollment url http://10.10.10.10:80 vrf vrf2

crypto pki trustpoint trustpoint1
    enrollment profile pki_profile
    vrf vrf1
    revocation-check crl

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto pki profile enrollment</td>
<td>Defines an enrollment profile.</td>
</tr>
</tbody>
</table>
enrollment url (ca-trustpoint)

To specify the enrollment parameters of a certification authority (CA), use the enrollment url command in ca-trustpoint configuration mode. To remove any of the configured parameters, use the no form of this command.

```
enrollment [mode] [retry period minutes] [retry count number] url url [pem]  
no enrollment [mode] [retry period minutes] [retry count number] url url [pem]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mode</td>
<td>(Optional) Specifies the registration authority (RA) mode, if your CA system provides an RA. By default, RA mode is disabled.</td>
</tr>
<tr>
<td>retry period</td>
<td>minutes (Optional) Specifies the period, in minutes, in which the router waits before sending the CA another certificate request. Valid values are from 1 to 60. The default is 1.</td>
</tr>
<tr>
<td>retry count</td>
<td>number (Optional) Specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. Valid values are from 1 to 100. The default is 10.</td>
</tr>
<tr>
<td>url</td>
<td>url (Optional) Specifies the URL of the file system where your router should send certificate requests. For enrollment method options, see the table below.</td>
</tr>
<tr>
<td>pem</td>
<td>(Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request.</td>
</tr>
</tbody>
</table>

**Command Default**

Your router does not know the CA URL until you specify it using the `url url` keyword and argument.

**Command Modes**

Ca-trustpoint configuration (config-ca-trustpoint)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3T</td>
<td>This command was introduced as the <code>enrollment url</code> (ca-identity) command.</td>
</tr>
<tr>
<td>12.2(8)T</td>
<td>This command was introduced. This command replaced the <code>enrollment url</code> (ca-identity) command.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was modified. The <code>url url</code> option was enhanced to support TFTP enrollment.</td>
</tr>
<tr>
<td>12.3(4)T</td>
<td>This command was modified. The <code>pem</code> keyword was added, and the <code>url url</code> option was enhanced to support an additional enrollment method—the Cisco IOS File System (IFS).</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>12.4(24)T</td>
<td>This command was modified. Support for IPv6 Secure Neighbor Discovery (SeND) was added.</td>
</tr>
</tbody>
</table>
This command was modified. Support for specifying the IPv6 address in a URL for the CA was added.

**Usage Guidelines**

Use the `mode` keyword to specify the mode supported by the CA. This keyword is required if your CA system provides an RA.

Use the `retry period` minutes option to change the retry period from the default of 1 minute between retries. After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a specified period of time (the retry period), the router will send another certificate request. By default, the router will send a maximum of ten requests until it receives a valid certificate, until the CA returns an enrollment error, or until the configured number of retries (specified through the `retry count number` option) is exceeded.

Use the `pem` keyword to issue certificate requests (using the `crypto pki enroll` command) or receive issued certificates (using the `crypto pki import certificate` command) in PEM-formatted files.

---

**Note**

When generating certificate requests in PEM format, your router does not have to have the CA certificate, which is obtained using the `crypto ca authenticate` command.

The `url` argument specifies or changes the URL of the CA. The table below lists the available enrollment methods.

**Table 4: Certificate Enrollment Methods**

<table>
<thead>
<tr>
<th>Enrollment Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>WORD</code></td>
<td>Enrolls through the Simple Certificate Enrollment Protocol (SCEP) (an HTTP URL). <strong>Note</strong> If you are using SCEP for enrollment, the URL must be in the form <code>http://CA_name</code>, where <code>CA_name</code> is the host Domain Name System (DNS) name, IPv4 address, or IPv6 address of the CA.</td>
</tr>
<tr>
<td><code>archive:</code></td>
<td>Enrolls through the archive: file system.</td>
</tr>
<tr>
<td><code>disk0:</code></td>
<td>Enrolls through the disc0 file system.</td>
</tr>
<tr>
<td><code>disk1:</code></td>
<td>Enrolls through the disc1 file system.</td>
</tr>
<tr>
<td><code>ftp:</code></td>
<td>Enrolls through the FTP file system.</td>
</tr>
</tbody>
</table>
| `http:`           | Enrolls through the HTTP file system. The URL must be in the following formats:  

  - `http://CA_name:80`, where `CA_name` is the Domain Name System (DNS)  
  - `http://[ipv6-address]:80`. For example: `http://[2001:DB8:1:1::1]:80`. The IPv6 address is in hexadecimal notation and must be enclosed in brackets in the URL. |
<table>
<thead>
<tr>
<th>Enrollment Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>https:</strong></td>
<td>Enrolls through the HTTPS file system. The URL must use the same formats as the HTTP: file system formats described above.</td>
</tr>
<tr>
<td><strong>null:</strong></td>
<td>Enrolls through the null file system</td>
</tr>
<tr>
<td><strong>nvram:</strong></td>
<td>Enrolls through Non-volatile Random-access Memory (NVRAM) file system</td>
</tr>
<tr>
<td><strong>pram:</strong></td>
<td>Enrolls through Parameter Random-access Memory (PRAM) file system</td>
</tr>
<tr>
<td><strong>rcp:</strong></td>
<td>Enrolls through the remote copy protocol (rcp) file system</td>
</tr>
<tr>
<td><strong>scp:</strong></td>
<td>Enrolls through the secure copy protocol (scp) file system</td>
</tr>
<tr>
<td><strong>snmp:</strong></td>
<td>Enrolls through the Simple Network Management Protocol (SNMP)</td>
</tr>
<tr>
<td><strong>system:</strong></td>
<td>Enrolls through the system file system</td>
</tr>
</tbody>
</table>
| **tftp:**        | Enrolls through the Trivial File Transfer Protocol (TFTP): file system.  
                  | **Note** The URL must be in the form: tftp://CA_name/file_specification |
| **tmpsys:**      | Enrolls through the IOS tmpsys file system. |
| **unix:**        | Enrolls through the UNIX file system. |

TFTP enrollment is used to send the enrollment request and retrieve the certificate of the CA and the certificate of the router. If the file_specification is included in the URL, the router appends an extension onto the file specification. When the `crypto pki authenticate` command is entered, the router retrieves the certificate of the CA from the specified TFTP server. As appropriate, the router appends the extension ".ca" to the filename or the fully qualified domain name (FQDN). (If the `url` option does not include a file specification, the FQDN of the router is used.)

The `crypto pki trustpoint` command replaces the `crypto ca identity` and `crypto ca trusted-root` commands and all related commands (all `ca-identity` and `trusted-root` configuration mode commands). If you enter a `ca-identity` or `trusted-root` command, the configuration mode and command is written back as pki-trustpoint.

An IPv6 address can be added to the URL for the CA in the Trustpoint configuration. It is important that this address be in brackets.

**Examples**

The following example shows how to declare a CA named "trustpoint" and specify the URL of the CA as http://example:80:

```
crypto pki trustpoint trustpoint
enrollment url http://example:80
```

The following example shows how to declare a CA named "trustpoint" and specify the IPv6 URL of the CA as http://[2001:DB8:1::1]:80:

```
crypto pki trustpoint trustpoint
enrollment url http://[2001:DB8:1::1]:80
```
crypto pki trustpoint trustpoint
enrollment url http://[2001:DB8:1:1::1]:80

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>crl query</td>
<td>Queries the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.</td>
</tr>
<tr>
<td></td>
<td>crypto pki authenticate</td>
<td>Authenticates the CA (by getting the certificate of the CA).</td>
</tr>
<tr>
<td></td>
<td>crypto pki enroll</td>
<td>Obtains the certificate or certificates of your router from the CA.</td>
</tr>
<tr>
<td></td>
<td>crypto pki trustpoint</td>
<td>Declares the CA that your router should use.</td>
</tr>
<tr>
<td></td>
<td>ocs p url</td>
<td>Specifies the URL of an online certificate status protocol (OCSP) server to override the OCSP server URL (if one exists) in the Authority Info Access (AIA) extension of the certificate.</td>
</tr>
</tbody>
</table>
eou allow

To allow additional Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) options, use the `eou allow` command in global configuration mode. To disable the options that have been set, use the `no` form of this command.

```
eou allow {clientless|ip-station-id}
no eou allow {clientless|ip-station-id}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clientless</code></td>
<td>Allows authentication of clientless hosts (systems that do not run Cisco Trust Agent).</td>
</tr>
<tr>
<td><code>ip-station-id</code></td>
<td>Allows an IP address in the station-id field.</td>
</tr>
</tbody>
</table>

### Command Default

No additional EAPoUDP options are allowed.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `eou allow` command used with the `clientless` keyword requires that a user group be configured on the Cisco Access Control Server (ACS) using the same username and password that are specified using the `eou clientless` command.

### Examples

The following example shows that clientless hosts are allowed:

```
Router (config)# eou allow clientless
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>eou clientless</code></td>
<td>Sets user group credentials for clientless hosts.</td>
</tr>
</tbody>
</table>
eou clientless

To set user group credentials for clientless hosts, use the **eou clientless** command in global configuration mode. To remove the user group credentials, use the **no** form of this command.

```plaintext
eou clientless {password password|username username}
no eou clientless {password|username}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password password</td>
<td>Sets a password.</td>
</tr>
<tr>
<td>username username</td>
<td>Sets a username.</td>
</tr>
</tbody>
</table>

**Command Default**

Username and password values are clientless.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For this command to be effective, the **eou allow** command must also be enabled.

**Examples**

The following example shows that a clientless host with the username "user1" has been configured:

```
Router (config)# eou clientless username user1
```

The following example shows that a clientless host with the password "user123" has been configured:

```
Router (config)# eou clientless password user123
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eou allow</td>
<td>Allows additional EAPoUDP options.</td>
</tr>
</tbody>
</table>
**eou default**

To set global Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) parameters to the default values, use the `eou default` command in global or interface configuration mode.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The EAPoUDP parameters are set to their default values.

**Command Modes**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

Using this command, you can reset existing values to their default values.

**Examples**

The following configuration example shows that EAPoUDP parameters have been set to their default values:

```
Router (config)# eou default
```
**eou initialize**

To manually initialize Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) state machines, use the `eou initialize` command in global configuration mode. This command has no `no` form.

```
eou initialize {all|authentication {clientless|eap|static}|interface interface-name|ip ip-address|mac mac-address|posturetoken string}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Initiates reauthentication of all EAPoUDP clients. This keyword is the default.</td>
</tr>
<tr>
<td>authentication</td>
<td>Specifies the authentication type.</td>
</tr>
<tr>
<td>clientless</td>
<td>Clientless authentication type.</td>
</tr>
<tr>
<td>eap</td>
<td>EAP authentication type.</td>
</tr>
<tr>
<td>static</td>
<td>Static authentication type.</td>
</tr>
<tr>
<td>interface interface-name</td>
<td>Specifies a specific interface.</td>
</tr>
<tr>
<td>ip ip-address</td>
<td>Specifies a specific IP address.</td>
</tr>
<tr>
<td>mac mac-address</td>
<td>Specifies a specific MAC address.</td>
</tr>
<tr>
<td>posturetoken string</td>
<td>Specifies a specific posture token.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If this command is used, existing EAPoUDP state machines will be reset.

**Examples**

The following example shows that all EAPoUDP state machines have been reauthenticated:

```
Router (config)# eou initialize all
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>eou revalidate</strong></td>
<td>Revalidates an EAPoUDP association.</td>
</tr>
</tbody>
</table>
eou logging

To enable Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) system logging events, use the `eou logging` command in global configuration mode. To remove EAPoUDP logging, use the `no` form of this command.

```
eou logging
no eou logging
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Logging is disabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows that EAPoUDP logging has been enabled:

```
Router (config)# eou logging
```

The following is sample EAPoUDP logging output:

```
Apr 9 10:04:09.824: %EOU-6-SESSION: IP=10.0.0.1| HOST=DETECTED| Interface=FastEthernet0/0
*Apr 9 10:04:09.900: %EOU-6-CTA: IP=10.0.0.1| CiscoTrustAgent=DETECTED
*Apr 9 10:06:19.576: %EOU-6-POLICY: IP=10.0.0.1| TOKEN=Healthy
*Apr 9 10:06:19.576: %EOU-6-POLICY: IP=10.0.0.1| ACLNAME=#ACSACL#-IP-HealthyACL-40921e54
*Apr 9 10:06:19.576: %EOU-6-POSTURE: IP=10.0.0.1| HOST=AUTHORIZED| Interface=FastEthernet0/0.420
*Apr 9 10:06:19.580: %EOU-6-AUTHTYPE: IP=10.0.0.1| AuthType=EAP
```

**eou max-retry**

To set the number of maximum retry attempts for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), use the `eou max-retry` command in global or interface configuration mode. To remove the number of retries that were entered, use the `no` form of this command.

```
eou max-retry number-of-retries
no eou max-retry number-of-retries
```

| Syntax Description | number-of-retries | Number of maximum retries that may be attempted. The value ranges from 1 through 10. The default is 3. |

**Command Default**
The default number of retries is 3.

**Command Modes**
- Global configuration (config)
- Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4</td>
<td>The value range was changed from 1 through 3 to 1 through 10.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

**Examples**
The following example shows that the maximum number of retries for an EAPoUDP session has been set for 2:

```
Router (config)# eou max-retry 2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show eou</td>
<td>Displays information about EAPoUDP global values or EAPoUDP session cache entries.</td>
</tr>
</tbody>
</table>
eou port

To set the UDP port for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), use the `eou port` command in global configuration mode. This command has no no form.

```
eou port port-number
```

**Syntax Description**

| port-number | Number of the port. The value ranges from 1 through 65535. The default value is 27186. |

**Command Default**

The default `port-number` value is 27186.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Ensure that the port you set does not conflict with other UDP applications.

**Examples**

The following example shows that the port for an EAPoUDP session has been set to 200:

```
Router (config)# eou port 200
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show eou</code></td>
<td>Displays information about EAPoUDP.</td>
</tr>
</tbody>
</table>
eou rate-limit

To set the number of simultaneous posture validations for Extensible Authentication Protocol over UDP (EAPoUDP), use the `eou rate-limit` command in global configuration mode. This command has no no form.

`eou rate-limit number-of-validations`

**Syntax Description**

| `number-of-validations` | Number of clients that can be simultaneously validated. The value ranges from 1 through 200. The default value is 20. |

**Command Default**

No default behaviors or values

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you set the rate limit to 0 (zero), rate limiting will be turned off.

If the rate limit is set to 100 and there are 101 clients, validation will not occur until one drops off.

To return to the default value, use the `eou default` command.

**Examples**

The following example shows that the number of posture validations has been set to 100:

```
Router (config)# eou rate-limit 100
```
**eou revalidate**

To revalidate an Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) association, use the `eou revalidate` command in privileged EXEC mode. To disable the revalidation, use the `no` form of this command.

```
eou revalidate {all|authentication {clientless|eap|static}|interface interface-name|ip ip-address|mac mac-address|posturetoken string}
no eou revalidate {all|authentication {clientless|eap|static}|interface interface-name|ip ip-address|mac mac-address|posturetoken string}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enables revalidation of all EAPoUDP clients. This keyword option is the default.</td>
</tr>
<tr>
<td>authentication</td>
<td>Specifies the authentication type.</td>
</tr>
<tr>
<td>clientless</td>
<td>Clientless authentication type.</td>
</tr>
<tr>
<td>eap</td>
<td>EAP authentication type.</td>
</tr>
<tr>
<td>static</td>
<td>Static authentication type.</td>
</tr>
<tr>
<td>interface interface-name</td>
<td>Name of the interface. (See the table below for the types of interface that may be shown.)</td>
</tr>
<tr>
<td>ip ip-address</td>
<td>IP address of the client.</td>
</tr>
<tr>
<td>mac mac-address</td>
<td>The 48-bit hardware address of the client.</td>
</tr>
<tr>
<td>posturetoken string</td>
<td>Name of the posture token.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you use this command, existing EAPoUDP sessions will be revalidated.

The table below lists the interface types that may be used with the `interface` keyword.

**Table 5: Description of Interface Types**

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Async</td>
<td>Asynchronous interface</td>
</tr>
</tbody>
</table>
## Interface Type

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BVI</td>
<td>Bridge-Group Virtual Interface</td>
</tr>
<tr>
<td>CDMA-Ix</td>
<td>Code division multiple access Internet exchange (CDMA Ix) interface</td>
</tr>
<tr>
<td>CTunnel</td>
<td>Connectionless Network Protocol (CLNS) tunnel (Ctunnel) interface</td>
</tr>
<tr>
<td>Dialer</td>
<td>Dialer interface</td>
</tr>
<tr>
<td>Ethernet</td>
<td>IEEE 802.3 standard interface</td>
</tr>
<tr>
<td>Lex</td>
<td>Lex interface</td>
</tr>
<tr>
<td>Loopback</td>
<td>Loopback interface</td>
</tr>
<tr>
<td>MFR</td>
<td>Multilink Frame Relay bundle interface</td>
</tr>
<tr>
<td>Multilink</td>
<td>Multilink-group interface</td>
</tr>
<tr>
<td>Null</td>
<td>Null interface</td>
</tr>
<tr>
<td>Serial</td>
<td>Serial interface</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Tunnel interface</td>
</tr>
<tr>
<td>Vif</td>
<td>Pragmatic General Multicast (PGM) Multicase Host interface</td>
</tr>
<tr>
<td>Virtual-PPP</td>
<td>Virtual PPP interface</td>
</tr>
<tr>
<td>Virtual-Template</td>
<td>Virtual template interface</td>
</tr>
<tr>
<td>Virtual-TokenRing</td>
<td>Virtual TokenRing interface</td>
</tr>
</tbody>
</table>

### Examples

The following example shows that all EAPoUDP clients are to be revalidated:

Router# **eou revalidate all**

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eou initialize</td>
<td>Manually initializes EAPoUDP state machines.</td>
</tr>
</tbody>
</table>
eou timeout

To set the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) timeout values, use the eou timeout command in global or interface configuration mode. To remove the value that was set, use the no form of this command.

eou timeout {aaa seconds|hold-period seconds|retransmit seconds|revalidation seconds|status query seconds}
no timeout {aaa seconds|hold-period seconds|retransmit seconds|revalidation seconds|status query seconds}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa seconds</td>
<td>Authentication, authorization, and accounting (AAA) timeout period, in seconds. The value range is from 1 through 60. Default=60.</td>
</tr>
<tr>
<td>hold-period seconds</td>
<td>Hold period following failed authentication, in seconds. The value range is from 60 through 86400. Default=180.</td>
</tr>
<tr>
<td>retransmit seconds</td>
<td>Retransmit period, in seconds. The value range is from 1 through 60. Default=3.</td>
</tr>
<tr>
<td>revalidation seconds</td>
<td>Revalidation period, in seconds. The value range is from 300 through 86400. Default=36000.</td>
</tr>
<tr>
<td>status query seconds</td>
<td>Status query period after revalidation, in seconds. The value range is from 30 through 1800. Default=300.</td>
</tr>
</tbody>
</table>

Command Default

No default behavior or values

Command Modes

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

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

Examples

The following example shows that the status query period after revalidation is set to 30:

Router (config)# eou timeout status query 30

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show eou</td>
<td>Displays information about EAPoUDP global values.</td>
</tr>
</tbody>
</table>
error-msg

To display a specific error message when a user logs on to a Secure Sockets Layer Virtual Private Network (SSL VPN) gateway, use the `error-msg` command in `webvpn acl` configuration mode. To remove the error message, use the `no` form of this command.

```
error-msg  message-string
no error-msg  message-string
```

### Syntax Description

| `message-string` | Error message to be displayed. |

### Command Default

No special error message is displayed.

### Command Modes

Webvpn acl configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If the `error-url` command is configured, the user is redirected to the error URL for every request that is not allowed. If the `error-url` command is not configured, the user gets a standard, gateway-generated information page showing the message that was configured using the `error-msg` command.

### Examples

This example shows that the following error message will be displayed when the user logs on to the SSL VPN gateway:

```
webvpn context context1
acl acl1
error-msg "If you have any questions, please contact <a href=mailto:employee1@example.com>Employee1</a>.
"
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl</td>
<td>Defines an ACL using a SSL VPN gateway at the Application Layer level and enters <code>webvpn acl</code> configuration mode.</td>
</tr>
<tr>
<td>error-url</td>
<td>Defines a URL as an ACL violation page using a SSL VPN gateway.</td>
</tr>
<tr>
<td>webvpn context</td>
<td>Configures a SSL VPN context and enters <code>webvpn context</code> configuration mode.</td>
</tr>
</tbody>
</table>
**error-url**

To define a URL as an access control list (ACL) violation page using a Secure Socket Layer Virtual Private Network (SSL VPN) gateway, use the `error-url` command in `webvpn acl` configuration mode. To remove the ACL violation page, use the `no` form of this command.

```
error-url access-deny-page-url
no error-url access-deny-page-url
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-deny-page-url</td>
<td>URL to which a user is directed for an ACL violation.</td>
</tr>
</tbody>
</table>

**Command Default**

If this command is not configured, the gateway redirects the ACL violation page to a predefined URL.

**Command Modes**

Webvpn acl configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the `error-url` command is configured, the user is redirected to a predefined URL for every request that is not allowed. If the `error-url` command is not configured, the user gets a standard, gateway-generated error page.

**Examples**

The following example shows that the URL “http://www.example.com” has been defined as the ACL violation page:

```
webvpn context context1
acl acl
   error-url "http://www.example.com"
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl</td>
<td>Defines an ACL using a SSL VPN gateway at the Application Layer level.</td>
</tr>
<tr>
<td>error-msg</td>
<td>Displays a specific error message when a user logs on to a SSL VPN gateway.</td>
</tr>
<tr>
<td>webvpn context</td>
<td>Configures the SSL VPN context and enters webvpn context configuration mode.</td>
</tr>
</tbody>
</table>
evaluate

To nest a reflexive access list within an access list, use the `evaluate` command in access-list configuration mode. To remove a nested reflexive access list from the access list, use the `no` form of this command.

`evaluate name`
`no evaluate name`

**Syntax Description**

| `name` | The name of the reflexive access list that you want evaluated for IP traffic entering your internal network. This is the name defined in the `permit` (reflexive) command. |

**Command Default**

Reflexive access lists are not evaluated.

**Command Modes**

Access-list configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.33(SRA).</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is used to achieve reflexive filtering, a form of session filtering.

Before this command will work, you must define the reflexive access list using the `permit` (reflexive) command.

This command nests a reflexive access list within an extended named IP access list.

If you are configuring reflexive access lists for an external interface, the extended named IP access list should be one which is applied to inbound traffic. If you are configuring reflexive access lists for an internal interface, the extended named IP access list should be one which is applied to outbound traffic. (In other words, use the access list opposite of the one used to define the reflexive access list.)

This command allows IP traffic entering your internal network to be evaluated against the reflexive access list. Use this command as an entry (condition statement) in the IP access list; the entry “points” to the reflexive access list to be evaluated.

As with all access list entries, the order of entries is important. Normally, when a packet is evaluated against entries in an access list, the entries are evaluated in sequential order, and when a match occurs, no more entries are evaluated. With a reflexive access list nested in an extended access list, the extended access list entries are evaluated sequentially up to the nested entry, then the reflexive access list entries are evaluated sequentially, and then the remaining entries in the extended access list are evaluated sequentially. As usual, after a packet matches any of these entries, no more entries will be evaluated.

**Examples**

The following example shows reflexive filtering at an external interface. This example defines an extended named IP access list `inboundfilters`, and applies it to inbound traffic at the interface. The access list definition permits all Border Gateway Protocol and Enhanced Interior Gateway Routing Protocol traffic.
Protocol traffic, denies all Internet Control Message Protocol traffic, and causes all Transmission Control Protocol traffic to be evaluated against the reflexive access list tcptraffic.

If the reflexive access list tcptraffic has an entry that matches an inbound packet, the packet will be permitted into the network. tcptraffic only has entries that permit inbound traffic for existing TCP sessions.

```
interface Serial 1
    description Access to the Internet via this interface
    ip access-group inboundfilters in
    ip access-list extended inboundfilters
        permit 190 any any
        permit eigrp any any
        deny icmp any any
        evaluate tcptraffic
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list</td>
<td>Defines an IP access list by name.</td>
</tr>
<tr>
<td>ip reflexive-list timeout</td>
<td>Specifies the length of time that reflexive access list entries will continue to exist when no packets in the session are detected.</td>
</tr>
<tr>
<td>permit (reflexive)</td>
<td>Creates a reflexive access list and enables its temporary entries to be automatically generated.</td>
</tr>
</tbody>
</table>
**evaluate (IPv6)**

To nest an IPv6 reflexive access list within an IPv6 access list, use the `evaluate (IPv6)` command in IPv6 access list configuration mode. To remove the nested IPv6 reflexive access list from the IPv6 access list, use the `no` form of this command.

```
evaluate access-list-name [sequence value]
no evaluate access-list-name [sequence value]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list-name</code></td>
<td>The name of the IPv6 reflexive access list that you want evaluated for IPv6 traffic entering your internal network. This is the name defined in the <code>permit (IPv6)</code> command. Names cannot contain a space or quotation mark, or begin with a numeric.</td>
</tr>
<tr>
<td><code>sequence value</code></td>
<td>(Optional) Specifies the sequence number for the IPv6 reflexive access list. The acceptable range is from 1 to 4294967295.</td>
</tr>
</tbody>
</table>

**Command Default**
IPv6 reflexive access lists are not evaluated.

**Command Modes**
IPv6 access list configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(23)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `evaluate (IPv6)` command is similar to the `evaluate (IPv4)` command, except that it is IPv6-specific.

This command is used to achieve IPv6 reflexive filtering, a form of session filtering.

Before this command will work, you must define the IPv6 reflexive access list using the `permit (IPv6)` command.

This command nests an IPv6 reflexive access list within an IPv6 access control list (ACL).

If you are configuring an IPv6 reflexive access list for an external interface, the IPv6 ACL should be one that is applied to inbound traffic. If you are configuring IPv6 reflexive access lists for an internal interface, the IPv6 ACL should be one that is applied to outbound traffic. (In other words, use the access list opposite of the one used to define the IPv6 reflexive access list.)

This command allows IPv6 traffic entering your internal network to be evaluated against the reflexive access list. Use this command as an entry (condition statement) in the IPv6 ACL; the entry "points" to the IPv6 reflexive access list to be evaluated.
As with all IPv6 ACL entries, the order of entries is important. Normally, when a packet is evaluated against entries in an IPv6 ACL, the entries are evaluated in sequential order, and when a match occurs, no more entries are evaluated. With an IPv6 reflexive access list nested in an IPv6 ACL, the IPv6 ACL entries are evaluated sequentially up to the nested entry, then the IPv6 reflexive access list entries are evaluated sequentially, and then the remaining entries in the IPv6 ACL are evaluated sequentially. As usual, after a packet matches any of these entries, no more entries will be evaluated.

IPv6 reflexive access lists do not have any implicit deny or implicit permit statements.

Examples

The **evaluate** command in the following example nests the temporary IPv6 reflexive access lists named TCPTRAFFIC and UDPTRAFFIC in the IPv6 ACL named OUTBOUND. The two reflexive access lists are created dynamically (session filtering is "triggered") when incoming TCP or UDP traffic matches the applicable permit entry in the IPv6 ACL named INBOUND. The OUTBOUND IPv6 ACL uses the temporary TCPTRAFFIC or UDPTRAFFIC access list to match (evaluate) outgoing TCP or UDP traffic related to the triggered session. The TCPTRAFFIC and UDPTRAFFIC lists time out automatically when no IPv6 packets match the permit statement that triggered the session (the creation of the temporary reflexive access list).

The order of IPv6 reflexive access list entries is not important because only permit statements are allowed in IPv6 reflexive access lists and reflexive access lists do not have any implicit conditions. The OUTBOUND IPv6 ACL simply evaluates the UDPTRAFFIC reflexive access list first and, if there were no matches, the TCPTRAFFIC reflexive access list second. Refer to the **permit** command for more information on configuring IPv6 reflexive access lists.

```
ipv6 access-list INBOUND
  permit tcp any any eq bgp reflect TCPTRAFFIC
  permit tcp any any eq telnet reflect TCPTRAFFIC
  permit udp any any reflect UDPTRAFFIC
ipv6 access-list OUTBOUND
  evaluate UDPTRAFFIC
  evaluate TCPTRAFFIC
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ipv6 access-list</strong></td>
<td>Defines an IPv6 access list and enters IPv6 access list configuration mode.</td>
</tr>
<tr>
<td><strong>permit (IPv6)</strong></td>
<td>Sets permit conditions for an IPv6 access list.</td>
</tr>
<tr>
<td><strong>show ipv6 access-list</strong></td>
<td>Displays the contents of all current IPv6 access lists.</td>
</tr>
</tbody>
</table>
To change router actions for a signature or signature category, use the `event-action` command in signature-definition-action-engine or IPS-category-action configuration mode. To revert to the default router action values, use the `no` form of this command.

```
event-action action
no event-action
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>action</code></td>
<td>Router actions for a specified signature or signature category. The <code>action</code> argument can be any of the following options:</td>
</tr>
</tbody>
</table>
| | • deny-attacker-inline
| | • deny-connection-inline
| | • deny-packet-inline
| | • produce-alert
| | • reset-tcp-connection
| Note | Event actions for an individual signature must be entered on a single line. However, event actions associated with a category can be entered separately or on a single line. |

**Command Default**
Default values for the signature or signature category will be used.

**Command Modes**
Signature-definition-action-engine configuration (config-sigdef-action-engine)
IPS-category-action configuration (config-ips-category-action)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Signature-Based Changes**
After signature-based changes are complete, Cisco IOS Intrusion Prevention System (IPS) prompts the user to confirm whether or not the changes are acceptable. Confirming the changes instructs Cisco IOS IPS to compile the changes for the signature and modify memory structures to reflect the change. Also, Cisco IOS IPS will save the changes to the location specified via the `ip ips config location` command (for example, flash:ips5/*.xml).

You can issue the `show ip ips signatures` command to verify the event-action configuration. (The `show running-config` command does not show individual signature tuning information.)

**Signature Category-Based Changes**
After signature category-based changes are complete, the category tuning information is saved in the command-line interface (CLI) configuration.
Category configuration information is processed in the order that it is entered. Thus, it is recommended that the process of retiring all signatures occur before all other category tuning.

If a category is configured more than once, the parameters entered in the second configuration will be added to or will replace the previous configuration.

**Examples**

The following example shows how to configure signature 5726 to reset all TCP connections and produce an alert:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature-definition
Router(config-sigdef)# signature 5726 0
Router(config-sigdef-sig)# engine
Router(config-sigdef-sig-engine)# event-action reset-tcp-connection produce-alert
Router(config-sigdef-sig-engine)# exit
Router(config-sigdef-sig)# exit
Router(config-sigdef)# ^Z
```

Do you want to accept these changes? [confirm]

```
*Nov 9 21:50:55.847: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 12 of 11 engines
*Nov 9 21:50:55.859: %IPS-6-ENGINE_READY: multi-string - build time 12 ms - packets for this engine will be scanned
*Nov 9 21:50:55.859: %SYS-5-CONFIG_I: Configured from console by cisco on console
```

The following example shows how to tune event-action parameters for the signature category “adware/spyware.” All the tuning information will be applied to all signatures that belong to the adware/spyware signature category.

```
Router(config)# ip ips signature category
Router(config-ips-category)# category attack adware/spyware
Router(config-ips-category-action)# event-action produce-alert
Router(config-ips-category-action)# event-action deny-packet-inline
Router(config-ips-category-action)# event-action reset-tcp-connection
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# ^Z
```

Do you want to accept these changes:[confirm]

```
y
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>engine</td>
<td>Enters the signature-definition-action-engine configuration mode, which allows you to change router actions for a specified signature.</td>
</tr>
<tr>
<td>ip ips config location</td>
<td>Specifies the location in which the router will save signature information.</td>
</tr>
<tr>
<td>signature</td>
<td>Specifies a signature for which the CLI user tunings will be changed.</td>
</tr>
<tr>
<td>show ip ips</td>
<td>Displays IPS information such as configured sessions and signatures.</td>
</tr>
</tbody>
</table>
exception access-group

To configure a device exception in a global consumer configuration, use the `exception access-group` command in TMS consumer configuration mode. To remove the device exception from the global TMS configuration, use the `no` form of this command.

Note

Effective with Cisco IOS Release 12.4(20)T, the `exception access-group` command is not available in Cisco IOS software.

```
exception access-group extended-acl
no exception access-group extended-acl
```

Syntax Description

- `extended-acl` Name or number of the extended access list.

Command Default

None.

Command Modes

TMS consumer configuration (cfg-tms-cons)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(15)XZ</td>
<td>This command was integrated into Cisco IOS Release 12.4(15)XZ.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The `exception access-group` command is configured to attach a local device exception to a consumer process. A local device exception is an override configured on the consumer that negates a mitigation enforcement action sent from the controller or from a TMS Rules Engine configuration (mitigation type service policy) configured on the consumer.

For example, traffic from the 192.168.1.0/24 network is considered to be suspect. So, an ACL drop enforcement action is configured for all traffic sourced from this network. However, a device with a host address in this range (192.168.1.55) needs to transit over a specific consumer. A local device exception is configured on the consumer to override ACL drop enforcement action.

The device exception is configured locally. A host IP address (or any other subset of the network) is defined in an extended access list and then referenced by the `exception access-group` command. The `tms-class` command is configured to associate an interface with the device exception. The enforcement action configured on the controller is not applied to traffic that is permitted by the access list.

Examples

The following example configures an device exception for the 192.168.1.55 host address:

```
Router(config)# ip access-list extended NAMED_ACL
Router(config-ext-nacl)# permit tcp host 192.168.1.55 any
Router(config-ext-nacl)# exit
```
Router(config)# interface Ethernet 0/0
Router(config-if)# ip access-group NAMED_ACL in
Router(config-if)# tms-class
Router(config-if)# exit
Router(config)# tms consumer
Router(config-tms-cons)# exception access-group NAMED_ACL
Router(config-tms-cons)# service-policy type tms TMS_POL_1
Router(config-tms-cons)# end

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tms consumer</td>
<td>Configures a consumer process on a router or networking device.</td>
</tr>
<tr>
<td>tms-class</td>
<td>Associates an interface with an ACL drop enforcement action.</td>
</tr>
</tbody>
</table>
exclusive-domain

To add or remove a domain name to or from the exclusive domain list so that the Cisco IOS firewall does not have to send lookup requests to the vendor server, use the exclusive-domain command in URL parameter-map configuration mode. To disable this capability, use the no form of this command.

exclusive-domain {deny|permit} domain-name
no exclusive-domain {deny|permit} domain-name

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Removes the specified domain name from the exclusive domain list. Blocks all traffic destined for the specified domain name.</td>
</tr>
<tr>
<td>permit</td>
<td>Adds the specified domain name to the exclusive domain list. Permits all traffic destined for the specified domain name.</td>
</tr>
<tr>
<td>domain-name</td>
<td>Domain name that is added or removed from the exclusive domain name list; for example, <a href="http://www.example.com">www.example.com</a>.</td>
</tr>
</tbody>
</table>

Command Default

Disabled.

Command Modes

URL parameter-map configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

When you are creating or modifying a URL parameter map, you can enter the exclusive-domain subcommand after you enter the parameter-map type urlfilter command. For detailed information about creating a parameter map, see the parameter-map type urlfilter command.

The exclusive-domain command allows you to specify a list of domain names (exclusive domains) so that the Cisco IOS firewall does not create a lookup request for the traffic that is destined for one of the domains in the exclusive list. Thus, you can avoid sending lookup requests to the web server for traffic that is destined for a host that is completely allowed to all users. You can enter the complete domain name or a partial domain name.

Complete Domain Name

If you add a complete domain name, such as www.example.com, to the exclusive domain list, all traffic whose URLs are destined for this domain (such as www.example.com/news and www.example.com/index) is excluded from the URL filtering policies of the vendor server. On the basis of the configuration, the URLs are permitted or blocked (denied).

Partial Domain Name

If you add only a partial domain name to the exclusive domain list, such as example.com, all URLs whose domain names end with this partial domain name (such as www.example.com/products and www.example.com/eng) are excluded from the URL filtering policies of the vendor server. On the basis of the configuration, the URLs are permitted or blocked (denied).
### Examples

The following example adds cisco.com to the exclusive domain list:

```
parameter-map type urlfilter ul
  exclusive-domain permit example.com
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip urlfilter exclusive-domain</code></td>
<td>Adds or removes a domain name to or from the exclusive domain list so that the Cisco IOS firewall does not have to send lookup requests to the vendor server.</td>
</tr>
<tr>
<td><code>parameter-map type urlfilter</code></td>
<td>Creates or modifies a parameter map for URL filtering parameters.</td>
</tr>
</tbody>
</table>
F through H

- filter-hash, on page 283
- filter-id, on page 284
- filter-version, on page 285
- filter tunnel, on page 286
- fingerprint, on page 287
- firewall, on page 289
- flow restrict, on page 290
- fpm package-group, on page 292
- fpm package-info, on page 293
- fqdn (IKEv2 profile), on page 294
- grant auto rollover, on page 295
- grant auto trustpoint, on page 298
- grant none, on page 302
- grant ra-auto, on page 305
- group (firewall), on page 308
- group (authentication), on page 309
- group (IKE policy), on page 310
- group (IKEv2 proposal), on page 312
- group (local RADIUS server), on page 314
- group (RADIUS), on page 316
- group-lock, on page 318
- group-object, on page 320
- group size, on page 322
- gtp, on page 325
- hardware statistics, on page 327
- hash (ca-trustpoint), on page 328
- hash (cs-server), on page 330
- hash (IKE policy), on page 334
- heading, on page 336
- hide-url-bar, on page 337
- holdtime, on page 338
- hop-limit, on page 339
- host (webvpn url rewrite), on page 340
• hostname (IKEv2 keyring), on page 341
• hostname (WebVPN), on page 343
• http proxy-server, on page 344
• http-redirect, on page 345
• hw-module slot subslot only, on page 346
**filter-hash**

Effective with Cisco IOS Release 15.2(4)M, the filter-hash command is not available in Cisco IOS software.

To specify the hash for verification and validation of decrypted contents, use the `filter-hash` command in Flexible Packet Matching (FPM) encryption filter configuration mode.

```
filter-hash hash-value
```

**Syntax Description**

| hash-value | Hash value obtained from the encrypted traffic classification definition file (eTCDF). |

**Command Default**

No hash value is specified.

**Command Modes**

FPM encryption filter configuration (c-map-match-enc-config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(4)M</td>
<td>This command was removed from the Cisco IOS software.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you have access to an eTCDF or if you know valid values to configure encrypted FPM filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the `class-map type` command, and use the `match encrypted` command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the `filter-hash` command to specify the hash for verification and validation of decrypted contents.

**Examples**

The following example shows how to specify the hash value from the eTCDF file for verification and validation of decrypted contents:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# filter-hash AABBCCDD11223344
Router(c-map-match-enc-config)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map type</td>
<td>Creates a class map to be used for matching packets to a specified class.</td>
</tr>
<tr>
<td>match encrypted</td>
<td>Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode.</td>
</tr>
</tbody>
</table>
**filter-id**

**Note**

Effective with Cisco IOS Release 15.2(4)M, the **filter-id** command is not available in Cisco IOS software.

To specify a filter-level ID for encrypted filters, use the **filter-id** command in FPM match encryption filter configuration mode.

**Syntax Description**

```
filter-id  id-value
```

- **id-value**: Filter-level ID value.

**Command Default**

No filter ID is specified.

**Command Modes**

FPM match encryption filter configuration (c-map-match-enc-config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(4)M</td>
<td>This command was removed from the Cisco IOS software.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **filter-id** command to specify a filter-level ID for encrypted filters.

**Examples**

The following example shows how to specify the filter ID value for an encrypted filter:

```
Router(config)# class-map type access-control match-all cl
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# filter-id id2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class-map type</td>
<td>Creates a class map to be used for matching packets to a specified class.</td>
</tr>
<tr>
<td>match encrypted</td>
<td>Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode.</td>
</tr>
</tbody>
</table>
Effective with Cisco IOS Release 15.2(4)M, the `filter-version` command is not available in Cisco IOS software.

To specify the filter-level version value for the encrypted filter, use the `filter-version` command in FPM match encryption filter configuration mode.

```
filter-version version
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>version</code></td>
<td>Filter-level version value of the encrypted filter.</td>
</tr>
</tbody>
</table>

### Command Default

No filter version is specified.

### Command Modes

FPM match encryption filter configuration (c-map-match-enc-config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(4)M</td>
<td>This command was removed from the Cisco IOS software.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the `class-map type` command, and use the `match encrypted` command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the `filter-version` command to specify the filter-level version value for the encrypted filter.

### Examples

The following example shows how to specify the filter version for the encrypted filter:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# filter-version v1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>class-map type</code></td>
<td>Creates a class map to be used for matching packets to a specified class.</td>
</tr>
<tr>
<td><code>match encrypted</code></td>
<td>Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode.</td>
</tr>
</tbody>
</table>
To configure a SSL VPN tunnel access filter, use **filter tunnel** command in webvpn group policy configuration mode. To remove the tunnel access filter, use the **no** form of this command.

```
filter tunnel {extended-acl acl-name}
no filter tunnel
```

**Syntax Description**

- `extended-acl` Defines the filter on the basis of an extended access list (ACL). A named, numbered, or expanded access list is entered.
- `acl-name` Specifies the name for the access list.

**Command Default**

A SSL VPN tunnel access filter is not configured.

**Command Modes**

Webvpn group policy configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The tunnel access filter is used to control network- and application-level access.

**Examples**

The following example shows how to configure a deny access filter for any host from the 192.0.2.0/24 network:

```
Device(config)# access-list 101 deny ip 192.0.2.0 0.0.0.255 any
Device(config)# webvpn context context1
Device(config-webvpn-context)# policy group ONE
Device(config-webvpn-group)# filter tunnel 101
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy group</td>
<td>Enters webvpn group policy configuration mode to configure a policy group.</td>
</tr>
<tr>
<td>webvpn context</td>
<td>Enters webvpn context configuration mode to configure the SSL VPN context.</td>
</tr>
</tbody>
</table>
fingerprint

To preenter a fingerprint that can be matched against the fingerprint of an untrusted certification authority (CA) certificate during authentication, use the `fingerprint` command in `pki trustpoint configuration` mode. To remove the preentered fingerprint, use the `no` form of this command.

```
fingerprint ca-fingerprint
no fingerprint ca-fingerprint
```

**Syntax Description**
- `ca-fingerprint` Certificate fingerprint.

**Command Default**
A fingerprint is not preentered for a trustpoint, and if the authentication request is interactive, you must verify the fingerprint that is displayed during authentication of the CA certificate. If the authentication request is noninteractive, the certificate will be rejected without a preentered fingerprint.

**Command Modes**
pki trustpoint configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(12)</td>
<td>This command was introduced. This release supports only message digest algorithm 5 (MD5) fingerprints.</td>
</tr>
<tr>
<td>12.3(13)T</td>
<td>Support was added for Secure Hash Algorithm 1 (SHA1), but only for Cisco IOS T releases.</td>
</tr>
<tr>
<td>12.4(24)T</td>
<td>Support for IPv6 Secure Neighbor Discovery (SeND) was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Note**
Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

**Note**
An authentication request made using the CLI is considered an interactive request. An authentication request made using HTTP or another management tool is considered a noninteractive request.

**Note**
The fingerprint check is performed only while authenticating the certificate of the first untrusted Certificate authority in a given CA hierarchy. In other words, Subordinate-CA certificates are not subjected to fingerprint checking if the Root-CA certificate is trusted already, however in the absence of the Root-CA certificate, authenticating the Subordinate CA’s certificate first will result in fingerprint checking. This is as per the current design.
Preenter the fingerprint if you want to avoid responding to the verify question during CA certificate authentication or if you will be requesting authentication noninteractively. The preentered fingerprint may be either the MD5 fingerprint or the SHA1 fingerprint of the CA certificate.

If you are authenticating a CA certificate and the fingerprint was preentered, if the fingerprint matches that of the certificate, the certificate is accepted. If the preentered fingerprint does not match, the certificate is rejected.

If you are requesting authentication noninteractively, the fingerprint must be preentered or the certificate will be rejected. The verify question will not be asked when authentication is requested noninteractively.

If you are requesting authentication interactively without preentering the fingerprint, the fingerprint of the certificate will be displayed, and you will be asked to verify it.

**Examples**

The following example shows how to preenter an MD5 fingerprint before authenticating a CA certificate:

```plaintext
Router(config)# crypto pki trustpoint myTrustpoint
Router(ca-trustpoint)# fingerprint 6513D537 7AEA61B7 29B7E8CD BBA510B
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate myTrustpoint
Certificate has the following attributes:
   Fingerprint MD5: 6513D537 7AEA61B7 29B7E8CD BBA510B
   Fingerprint SHA1: 998CCFAA 5816ECDE 38FC217F 04C11F1D DA06667E
Trustpoint Fingerprint: 6513D537 7AEA61B7 29B7E8CD BBA510B
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
Router (config)#
```

The following is an example for Cisco Release 12.3(12). Note that the SHA1 fingerprint is not displayed because it is not supported by this release.

```plaintext
Router(config)# crypto ca trustpoint myTrustpoint
Router(ca-trustpoint)# fingerprint 6513D537 7AEA61B7 29B7E8CD BBA510B
Router(ca-trustpoint)# exit
Router(config)# crypto ca authenticate myTrustpoint
Certificate has the following attributes:
   Fingerprint: 6513D537 7AEA61B7 29B7E8CD BBA510B
Trustpoint Fingerprint: 6513D537 7AEA61B7 29B7E8CD BBA510B
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
Router(config)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ca authenticate</td>
<td>Authenticates the CA (by getting the certificate of the CA).</td>
</tr>
<tr>
<td>crypto ca trustpoint</td>
<td>Declares the CA that your router should use.</td>
</tr>
</tbody>
</table>
firewall

To specify secure virtual LAN (VLAN) groups and to attach them to firewall modules, use the `firewall` command in global configuration mode. To disable the configuration, use the `no` form of this command.

```
firewall {autostate|module number vlan-group number|multiple-vlan-interfaces|vlan-group number vlan-range}

no firewall {autostate|module number vlan-group number|multiple-vlan-interfaces|vlan-group number vlan-range}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autostate</td>
<td>Enables auto state.</td>
</tr>
<tr>
<td>module</td>
<td>Specifies the module number to which a VLAN group is attached.</td>
</tr>
<tr>
<td>number</td>
<td>Module number. Valid values are from 1 to 6.</td>
</tr>
<tr>
<td>vlan-group number</td>
<td>Specifies the secure group to which the VLANs are attached.</td>
</tr>
<tr>
<td>number</td>
<td>Group number. The range is from 1 to 65535.</td>
</tr>
<tr>
<td>multiple-vlan-interfaces</td>
<td>Enables multiple VLAN interfaces mode for firewall modules.</td>
</tr>
<tr>
<td>vlan-range</td>
<td>VLAN range. Valid values are from 2 to 1001 and 1006 to 4094.</td>
</tr>
</tbody>
</table>

**Command Default**

No secure VLAN groups are attached to firewall modules.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SX</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a VLAN group:

```
Router(config)# firewall vlan-group 34 1-20
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show firewall vlan-group</td>
<td>Displays secure VLANs attached to a secure group.</td>
</tr>
</tbody>
</table>
flow restrict

To restrict the traffic coming from Cisco Easy VPN inside interface to go out in clear text when a VPN tunnel is down, use the `flow restrict` command in Cisco Easy VPN Remote configuration mode. To allow traffic in a VPN connection, use the `no` form of this command.

```
flow restrict
no flow restrict
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

If this command is not used, all traffic will go out in clear text when a VPN connection is down.

**Command Modes**

Cisco Easy VPN Remote configuration (config-crypto-ezvpn)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before you configure the `flow restrict` command, you must use the `crypto ipsec client ezvpn` command to place the device in the Cisco Easy VPN remote configuration mode.

**Example**

```
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
!
!
crypto ipsec transform-set 3DES-SHA esp-3des esp-sha-hmac
!
!
crypto ipsec client ezvpn customer-vpn
  connect auto
  group vpntest key cisco
  mode network-extension
  peer 10.198.16.132 default
  flow restrict
  virtual-interface 2
  username cisco password cisco
  xauth userid mode local
!  
crypto ipsec client ezvpn aap01651
  connect auto
  group vpntest key cisco
  mode network-extension
  peer 10.198.16.153
  flow restrict
  virtual-interface 1
  username cisco password cisco
  xauth userid mode local
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crypto ipsec client ezvpn</code></td>
<td>Creates a Cisco Easy VPN remote configuration.</td>
</tr>
</tbody>
</table>
**fpm package-group**

**Note**
Effective with Cisco IOS Release 15.2(4)M, the `fpm package-group` command is not available in Cisco IOS software.

To configure flexible packet matching (fpm) package support, use the `fpm package-group` command in global configuration mode. To disable fpm package support, use the `no` form of this command.

```
fpm package-group [fpm-group-name]
no fpm package-group [fpm-group-name]
```

**Syntax Description**
- `fpm-group-name`: Specifies the fpm package group name.

**Command Default**
FPM groups are not configured by default.

**Command Modes**
Global configuration (config)\#

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(4)M</td>
<td>This command was removed from the Cisco IOS software.</td>
</tr>
</tbody>
</table>

**Examples**

The following example enables fpm package-group:

`Router(config)# fpm package-group fpm-group-76`

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fpm package-info</td>
<td>Enables fpm package transfer.</td>
</tr>
</tbody>
</table>
fpm package-info

Note

Effective with Cisco IOS Release 15.2(4)M, the fpm package-info command is not available in Cisco IOS software.

To configure flexible packet matching (FPM) package transfer from an FPM server to a local server, use the fpm package-info command in global configuration mode. To disable fpm packet transfer, use the no form of this command.

Syntax Description

This command has no keywords or arguments.

Command Default

The command is not configured by default.

Command Modes

Global configuration (config)#

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(4)M</td>
<td>This command was removed from the Cisco IOS software.</td>
</tr>
</tbody>
</table>

Examples

The following example enables fpm package transfer:

Router(config)# fpm package-info

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fpm package-group</td>
<td>Configures fpm package group support.</td>
</tr>
<tr>
<td>show fpm package-group</td>
<td>Displays fpm package matching support configuration details.</td>
</tr>
<tr>
<td>show fpm package-info</td>
<td>Displays fpm package transfer configuration details.</td>
</tr>
</tbody>
</table>
fqdn (IKEv2 profile)

To derive the name mangler from the remote identity of type Fully Qualified Domain Name (FQDN), use the `fqdn` command in IKEv2 name mangler configuration mode. To remove the name derived from FQDN, use the `no` form of this command.

```
fqdn {all|domain|hostname}
no fqdn
```  

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Derives the name mangler from the entire FQDN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>Derives the name mangler from the domain name of FQDN.</td>
</tr>
<tr>
<td>hostname</td>
<td>Derives the name mangler from the hostname of FQDN.</td>
</tr>
</tbody>
</table>

Command Default
No default behavior or values.

Command Modes
IKEv2 name mangler configuration (config-ikev2-name-mangler)

Command History
```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(3)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
</tbody>
</table>
```

Usage Guidelines
Use this command to derive the name mangler from the remote identity of type FQDN.

Examples
The following example shows how to derive a name for the name mangler from the hostname of FQDN:

```
Router(config)# crypto ikev2 name-mangler mangler2
Router(config-ikev2-name-mangler)# fqdn hostname
```  

Related Commands
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2 name-mangler</td>
<td>Defines a name mangler.</td>
</tr>
</tbody>
</table>
```
**grant auto rollover**

To enable automatic granting of certificate reenrollment requests for a Cisco IOS subordinate certificate authority (CA) server or registration authority (RA) mode CA, use the `grant auto rollover` command in certificate server configuration mode. To disable automatic granting of certificate reenrollment requests for a Cisco IOS subordinate or RA-mode CA server, use the `no` form of this command.

```
grant auto rollover {ca-cert|ra-cert}
no grant auto rollover {ca-cert|ra-cert}
```

**Syntax Description**
- `ca-cert` Specifies that auto renewal is enabled for the subordinate CA rollover certificate.
- `ra-cert` Specifies that auto renewal is enabled for the RA-mode CA rollover certificate.

**Command Default**
Automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA-mode CA reenrollment requests is not enabled. Reenrollment requests will have to be granted manually.

**Command Modes**
Certificate server configuration (cs-server)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
You must configure the `crypto pki server` command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

The first time a CA is enabled, a certificate request is sent to its superior CA. This initial request must be granted manually. The `grant auto rollover` command allows subsequent renewal certificate grant requests to be automatically processed by the CA for either a subordinate CA certificate (by designating the `ca-cert` keyword) or an RA-mode CA (by designating the `ra-cert` keyword), thereby eliminating the need for operator intervention.

**Examples**
The following example shows how the user can enable automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server:

```
Router(config)#crypto pki server CA
Router(cs-server)#grant auto rollover ca-cert
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-rollover</td>
<td>Enables the automated CA certificate rollover functionality.</td>
</tr>
<tr>
<td>cdp-url</td>
<td>Specifies a CDP to be used in certificates that are issued by the certificate server.</td>
</tr>
<tr>
<td>crl (cs-server)</td>
<td>Specifies the CRL PKI CS.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>crypto pki server</td>
<td>Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials</td>
</tr>
<tr>
<td>database archive</td>
<td>Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.</td>
</tr>
<tr>
<td>database level</td>
<td>Controls what type of data is stored in the certificate enrollment database.</td>
</tr>
<tr>
<td>database url</td>
<td>Specifies the location where database entries for the CS is stored or published.</td>
</tr>
<tr>
<td>database username</td>
<td>Specifies the requirement of a username or password to be issued when accessing the primary database location.</td>
</tr>
<tr>
<td>default (cs-server)</td>
<td>Resets the value of the CS configuration command to its default.</td>
</tr>
<tr>
<td>grant auto trustpoint</td>
<td>Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.</td>
</tr>
<tr>
<td>grant none</td>
<td>Specifies all certificate requests to be rejected.</td>
</tr>
<tr>
<td>grant ra-auto</td>
<td>Specifies that all enrollment requests from an RA be granted automatically.</td>
</tr>
<tr>
<td>hash (cs-server)</td>
<td>Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.</td>
</tr>
<tr>
<td>issuer-name</td>
<td>Specifies the DN as the CA issuer name for the CS.</td>
</tr>
<tr>
<td>lifetime (cs-server)</td>
<td>Specifies the lifetime of the CA or a certificate.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mode ra</td>
<td>Enters the PKI server into RA certificate server mode.</td>
</tr>
<tr>
<td>mode sub-cs</td>
<td>Enters the PKI server into sub-certificate server mode</td>
</tr>
<tr>
<td>redundancy (cs-server)</td>
<td>Specifies that the active CS is synchronized to the standby CS.</td>
</tr>
<tr>
<td>serial-number (cs-server)</td>
<td>Specifies whether the router serial number should be included in the certificate request.</td>
</tr>
<tr>
<td>show (cs-server)</td>
<td>Displays the PKI CS configuration.</td>
</tr>
<tr>
<td>shutdown (cs-server)</td>
<td>Allows a CS to be disabled without removing the configuration.</td>
</tr>
</tbody>
</table>
grant auto trustpoint

To specify the certification authority (CA) trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests, use the `grant auto trustpoint` command in certificate server configuration mode. To remove the name of the trustpoint holding the trusted CA certificate, use the `no` form of this command.

```
grant auto trustpoint  label
no grant auto trustpoint  label
```

### Syntax Description

| label | Name of the non-Cisco IOS CA trustpoint. |

### Command Default

No default behavior or values.

### Command Modes

Certificate server configuration (cs-server)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(11)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)SXE</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXE.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

You must configure the `crypto pki server` command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

After the network administrator for the server configures and authenticates a trustpoint for the CA of another vendor, the `grant auto trustpoint` command is issued to reference the newly created trustpoint and enroll the router with a Cisco IOS CA.

#### Note

The newly created trustpoint can only be used one time (which occurs when the router is enrolled with the Cisco IOS CA). After the initial enrollment is successfully completed, the credential information will be deleted from the enrollment profile.

The Cisco IOS certificate server will automatically grant only the requests from clients who were already enrolled with the CA of another vendor. All other requests must be manually granted—unless the server is set to be in auto grant mode (through the `grant automatic` command).

#### Caution

The `grant automatic` command can be used for testing and building simple networks and should be disabled before the network is accessible by the Internet. However, it is recommended that you do not issue this command if your network is generally accessible.

### Examples

The following example shows how to configure a client router and a Cisco IOS certificate server to exchange enrollment requests through a certificate enrollment profile:

```bash
grant auto trustpoint  label
```
! Define the trustpoint “msca-root” that points to the non-Cisco IOS CA and enroll and ! authenticate the client with the non-Cisco IOS CA.
crypto pki trustpoint msca-root
    enrollment mode ra
    enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
    ip-address FastEthernet2/0
    revocation-check crl

! Configure trustpoint “cs” for Cisco IOS CA.
crypto pki trustpoint cs
    enrollment profile cs1
    revocation-check crl

! Define enrollment profile “cs1,” which points to Cisco IOS CA and mention (via the ! enrollment credential command) that “msca-root” is being initially enrolled with the ! Cisco IOS CA.
crypto pki profile enrollment cs1
    enrollment url http://cs:80
    enrollment credential msca-root

! Configure the certificate server, and issue the grant auto trustpoint command to ! instruct ! the certificate server to accept enrollment request only from clients who are ! already ! enrolled with trustpoint “msca-root.”
crypto pki server cs
    database level minimum
    database url nvram:
    issuer-name CN=cs
    grant auto trustpoint msca-root

! crypto pki trustpoint cs
    revocation-check crl
rsakeypair cs

! crypto pki trustpoint msca-root
    enrollment mode ra
    enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
    revocation-check crl

---

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-rollover</td>
<td>Enables the automated CA certificate rollover functionality.</td>
</tr>
<tr>
<td>cdp-url</td>
<td>Specifies a CDP to be used in certificates that are issued by the certificate server.</td>
</tr>
<tr>
<td>crl (cs-server)</td>
<td>Specifies the CRL PKI CS.</td>
</tr>
<tr>
<td>crypto pki server</td>
<td>Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials</td>
</tr>
<tr>
<td>database archive</td>
<td>Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>database level</td>
<td>Controls what type of data is stored in the certificate enrollment database.</td>
</tr>
<tr>
<td>database url</td>
<td>Specifies the location where database entries for the CS is stored or published.</td>
</tr>
<tr>
<td>database username</td>
<td>Specifies the requirement of a username or password to be issued when accessing the primary database location.</td>
</tr>
<tr>
<td>default (cs-server)</td>
<td>Resets the value of the CS configuration command to its default.</td>
</tr>
<tr>
<td>grant auto rollover</td>
<td>Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.</td>
</tr>
<tr>
<td>grant none</td>
<td>Specifies all certificate requests to be rejected.</td>
</tr>
<tr>
<td>grant ra-auto</td>
<td>Specifies that all enrollment requests from an RA be granted automatically.</td>
</tr>
<tr>
<td>hash (cs-server)</td>
<td>Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.</td>
</tr>
<tr>
<td>issuer-name</td>
<td>Specifies the DN as the CA issuer name for the CS.</td>
</tr>
<tr>
<td>lifetime (cs-server)</td>
<td>Specifies the lifetime of the CA or a certificate.</td>
</tr>
<tr>
<td>mode ra</td>
<td>Enters the PKI server into RA certificate server mode.</td>
</tr>
<tr>
<td>mode sub-cs</td>
<td>Enters the PKI server into sub-certificate server mode</td>
</tr>
<tr>
<td>redundancy (cs-server)</td>
<td>Specifies that the active CS is synchronized to the standby CS.</td>
</tr>
<tr>
<td>serial-number (cs-server)</td>
<td>Specifies whether the router serial number should be included in the certificate request.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>show (cs-server)</td>
<td>Displays the PKI CS configuration.</td>
</tr>
<tr>
<td>shutdown (cs-server)</td>
<td>Allows a CS to be disabled without removing the configuration.</td>
</tr>
</tbody>
</table>
grant none

To specify all certificate requests to be rejected, use the grant none command in certificate server configuration mode. To disable automatic rejection of certificate enrollment, use the no form of this command.

grant none
no grant none

Syntax Description

This command has no arguments or keywords.

Command Default

Certificate enrollment is manual; that is, authorization is required.

Command Modes

Certificate server configuration (cs-server)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You must configure the crypto pki server command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

Examples

The following example shows how to automatically reject all certificate enrollment requests for the certificate server “myserver”:

Router#(config) ip http server
Router#(config) crypto pki server myserver
Router#(cs-server) database level minimum
Router#(cs-server)#
grant none

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-rollover</td>
<td>Enables the automated CA certificate rollover functionality.</td>
</tr>
<tr>
<td>cdp-url</td>
<td>Specifies a CDP to be used in certificates that are issued by the certificate server.</td>
</tr>
<tr>
<td>crl (cs-server)</td>
<td>Specifies the CRL PKI CS.</td>
</tr>
<tr>
<td>crypto pki server</td>
<td>Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>database archive</td>
<td>Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.</td>
</tr>
<tr>
<td>database level</td>
<td>Controls what type of data is stored in the certificate enrollment database.</td>
</tr>
<tr>
<td>database url</td>
<td>Specifies the location where database entries for the CS is stored or published.</td>
</tr>
<tr>
<td>database username</td>
<td>Specifies the requirement of a username or password to be issued when accessing the primary database location.</td>
</tr>
<tr>
<td>default (cs-server)</td>
<td>Resets the value of the CS configuration command to its default.</td>
</tr>
<tr>
<td>grant auto rollover</td>
<td>Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.</td>
</tr>
<tr>
<td>grant auto trustpoint</td>
<td>Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.</td>
</tr>
<tr>
<td>grant ra-auto</td>
<td>Specifies that all enrollment requests from an RA be granted automatically.</td>
</tr>
<tr>
<td>hash (cs-server)</td>
<td>Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.</td>
</tr>
<tr>
<td>issuer-name</td>
<td>Specifies the DN as the CA issuer name for the CS.</td>
</tr>
<tr>
<td>lifetime (cs-server)</td>
<td>Specifies the lifetime of the CA or a certificate.</td>
</tr>
<tr>
<td>mode ra</td>
<td>Enters the PKI server into RA certificate server mode.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mode sub-cs</td>
<td>Enters the PKI server into sub-certificate server mode</td>
</tr>
<tr>
<td>redundancy (cs-server)</td>
<td>Specifies that the active CS is synchronized to the standby CS.</td>
</tr>
<tr>
<td>serial-number (cs-server)</td>
<td>Specifies whether the router serial number should be included in the certificate request.</td>
</tr>
<tr>
<td>show (cs-server)</td>
<td>Displays the PKI CS configuration.</td>
</tr>
<tr>
<td>shutdown (cs-server)</td>
<td>Allows a CS to be disabled without removing the configuration.</td>
</tr>
</tbody>
</table>
grant ra-auto

To specify that all enrollment requests from a Registration Authority (RA) be granted automatically, use the `grant ra-auto` command in certificate server configuration mode. To disable automatic certificate enrollment, use the `no` form of this command.

```
grant ra-auto
no grant ra-auto
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Certificate enrollment is manual; that is, authorization is required.

**Command Modes**

Certificate server configuration (cs-server)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must configure the `crypto pki server` command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

When grant ra-auto mode is configured on the issuing certificate server, ensure that the RA mode certificate server is running in manual grant mode so that enrollment requests are authorized individually by the RA.

**Note**

For the `grant ra-auto` command to work, you have to include “cn=ioscs RA” or “ou=ioscs RA” in the subject name of the RA certificate.

**Examples**

The following output shows that the issuing certificate server is configured to issue a certificate automatically if the request comes from an RA:

```
Router (config)# crypto pki server myserver
Router-ca (cs-server)# grant ra-auto
% This will cause all certificate requests that are already authorized by known RAs to be automatically granted.
Are you sure you want to do this? [yes/no]:yes
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-rollover</td>
<td>Enables the automated CA certificate rollover functionality.</td>
</tr>
<tr>
<td>cdp-url</td>
<td>Specifies a CDP to be used in certificates that are issued by the certificate server.</td>
</tr>
<tr>
<td>crl (cs-server)</td>
<td>Specifies the CRL PKI CS.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>crypto pki server</td>
<td>Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials</td>
</tr>
<tr>
<td>database archive</td>
<td>Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.</td>
</tr>
<tr>
<td>database level</td>
<td>Controls what type of data is stored in the certificate enrollment database.</td>
</tr>
<tr>
<td>database url</td>
<td>Specifies the location where database entries for the CS is stored or published.</td>
</tr>
<tr>
<td>database username</td>
<td>Specifies the requirement of a username or password to be issued when accessing the primary database location.</td>
</tr>
<tr>
<td>default (cs-server)</td>
<td>Resets the value of the CS configuration command to its default.</td>
</tr>
<tr>
<td>grant auto rollover</td>
<td>Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.</td>
</tr>
<tr>
<td>grant auto trustpoint</td>
<td>Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.</td>
</tr>
<tr>
<td>grant none</td>
<td>Specifies all certificate requests to be rejected.</td>
</tr>
<tr>
<td>hash (cs-server)</td>
<td>Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.</td>
</tr>
<tr>
<td>issuer-name</td>
<td>Specifies the DN as the CA issuer name for the CS.</td>
</tr>
<tr>
<td>lifetime (cs-server)</td>
<td>Specifies the lifetime of the CA or a certificate.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mode ra</td>
<td>Enters the PKI server into RA certificate server mode.</td>
</tr>
<tr>
<td>mode sub-cs</td>
<td>Enters the PKI server into sub-certificate server mode.</td>
</tr>
<tr>
<td>redundancy (cs-server)</td>
<td>Specifies that the active CS is synchronized to the standby CS.</td>
</tr>
<tr>
<td>serial-number (cs-server)</td>
<td>Specifies whether the router serial number should be included in the certificate request.</td>
</tr>
<tr>
<td>show (cs-server)</td>
<td>Displays the PKI CS configuration.</td>
</tr>
<tr>
<td>shutdown (cs-server)</td>
<td>Allows a CS to be disabled without removing the configuration.</td>
</tr>
</tbody>
</table>
group (firewall)

To enter redundancy application group configuration mode, use the group command in redundancy application configuration mode. To remove the group configuration, use the no form of this command.

```
group id
no group id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Redundancy group ID. Valid values are 1 and 2.</td>
</tr>
</tbody>
</table>

**Command Default**

No group is configured.

**Command Modes**

Redundancy application configuration (config-red-app)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.1S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a redundancy group with group ID 1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>application redundancy</td>
<td>Enters redundancy application configuration mode.</td>
</tr>
</tbody>
</table>
**group (authentication)**

To specify the authentication, authorization, and accounting (AAA) TACACS+ server group to use for preauthentication, use the `group` command in AAA preauthentication configuration mode. To remove the `group` command from your configuration, use the `no` form of this command.

```
group tacacs+ server-group
no group tacacs+ server-group
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tacacs+</td>
<td>Uses a TACACS+ server for authentication.</td>
</tr>
<tr>
<td>server-group</td>
<td>Name of the server group to use for authentication.</td>
</tr>
</tbody>
</table>

**Command Default**

No method list is configured.

**Command Modes**

AAA preauthentication configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must configure the `group` command before you configure any other AAA preauthentication command (`clid`, `ctype`, `dnis`, or `dnis bypass`).

**Examples**

The following example enables Dialed Number Identification Service (DNIS) preauthentication using the abc123 server group and the password aaa-DNIS:

```
aaa preauth
  group abc123
  dnis password aaa-DNIS
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa preauth</code></td>
<td>Enters AAA preauthentication mode.</td>
</tr>
<tr>
<td><code>dnis (authentication)</code></td>
<td>Enables AAA preauthentication using DNIS.</td>
</tr>
</tbody>
</table>
group (IKE policy)

To specify one or more Diffie-Hellman (DH) group identifier(s) for use in an Internet Key Exchange (IKE) policy, which defines a set of parameters to be used during IKE negotiation, use the **group** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. To reset the DH group identifier to the default value, use the **no** form of this command.

```
  group {1|2|5|14|16|19|20|24}
  no group
```

### Syntax Description

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Specifies the 768-bit DH group.</td>
</tr>
<tr>
<td>2</td>
<td>Specifies the 1024-bit DH group.</td>
</tr>
<tr>
<td>5</td>
<td>Specifies the 1536-bit DH group.</td>
</tr>
<tr>
<td>14</td>
<td>Specifies the 2048-bit DH group.</td>
</tr>
<tr>
<td>15</td>
<td>Specifies the 3072-bit DH group.</td>
</tr>
<tr>
<td>16</td>
<td>Specifies the 4096-bit DH group.</td>
</tr>
<tr>
<td>19</td>
<td>Specifies the 256-bit elliptic curve DH (ECDH) group.</td>
</tr>
<tr>
<td>20</td>
<td>Specifies the 384-bit ECDH group.</td>
</tr>
<tr>
<td>21</td>
<td>Specifies the 521-bit elliptic curve DH (ECDH) group.</td>
</tr>
<tr>
<td>24</td>
<td>Specifies the 2048-bit DH/DSA group.</td>
</tr>
</tbody>
</table>

### Command Default

DH group 1

### Command Modes

ISAKMP policy configuration (config-isakmp)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(1.3)T</td>
<td>Support was added for DH group 5.</td>
</tr>
<tr>
<td>12.4(4)T</td>
<td>Support for IPv6 was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.2</td>
<td>Support was added for DH groups 14, 15, and 16 on the Cisco ASR 1000 series routers.</td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
</tr>
<tr>
<td>15.1(2)T</td>
<td>This command was modified. The 14, 15, 16, 19, and 20 keywords were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

The group chosen must be strong enough (have enough bits) to protect the IPsec keys during negotiation. A generally accepted guideline recommends the use of a 2048-bit group after 2013 (until 2030). Either group 14 or group 24 can be selected to meet this guideline. Even if a longer-lived security method is needed, the use of Elliptic Curve Cryptography is recommended, but group 15 and group 16 can also be considered.

The ISAKMP group and the IPsec perfect forward secrecy (PFS) group should be the same if PFS is used. If PFS is not used, a group is not configured in the IPsec crypto map.

**Examples**

The following example shows how to configure an IKE policy with the 1024-bit DH group (all other parameters are set to the defaults):

```
Router(config)# crypto isakmp policy 15
Router(config-isakmp) group 2
Router(config-isakmp)
exit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication (IKE policy)</td>
<td>Specifies the authentication method within an IKE policy.</td>
</tr>
<tr>
<td>crypto isakmp policy</td>
<td>Defines an IKE policy.</td>
</tr>
<tr>
<td>encryption (IKE policy)</td>
<td>Specifies the encryption algorithm within an IKE policy.</td>
</tr>
<tr>
<td>hash (IKE policy)</td>
<td>Specifies the hash algorithm within an IKE policy.</td>
</tr>
<tr>
<td>lifetime (IKE policy)</td>
<td>Specifies the lifetime of an IKE SA.</td>
</tr>
<tr>
<td>show crypto isakmp policy</td>
<td>Displays the parameters for each IKE policy.</td>
</tr>
</tbody>
</table>
group (IKEv2 proposal)

To specify one or more Diffie-Hellman (DH) group identifier(s) for use in an Internet Key Exchange Version 2 (IKEv2) proposal, use the `group` command in IKEv2 proposal configuration mode. To reset the DH group identifier to the default value, use the `no` form of this command.

```
group group_type
no group
```

**Syntax Description**

- `group_type`: Specifies the DH group.

**Command Default**

DH group 2 and 5 in the IKEv2 proposal.

**Command Modes**

IKEv2 proposal configuration (config-ikev2-proposal)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(2)T</td>
<td>This command was modified. The 14, 15, 16, 19, and 20 keywords were added.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

The group type can be one of the following:

<table>
<thead>
<tr>
<th>Group Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Specifies the 768-bit DH group.</td>
</tr>
<tr>
<td>2</td>
<td>Specifies the 1024-bit DH group.</td>
</tr>
<tr>
<td>5</td>
<td>Specifies the 1536-bit DH group.</td>
</tr>
<tr>
<td>14</td>
<td>Specifies the 2048-bit DH group.</td>
</tr>
<tr>
<td>15</td>
<td>Specifies the 3072-bit DH group.</td>
</tr>
<tr>
<td>16</td>
<td>Specifies the 4096-bit DH group.</td>
</tr>
<tr>
<td>19</td>
<td>Specifies the 256-bit elliptic curve DH (ECDH) group.</td>
</tr>
<tr>
<td>Group Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>20</td>
<td>Specifies the 384-bit ECDH group.</td>
</tr>
<tr>
<td>21</td>
<td>Specifies the 521-bit elliptic curve DH (ECDH) group.</td>
</tr>
<tr>
<td>24</td>
<td>Specifies the 2048-bit DH/DSA group.</td>
</tr>
</tbody>
</table>

The group chosen must be strong enough (have enough bits) to protect the IPsec keys during negotiation. A generally accepted guideline recommends the use of a 2048-bit group after 2013 (until 2030). Either group 14 or group 24 can be selected to meet this guideline. Even if a longer-lived security method is needed, the use of Elliptic Curve Cryptography is recommended, but group 15 and group 16 can also be considered.

### Examples

The following example shows how to configure an IKEv2 proposal with the 1024-bit DH group:

```
Device(config)# crypto ikev2 proposal proposal1
Device(config-ikev2-proposal)# group 2
Device(config-ikev2-proposal)# exit
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2 proposal</td>
<td>Defines an IKEv2 proposal.</td>
</tr>
<tr>
<td>encryption (ikev2 proposal)</td>
<td>Specifies the encryption algorithm in an IKEv2 proposal.</td>
</tr>
<tr>
<td>integrity (ikev2 proposal)</td>
<td>Specifies the integrity algorithm in an IKEv2 proposal.</td>
</tr>
<tr>
<td>show crypto ikev2 proposal</td>
<td>Displays the algorithms configured in each IKEv2 proposal.</td>
</tr>
</tbody>
</table>
**group (local RADIUS server)**

To enter user group configuration mode and to configure shared settings for a user group, use the `group` command in local RADIUS server configuration mode. To remove the group configuration from the local RADIUS server, use the `no` form of this command.

```
group group-name
no group  group-name
```

**Syntax Description**

- `group-name`: Name of user group.

**Command Default**

No default behavior or values

**Command Modes**

Local RADIUS server configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(11)JA</td>
<td>This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.</td>
</tr>
<tr>
<td>12.3(11)T</td>
<td>This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows that shared settings are being configured for group “team1”:

```
group team1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>block count</td>
<td>Configures the parameters for locking out members of a group to help protect against unauthorized attacks.</td>
</tr>
<tr>
<td>clear radius local-server</td>
<td>Clears the statistics display or unblocks a user.</td>
</tr>
<tr>
<td>debug radius local-server</td>
<td>Displays the debug information for the local server.</td>
</tr>
<tr>
<td>nas</td>
<td>Adds an access point or router to the list of devices that use the local authentication server.</td>
</tr>
<tr>
<td>radius-server host</td>
<td>Specifies the remote RADIUS server host.</td>
</tr>
<tr>
<td>radius-server local</td>
<td>Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.</td>
</tr>
<tr>
<td>reauthentication time</td>
<td>Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.</td>
</tr>
<tr>
<td>show radius local-server statistics</td>
<td>Displays statistics for a local network access server.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>ssid</td>
<td>Specifies up to 20 SSIDs to be used by a user group.</td>
</tr>
<tr>
<td>user</td>
<td>Authorizes a user to authenticate using the local authentication server.</td>
</tr>
<tr>
<td>vlan</td>
<td>Specifies a VLAN to be used by members of a user group.</td>
</tr>
</tbody>
</table>
To specify the authentication, authorization, and accounting (AAA) RADIUS server group to use for preauthentication, use the `group` command in AAA preauthentication configuration mode. To remove the `group` command from your configuration, use the `no` form of this command.

```plaintext
group server-group
no group server-group
```

### Syntax Description
- `server-group` Specifies a AAA RADIUS server group.

### Command Default
No default behavior or values.

### Command Modes
- AAA preauthentication configuration

### Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
You must configure a RADIUS server group with the `aaa group server radius` command in global configuration mode before using the `group` command in AAA preauthentication configuration mode.

You must configure the `group` command before you configure any other AAA preauthentication command (`clid, ctype, dnis, or dnis bypass`).

### Examples
The following example shows the creation of a RADIUS server group called “maestro” and then specifies that DNIS preauthentication be performed using this server group:

```plaintext
aaa group server radius maestro
    server 10.1.1.1
    server 10.2.2.2
    server 10.3.3.3
aaa preauth
    group maestro
    dnis required
```

### Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa group server radius</code></td>
<td>Groups different RADIUS server hosts into distinct lists and distinct methods.</td>
</tr>
<tr>
<td><code>clid</code></td>
<td>Preauthenticates calls on the basis of the CLID number.</td>
</tr>
<tr>
<td><code>ctype</code></td>
<td>Preauthenticates calls on the basis of the call type.</td>
</tr>
<tr>
<td><code>dnis (RADIUS)</code></td>
<td>Preauthenticates calls on the basis of the DNIS number.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>dnis bypass (AAA preauthentication configuration)</td>
<td>Specifies a group of DNIS numbers that will be bypassed for preauthentication.</td>
</tr>
</tbody>
</table>
group-lock

The **group-lock** command attribute is used to check if a user attempting to connect to a group belongs to this group. This attribute is used in conjunction with the extended authentication (Xauth) username. The user name must include the group to which it belongs. The group is then matched against the VPN group name (ID_KEY_ID) that is passed during the Internet Key Exchange (IKE). If the groups do not match, then the client connection is terminated.

To allow the extended authentication (Xauth) username to be entered when preshared key authentication is used with IKE, use the **group-lock** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove the group lock, use the **no** form of this command.

---

**Note**

Preshared keys are supported only. Certificates are not supported.

```plaintext
    group-lock
    no  group-lock
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Group lock is not configured.

**Command Modes**

ISAKMP group configuration (config-isakmp-group)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(13)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The Group-Lock attribute can be used if preshared key authentication is used with IKE. When the user enables the **group-lock** command attribute, one of the following extended Xauth usernames can be entered:

- name/group
- name\group
- name@group
- name%group

where the `/ @ %` are the delimiters. The group that is specified after the delimiter is then compared against the group identifier that is sent during IKE aggressive mode. The groups must match or the connection is rejected.
Caution
Do not use the Group-Lock attribute if you are using RSA signature authentication mechanisms such as certificates. Use the User-VPN-Group attribute instead.

The Group-Lock attribute is configured on a Cisco IOS router or in the RADIUS profile. This attribute has local (gateway) significance only and is not passed to the client.

Note
If local authentication is used, then the Group-Lock attribute is the only option.

The username in the local or RADIUS database must be of the following format:
username[\/,\%,@]group.

Examples
The following example shows how Group-Lock attribute is configured in the CLI using the `group-lock` command:

```
crypto isakmp client configuration group cisco
    group-lock
```

The following example shows how an attribute-value (AV) pair for the User-VPN-Group attribute is added in the RADIUS configuration:

```
ipse:group-lock=1
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>acl</code></td>
<td>Configures split tunneling.</td>
</tr>
<tr>
<td><code>crypto isakmp client configuration group</code></td>
<td>Specifies the DNS domain to which a group belongs.</td>
</tr>
</tbody>
</table>
**group-object**

To specify a nested reference to a type of user group within an object group, use the `group-object` command in object-group identity configuration mode. To remove the user group from the object group, use the `no` form of this command.

```
group-object name
no group-object name
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Nested user group name.</td>
</tr>
</tbody>
</table>

### Command Default

No nested user group is defined.

### Command Modes

Object-group identity configuration (config-object-group)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(1)S</td>
<td>This command was introduced in Cisco IOS Release 15.2(1)S.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.5</td>
<td>This command was introduced in Cisco IOS XE Release 3.5.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

In addition to a security group that is specified for the object group, a group object can be specified for a nested user group. The `group-object` command is used in the class map configuration of the Security Group Access (SGA) Zone-Based Policy firewall (ZBPF). Multiple nested user groups can be specified using this command.

**Note**

A policy map must also be configured for the SGA ZBPF.

### Examples

The following example shows how the `group-object` command is used in the class map configuration of the SGA ZBPF.

```
Router(config)# object-group security myobject1
Router(config-object-group)# security-group tag-id 1
Router(config-object-group)# end
Router(config)# object-group security myobject1b
Router(config-object-group)# security-group tag-id 2
Router(config-object-group)# end
Router(config)# object-group security myobject1
Router(config-object-group)# group-object myobject1a
Router(config-object-group)# group-object myobject1b
Router(config-object-group)# end
Router(config)# class-map type inspect match-any myclass1
Router(config-cmap)# match group-object security source myobject1
Router(config-cmap)# end
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug object-group event</td>
<td>Enables debug messages for object-group events.</td>
</tr>
<tr>
<td>match group-object security</td>
<td>Matches traffic from a user in the security group.</td>
</tr>
<tr>
<td>object-group security</td>
<td>Creates an object group to identify traffic coming from a specific user or endpoint.</td>
</tr>
<tr>
<td>security-group</td>
<td>Specifies the membership of the security group for an object group.</td>
</tr>
<tr>
<td>show object-group</td>
<td>Displays the content of all user groups.</td>
</tr>
</tbody>
</table>
**group size**

To set the group size (sender ID length) for Suite B, use the `group size` command in GDOI local server configuration mode. To return a group size to the default size, use the `no` form of this command.

```
group size {small {8 | 12 | 16} | medium | large}
no group size [small {8 | 12 | 16} | medium | large]
```

| Syntax Description | small {8 | 12 | 16} | Specifies an 8-, 12-, or 16-bit sender identifier (SID). |
|--------------------|---------------------|--------------------------------------------------------|
|                    | medium              | Specifies a 24-bit SID.                                 |
|                    | large               | Specifies a 32-bit SID (FIPS 140-2 operating mode).     |

**Command Default**

Medium

**Command Modes**

GDOI local server configuration (gdoi-local-server)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(4)M</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

SID lengths of 8, 12, or 16 bits ensure interoperability with the GDOI standard that is described in RFC 6054, *Using Counter Modes with Encapsulating Security Payload (ESP) and Authentication Header (AH) to Protect Group Traffic*.

For most deployments, a group size of medium is recommended; therefore, using this command is optional. Any group size other than medium should be used only for interoperability (for which a small 8-bit, small 12-bit, or small 16-bit size should be used) or if you need to strictly adhere to FIPS 140-2 compliance (in which case, large is required). If you use this command, you should choose the group size based on the anticipated number of key servers (KSs) and group members (GMs).

When you change the group size in a group with cooperative KSs while Suite B (meaning ESP-GCM or ESP-GMAC) is configured and while the Suite B policy has been generated, you must change the group size on all secondary KSs before changing it on the primary KS.

Changing the group size causes the group to reinitialize (so that the new SID length can be used). The following prompt appears:

```
Device(gdoi-local-server)# group size large
% Changing Group Size from MEDIUM to LARGE will cause
% the group to re-initialize...
Are you sure you want to proceed? [yes/no]:
```

If the group size is decreasing and KS SIDs (KSSID(s)) were configured that are not supported in the new group size (for example, 256 was configured with large and you changed it to medium, which has a maximum KSSID value of 127), the following prompt appears:
Device(gdoi-local-server)# group size medium
% Changing the Group Size from LARGE to MEDIUM will cause the group to
% re-initialize & the following configured Key Server SIDs will be lost:
% 256, 510-511
Are you sure you want to proceed? [yes/no]:

If cooperative KSs are configured, changing the group size on a secondary cooperative KS will not change the group size used and will not cause reinitialization until the primary cooperative KS changes the group size and reinitializes the group:

Device(gdoi-local-server)# group size large
% Secondary COOP-KS will change configured Group Size from MEDIUM to LARGE
% but will not use this Group Size until Primary COOP-KS changes as well.

If the group is currently reinitializing, changing the group size is denied:

Device(gdoi-local-server)# group size large
% Group Size Configuration Denied:
% Please wait for group getvpn to finish re-initialization
% and try changing the Group Size again.

If cooperative KSs are configured and the local KS is primary, changing the group size is denied if all of the secondary cooperative KS peers have not already changed their group size to the new group size:

Device(gdoi-local-server)# group size large
% Primary COOP-KS cannot change Group Size from MEDIUM to LARGE while the
% following Secondary COOP-KS peers have not changed to LARGE:
% 10.0.9.1 (Group Size: MEDIUM)

If cooperative KSs are configured and the local KS is primary, changing the group size is denied if all of the secondary cooperative KS peers are not alive (meaning that there is a network split):

Device(gdoi-local-server)# group size large
% Primary COOP-KS cannot change Group Size from MEDIUM to LARGE while
% there is a network split with the following COOP-KS peers:
% 10.0.8.1 (Role: Primary, Status: Dead)

Examples

The following example shows how to configure a SID length of 16-bit small:

Device# crypto gdoi group GETVPN
Device(config-gdoi-group) server local
Device(gdoi-local-server) group size small 16
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crypto gdoi group</code></td>
<td>Creates a GDOI group and enters GDOI group configuration mode.</td>
</tr>
</tbody>
</table>
gtp

To configure the inspection parameters for General Packet Radio Service (GPRS) Tunneling Protocol (GTP), use the `gtp` command in parameter-map profile configuration mode. To disable the inspection parameters for GTP, use the `no` form of this command.

```
gtp {request-queue elements|timeout {gsn|pdp-context|signaling|tunnel} minutes|request-queue seconds|tunnel-limit number}
no gtp {request-queue|timeout {gsn|pdp-context|signaling|tunnel|request-queue}|tunnel-limit}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>request-queue</code></td>
<td>Specifies the queue depth of GTP requests.</td>
</tr>
<tr>
<td><code>elements</code></td>
<td>Number of elements in a queue. The range is from 1 to 4294967295. The default is 200.</td>
</tr>
<tr>
<td><code>timeout</code></td>
<td>Configures the timeout values for GTP.</td>
</tr>
<tr>
<td><code>gsn</code></td>
<td>Specifies the timeout value for the inactive GPRS Support Node (GSN).</td>
</tr>
<tr>
<td><code>minutes</code></td>
<td>Timeout in minutes. The range is from 1 to 35791. The default is 30.</td>
</tr>
<tr>
<td><code>pdp-context</code></td>
<td>Specifies the timeout value for inactive Packet Data Protocol (PDP) -Context.</td>
</tr>
<tr>
<td><code>request-queue</code></td>
<td>Specifies the timeout value for the inactive request queue.</td>
</tr>
<tr>
<td><code>seconds</code></td>
<td>Timeout in seconds. The range is from 1 to 2147483. The default value is 60.</td>
</tr>
<tr>
<td><code>signaling</code></td>
<td>Specifies the timeout value for inactive signaling.</td>
</tr>
<tr>
<td><code>tunnel</code></td>
<td>Specifies the timeout value for an inactive tunnel. The default value is 30 minutes.</td>
</tr>
<tr>
<td><code>tunnel-limit</code></td>
<td>Specifies the number of maximum allowed GTP tunnels.</td>
</tr>
<tr>
<td><code>number</code></td>
<td>Number of allowed GTP tunnels. The range is from 1 to 4294967295. The default is 500.</td>
</tr>
</tbody>
</table>

### Command Default

Inspect parameters are not configured for GTP.

### Command Modes

Parameter-map profile configuration (config-profile)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.4S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `request-queue` keyword specifies the maximum number of GTP requests that will be queued while waiting for a response. When the specified limit is reached and a new request arrives, the request that has been in the queue for the longest time is removed. After the inactivity timer has elapsed, the request will be removed from the queue.

### Examples

The following examples show how to configure the maximum number of GTP requests that will be queued while waiting for a response.

---

Cisco IOS Security Command Reference: Commands D to L
Router(config)# parameter-map type inspect pamap1
Router(config-profile)# gtp request-queue 100

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>parameter-map type inspect</td>
<td>Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect action.</td>
</tr>
</tbody>
</table>
**hardware statistics**

To enable the collection of hardware statistics, use the `hardware statistics` command in IPv6 or IPv4 access-list configuration mode. To disable this feature, use the `no` form of this command.

```
hardware statistics
no hardware statistics
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
This command is disabled by default.

**Command Modes**
IPv6 access-list configuration (config-ipv6-acl)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The hardware statistics command affects only global access-list (ACL) counters.

**Examples**
The following example enables the collection of hardware statistics in an IPv6 configuration:

```
Router(config-ipv6-acl)# hardware statistics
```
hash (ca-trustpoint)

To specify the cryptographic hash algorithm function for the signature that the Cisco IOS client uses to sign its self-signed certificates, use the `hash` command in ca-trustpoint configuration mode. To return to the default cryptographic hash function, use the `no` form of this command.

**Syntax Description**

- `hash {md5|sha1|sha256|sha384|sha512}`
  - `md5` Specifies that Message-Digest algorithm 5 (MD5) hash function is used.
  - `sha1` Specifies that Secure Hash Algorithm (SHA-1) hash function is used as the default hash algorithm for RSA keys.
  - `sha256` Specifies that the SHA-256 hash function is used as the hash algorithm for Elliptic Curve (EC) 256 bit keys.
  - `sha384` Specifies that the SHA-384 hash function is used as the hash algorithm for EC 384 bit keys.
  - `sha512` Specifies that the SHA-512 hash function is used as the hash algorithm for EC 384 bit keys.

**Command Default**

The Cisco IOS client uses the MD5 cryptographic hash function for self-signed certificates by default.

**Command Modes**

Ca-trustpoint configuration (ca-trustpoint)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.4</td>
<td>This command was implemented on the Cisco ASR 1000 series routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Any specified `hash` command algorithm keyword option can be used to over-ride the default setting for the trustpoint. This setting then becomes the default cryptographic hash algorithm function for self-signed certificates by default.
The algorithm does not specify what kind of signature the certificate authority (CA) uses when it issues a certificate to the client.

Examples

The following example configures the trustpoint “MyTP” and sets the cryptographic hash function to SHA-384:

crypto pki trustpoint MyTP
    enrollment url http://MyTP
    ip-address FastEthernet0/0
    revocation-check none
    hash sha384

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hash (cs-server)</td>
<td>Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.</td>
</tr>
</tbody>
</table>
hash (cs-server)

To specify the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the certificate authority (CA), use the hash command in certificate server configuration mode. To return to the default cryptographic hash function, use the no form of this command.

```
hash {md5|sha1|sha256|sha384|sha512}
```

no hash

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Command Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>md5</td>
<td>Specifies that the Message-Digest algorithm 5 (MD5), the default hash function is used.</td>
</tr>
<tr>
<td>sha1</td>
<td>Specifies that the Secure Hash Algorithm (SHA-1) hash function is used.</td>
</tr>
<tr>
<td>sha256</td>
<td>Specifies that the SHA-256 hash function is used.</td>
</tr>
<tr>
<td>sha384</td>
<td>Specifies that the SHA-384 hash function is used.</td>
</tr>
<tr>
<td>sha512</td>
<td>Specifies that the SHA-512 hash function is used.</td>
</tr>
</tbody>
</table>

Command Default:
By default, to sign certificates issued by CA, the Cisco IOS client uses the MD5 cryptographic hash function.

Command Modes:
Certificate server configuration (cs-server)

Command History:

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines:

Note
Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

You must configure the crypto pki server command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

The hash command in cs-server configuration mode sets the hash function for the signature that the Cisco IOS CA uses to sign all of the certificates issued by the server. If the CA is a root CA, it uses the hash function in its own, self-signed certificate.

Examples:
The following example configures a certificate server, MyCS, and sets the cryptographic hash function to SHA-512 for the certificate server:

```
crypto pki server MyCS
database level complete
issuer-name CN=company, L=city, C=country
grant auto trustpoint
```
hash sha512
lifetime crl 168

The following is sample output from the show crypto ca certificates command. This output shows that the CA has been configured and that the hash function SHA-512 has been specified.

CA Certificate
Status: Available
Certificate Serial Number: 01
Certificate Usage: Signature
Issuer:
cn=company
l=city
c=country
Subject:
cn=company
l=city
c=country
Validity Date:
start date: 01:32:35 GMT Aug 3 2006
end date: 01:32:35 GMT Aug 2 2009
Associated Trustpoints: MyTP
Certificate Subject:
Name: MyCS.cisco.com
IP Address: 192.168.10.2
Status: Pending Key
Usage: General Purpose
Certificate Request Fingerprint SHA1: 05080A60 82DE9395 B35607C2 38F3A0C3 50609EF8
Associated Trustpoint: MyTP

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-rollover</td>
<td>Enables the automated CA certificate rollover functionality.</td>
</tr>
<tr>
<td>cdp-url</td>
<td>Specifies a CDP to be used in certificates that are issued by the certificate server.</td>
</tr>
<tr>
<td>crl (cs-server)</td>
<td>Specifies the CRL PKI CS.</td>
</tr>
<tr>
<td>crypto pki server</td>
<td>Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials</td>
</tr>
<tr>
<td>database archive</td>
<td>Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.</td>
</tr>
<tr>
<td>database level</td>
<td>Controls what type of data is stored in the certificate enrollment database.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>database url</td>
<td>Specifies the location where database entries for the CS is stored or published.</td>
</tr>
<tr>
<td>database username</td>
<td>Specifies the requirement of a username or password to be issued when accessing the primary database location.</td>
</tr>
<tr>
<td>default (cs-server)</td>
<td>Resets the value of the CS configuration command to its default.</td>
</tr>
<tr>
<td>grant auto rollover</td>
<td>Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.</td>
</tr>
<tr>
<td>grant auto trustpoint</td>
<td>Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.</td>
</tr>
<tr>
<td>grant none</td>
<td>Specifies all certificate requests to be rejected.</td>
</tr>
<tr>
<td>grant ra-auto</td>
<td>Specifies that all enrollment requests from an RA be granted automatically.</td>
</tr>
<tr>
<td>issuer-name</td>
<td>Specifies the DN as the CA issuer name for the CS.</td>
</tr>
<tr>
<td>lifetime (cs-server)</td>
<td>Specifies the lifetime of the CA or a certificate.</td>
</tr>
<tr>
<td>mode ra</td>
<td>Enters the PKI server into RA certificate server mode.</td>
</tr>
<tr>
<td>mode sub-cs</td>
<td>Enters the PKI server into sub-certificate server mode.</td>
</tr>
<tr>
<td>redundancy (cs-server)</td>
<td>Specifies that the active CS is synchronized to the standby CS.</td>
</tr>
<tr>
<td>serial-number (cs-server)</td>
<td>Specifies whether the router serial number should be included in the certificate request.</td>
</tr>
<tr>
<td>show (cs-server)</td>
<td>Displays the PKI CS configuration.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>shutdown (cs-server)</td>
<td>Allows a CS to be disabled without removing the configuration.</td>
</tr>
</tbody>
</table>
hash (IKE policy)

To specify the hash algorithm within an Internet Key Exchange policy, use the hash command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the hash algorithm to the default secure hash algorithm (SHA-1) hash algorithm, use the no form of this command.

hash {sha|sha256|sha384|md5}
no hash

**Syntax Description**

- **sha**: Specifies SHA-1 (HMAC variant) as the hash algorithm.
- **sha256**: Specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm.
- **sha384**: Specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.
- **md5**: Specifies MD5 (HMAC variant) as the hash algorithm.

**Command Default**

The SHA-1 hash algorithm

**Command Modes**

ISAKMP policy configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(4)T</td>
<td>IPv6 support was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on Cisco ASR 1000 Series Routers.</td>
</tr>
<tr>
<td>15.1(2)T</td>
<td>This command was modified. The sha256 and sha384 keywords were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use this command to specify the hash algorithm to be used in an IKE policy.
The following example configures an IKE policy with the MD5 hash algorithm (all other parameters are set to the defaults):

```
crypto isakmp policy 15
  hash md5
  exit
```
heading

To configure the heading that is displayed above URLs listed on the portal page of a SSL VPN, use the `heading` command in `webvpn URL list configuration` mode. To remove the heading, use the `no` form of this command.

`heading text-string`

`no heading`

**Syntax Description**

| text-string | The URL list heading entered as a text string. The heading must be in quotation marks if it contains spaces. |

**Command Default**

A heading is not configured.

**Command Modes**

Webvpn URL list configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example configures a heading for a URL list:

```plaintext
Router(config)# webvpn context context1
Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading "Quick Links"
Router(config-webvpn-url)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>url-list</code></td>
<td>Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN.</td>
</tr>
</tbody>
</table>
hide-url-bar

To prevent the URL bar from being displayed on the SSL VPN portal page, use the hide-url-bar command in webvpn group policy configuration mode. To display the URL bar on the portal page, use the no form of this command.

hide-url-bar
no  hide-url-bar

Syntax Description
This command has no arguments or keywords.

Command Default
The URL bar is displayed on the SSL VPN portal page.

Command Modes
Webvpn group policy configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
The configuration of this command applies only to clientless mode access.

Examples
The following example hides the URL bar on the SSL VPN portal page:

Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# hide-url-bar
Router(config-webvpn-group)#

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy group</td>
<td>Enters webvpn group policy configuration mode to configure a policy group.</td>
</tr>
<tr>
<td>webvpn context</td>
<td>Enters webvpn context configuration mode to configure the SSL VPN context.</td>
</tr>
</tbody>
</table>
**holdtime**

To configure the hold time for Internet Key Exchange Version 2 (IKEv2) gateways in a Hot Standby Router Protocol (HSRP) cluster, use the `holdtime` command in IKEv2 cluster configuration mode. To restore the default hold time, use the `no` form of this command.

```
holdtime milliseconds
no holdtime
```

### Syntax Description

| milliseconds | Interval, in milliseconds, before a peer is considered dead. The range is from 100 to 120000. The default is 3000. |

### Command Default

The default is 3000 milliseconds if the hold time is not configured.

### Command Modes

IKEv2 cluster configuration (config-ikev2-cluster)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(4)M</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

You must enable the `crypto ikev2 cluster` command before enabling the `holdtime` command.

### Examples

The following example shows how to set the hold time to receive messages from a peer to 100 milliseconds:

```
Device(config)# crypto ikev2 cluster
Device(config-ikev2-cluster)# holdtime 100
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2 cluster</td>
<td>Defines an IKEv2 cluster policy in an HSRP cluster.</td>
</tr>
</tbody>
</table>
**hop-limit**

To verify the advertised hop-count limit, use the `hop-limit` command in RA guard policy configuration mode.

```
hop-limit {maximum|minimum} limit
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>maximum limit</strong></td>
</tr>
<tr>
<td>Verifies that the hop-count limit is lower than that set by the <code>limit</code> argument.</td>
</tr>
<tr>
<td><strong>minimum limit</strong></td>
</tr>
<tr>
<td>Verifies that the hop-count limit is greater than that set by the <code>limit</code> argument.</td>
</tr>
</tbody>
</table>

**Command Default**

No hop-count limit is specified.

**Command Modes**

RA guard policy configuration
(config-ra-guard)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
<tr>
<td>15.0(2)SE</td>
<td>This command was integrated into Cisco IOS Release 15.0(2)SE.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `hop-limit` command enables verification that the advertised hop-count limit is greater than or less than the value set by the `limit` argument. Configuring the `minimum limit` keyword and argument can prevent an attacker from setting a low hop-count limit value on the hosts to block them from generating traffic to remote destinations; that is, beyond their default router. If the advertised hop-count limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Configuring the `maximum limit` keyword and argument enables verification that the advertised hop-count limit is lower than the value set by the `limit` argument. If the advertised hop-count limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

**Examples**

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and sets a minimum hop-count limit of 3:

```
Router(config) # ipv6 nd raguard policy raguard1
Router(config-ra-guard) # hop-limit minimum 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd raguard policy</td>
<td>Defines the RA guard policy name and enters RA guard policy configuration mode.</td>
</tr>
</tbody>
</table>
host (webvpn url rewrite)

To select the name of the host site to be mangled on a Secure Socket Layer virtual private network (SSL VPN) gateway, use the **host** command in `webvpn url rewrite` configuration mode. To deselect a site, use the **no** form of this command.

```
host  host-name
no  host  host-name
```

**Syntax Description**

- **host-name**: Hostname of the site to be mangled.

**Command Default**

A host site is not selected.

**Command Modes**

Webvpn url rewrite (config-webvpn-url-rewrite)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows that the site www.examplecompany.com is to be mangled:

```
Router (config)# webvpn context
Router (config-webvpn-context)# url rewrite
Router (config-webvpn-url-rewrite)# host www.examplecompany.com
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip (webvpn url rewrite)</td>
<td>Configures the IP address of the site to be mangled on an SSL VPN gateway.</td>
</tr>
<tr>
<td>unmatched-action (webvpn url rewrite)</td>
<td>Defines the action when the user request does not match the IP address or host site configuration.</td>
</tr>
</tbody>
</table>
hostname (IKEv2 keyring)

To specify the hostname for the peer in the Internet Key Exchange Version 2 (IKEv2) keyring, use the `hostname` command IKEv2 keyring peer configuration mode. To remove the hostname, use the `no` form of this command.

```
hostname name
no hostname
```

**Syntax Description**

- `name` Name for the peer.

**Command Default**

The hostname is not specified.

**Command Modes**

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When configuring the IKEv2 keyring, use this command to identify the peer using hostname, which is:

- Independent of the IKEv2 identity.
- Available on an IKEv2 initiator only.
- Provided by IPsec to IKEv2 as part of a security association setup request to identify the peer.
- Used to identify the peer only with crypto maps and not with tunnel protection.

**Examples**

The following example shows how to configure the hostname for a peer when configuring an IKEv2 keyring:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description peer1
Router(config-ikev2-keyring-peer)# hostname peer1.example.com
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address (ikev2 keyring)</td>
<td>Specifies the IPv4 address or the range of the peers in IKEv2 key.</td>
</tr>
<tr>
<td>crypto ikev2 keyring</td>
<td>Defines an IKEv2 keyring.</td>
</tr>
<tr>
<td>description (ikev2 keyring)</td>
<td>Describes an IKEv2 peer or a peer group for the IKEv2 keyring.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>identity (ikev2 keyring)</td>
<td>Identifies the peer with IKEv2 types of identity.</td>
</tr>
<tr>
<td>peer</td>
<td>Defines a peer or a peer group for the keyring.</td>
</tr>
<tr>
<td>pre-shared-key (ikev2 keyring)</td>
<td>Defines a preshared key for the IKEv2 peer.</td>
</tr>
</tbody>
</table>
hostname (WebVPN)

To configure the hostname for a SSL VPN gateway, use the hostname command in webvpn gateway configuration mode. To remove the hostname from the SSL VPN gateway configuration, use the no form of this command.

```
hostname name
no hostname
```

**Syntax Description**
- `name` Specifies the hostname.

**Command Default**
The hostname is not configured.

**Command Modes**
Webvpn gateway configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
A hostname is configured for use in the URL and cookie-mangling process. In configurations where traffic is balanced among multiple SSL VPN gateways, the hostname configured with this command maps to the gateway IP address configured on the load-balancing device(s).

**Examples**
The following example configures a hostname for a SSL VPN gateway:

```
Router(config)# webvpn gateway GW_1
Router(config-webvpn-gateway)# hostname VPN_Server
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>webvpn gateway</td>
<td>Defines a SSL VPN gateway and enters webvpn gateway configuration mode.</td>
</tr>
</tbody>
</table>
http proxy-server

To direct Secure Socket Layer virtual private network (SSL VPN) user requests through a backend HTTP proxy server, use the `http proxy-server` command in webvpn policy group configuration mode. To redirect user requests to internal servers, use the `no` form of this command.

```
http proxy-server {dns-name ip-address} port port-number
no http proxy-server
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dns-name</code></td>
<td>Domain Name System (DNS) to be directed to the HTTP proxy server.</td>
</tr>
<tr>
<td><code>ip-address</code></td>
<td>IP address to be directed to the HTTP proxy server.</td>
</tr>
<tr>
<td><code>port port-number</code></td>
<td>Port number of the backend HTTP proxy server.</td>
</tr>
</tbody>
</table>

**Command Default**

User requests are routed directly to internal servers.

**Command Modes**

Webvpn policy group configuration (config-webvpn-group)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows that requests from IP address 10.1.1.1 are to be routed to the proxy server (port number 2034):

```
Router (config)# webvpn context e1
Router (config-webvpn-context)# policy group g1
Router (config-webvpn-group)# http proxy-server 10.1.1.1 port 2034
Router (config-webvpn-group)# exit
Router (config-webvpn-context)# default-group-policy g1
```
http-redirect

To configure HTTP traffic to be carried over secure HTTP (HTTPS), use the `http-redirect` command in `webvpn gateway` configuration mode. To remove the HTTPS configuration from the SSL VPN gateway, use the `no` form of this command.

```
http-redirect [port number]
no http-redirect
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>port number</code></td>
<td>(Optional) Specifies a port number. The value for this argument is a number from 1 to 65535.</td>
</tr>
</tbody>
</table>

**Command Default**

The following default value is used if this command is configured without entering the `port` keyword:

```
port number : 80
```

**Command Modes**

Webvpn gateway configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When this command is enabled, the HTTP port is opened and the SSL VPN gateway listens for HTTP connections. HTTP connections are redirected to use HTTPS. Entering the `port` keyword and `number` argument configures the gateway to listen for HTTP traffic on the specified port. Entering the `no` form, disables HTTP traffic redirection. HTTP traffic is handled by the HTTP server if one is running.

**Examples**

The following example, starting in global configuration mode, redirects HTTP traffic (on TCP port 80) over to HTTPS (on TCP port 443):

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# http-redirect
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>webvpn gateway</td>
<td>Defines a SSL VPN gateway and enters webvpn gateway configuration mode.</td>
</tr>
</tbody>
</table>
**hw-module slot subslot only**

**Note**
This command is deleted effective with Cisco IOS Release 12.2SXI.

To change the mode of the Cisco 7600 SSC-400 card to allocate full buffers to the specified subslot, use the **hw-module slot subslot only** command in global configuration mode. If this command is not used, the total amount of buffers available is divided between the two subslots on the Cisco 7600 SSC-400.

**Note**
This command automatically generates a reset on the Cisco 7600 SSC-400. See Usage Guidelines below for details.

```
hw-module slot slot subslot subslot only
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>slot</code></td>
<td>Chassis slot number where the Cisco 7600 SSC-400 is located. Refer to the appropriate hardware manual for slot information. For SIPs and SSCs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.</td>
</tr>
<tr>
<td><code>subslot</code></td>
<td>Secondary slot number on the SSC where the IPSec VPN SPA is installed.</td>
</tr>
</tbody>
</table>

**Command Default**
No default behavior or values.

**Command Modes**
Global configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(18)SXF2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>12.2SXI</td>
<td>This command was deleted.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Follow these guidelines and restrictions when configuring a Cisco 7600 SSC-400 and IPSec VPN SPAs using the **hw-module slot subslot only** command:

- This command is useful when supporting IP multicast over GRE on the IPSec VPN SPA.
- When this command is executed, it automatically takes a reset action on the Cisco 7600 SSC-400 and issues the following prompt to the console:

  Module n will be reset? Confirm [n]:

---

**F through H**

---

**Cisco IOS Security Command Reference: Commands D to L**

---

346
The prompt will default to “N” (no). You must type “Y” (yes) to activate the reset action.

- When in this mode, if you manually plug in a second SPA, or if you attempt to reset the SPA (by entering a `no hw-module subslot shutdown` command, for example), a message is displayed on the router console which refers you to the customer documentation.

**Examples**

The following example allocates full buffers to the SPA that is installed in subslot 0 of the SIP located in slot 1 of the router and takes a reset action of the Cisco 7600 SSC-400.

```
Router(config)# hw-module slot 4 subslot 1 only
Module 4 will be reset? Confirm [no]: y
```

Note that the prompt will default to “N” (no). You must type “Y” (yes) to activate the reset action.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip multicast-routing</code></td>
<td>Enables IP multicast routing.</td>
</tr>
<tr>
<td><code>ip pim</code></td>
<td>Enables Protocol Independent Multicast (PIM) on an interface.</td>
</tr>
</tbody>
</table>
icmp idle-timeout through ip http ezvpn

- icmp idle-timeout, on page 351
- ida-client server url, on page 352
- identifier, on page 353
- identity local, on page 355
- identity (IKEv2 keyring), on page 357
- identity (IKEv2 profile), on page 359
- identity address ipv4, on page 361
- identity number, on page 362
- identity policy, on page 363
- identity profile, on page 364
- identity profile eapoudp, on page 366
- idle-timeout (WebVPN), on page 367
- if-state nhrp, on page 368
- import, on page 369
- include-local-lan, on page 370
- incoming, on page 372
- initial-contact force, on page 374
- initiate mode, on page 375
- inservice (WebVPN), on page 376
- inspect, on page 377
- inspect (config-profile), on page 379
- integrity, on page 380
- interface (RITE), on page 382
- interface (VASI), on page 384
- interface virtual-template, on page 386
- ip (webvpn url rewrite), on page 389
- ip access-group, on page 390
- ip access-list, on page 392
- ip access-list hardware permit fragments, on page 395
- ip access-list logging interval, on page 397
- ip access-list log-update, on page 398
- ip access-list resequence, on page 400
- ip access-list logging hash-generation, on page 402
icmp idle-timeout through ip http ezvpn
icmp idle-timeout

To configure the timeout for Internet Control Message Protocol (ICMP) sessions, use the `icmp idle-timeout` command in parameter-map type inspect configuration mode. To disable the timeout, use the `no` form of this command.

```
icmp idle-timeout  seconds  [{ageout-time  seconds}]  
no  icmp idle-timeout
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>ICMP timeout, in seconds. The default is 10. Valid values are from 1 to 2147483.</td>
</tr>
<tr>
<td><code>ageout-time seconds</code></td>
<td>(Optional) Specifies the aggressive aging time for ICMP packets. Valid values are from 1 to 2147483.</td>
</tr>
</tbody>
</table>

### Command Default

The timeout default is 10 seconds.

### Command Modes

Parameter-map type inspect configuration (config-profile)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.4S</td>
<td>This command was modified. The <code>ageout-time seconds</code> keyword and argument pair was added.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

When you configure an inspect parameter map, you can enter the `icmp idle-timeout` command after you enter the `parameter-map type inspect` command. For detailed information about creating a parameter map, see the `parameter-map type inspect` command.

### Examples

The following example shows how to specify the ICMP session timeout as 90 seconds:

```
parameter-map type inspect insp-params
  icmp idle-timeout 90
```

The following example shows how to specify the ICMP session aging out time as 50 seconds:

```
parameter-map type inspect insp-params
  icmp idle-timeout 90 ageout 50
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>parameter-map type inspect</code></td>
<td>Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the <code>inspect</code> action.</td>
</tr>
</tbody>
</table>
**ida-client server url**

To specify the IDA-server url that the IOS IDA client communicates with to download files from the Cisco.com server, use the `ida-client server url` command in global configuration mode. To revert back to the default value, use the `no` form of this command.

```
ida-client server url
no ida-client server url
```

**Syntax Description**

- `url` Specifies the IDA-server url. You must enter the following URL:
  
  https://www.cisco.com/cgi-bin/front.x/ida/locator/locator.pl

**Command Default**

The default IDA-server URL is: https://www.cisco.com/cgi-bin/ida/locator/locator.pl

**Note**

Do not use the default URL in your configuration.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(1)T</td>
<td>This command was modified to include a default IDA-server URL.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Enter the following URL for the `ida-client server url` command to specify the IDA-server URL:

```
Router(config)# ida-client server url
https://www.cisco.com/cgi-bin/front.x/ida/locator/locator.pl
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ips signature update cisco</td>
<td>Initiates a one-time download of an IPS signatures from Cisco.com.</td>
</tr>
<tr>
<td>upgrade automatic abortversion</td>
<td>Cancels the scheduled reloading of the router with a new Cisco IOS software image.</td>
</tr>
<tr>
<td>upgrade automatic getversion</td>
<td>Downloads a Cisco IOS software image directly from <a href="http://www.cisco.com">www.cisco.com</a> or from a non-Cisco server.</td>
</tr>
<tr>
<td>upgrade automatic runversion</td>
<td>Reloads the router with a new Cisco IOS software image.</td>
</tr>
</tbody>
</table>
**identifier**

To assign a GDOI key server (KS) sender identifier (KSSID) to a KS, use the `identifier` command in GDOI local server configuration mode. To disable a GDOI KS identifier, use the `no` form of this command.

```
identifier
no identifier
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No KSSID are assigned to the KS.

**Command Modes**

GDOI local server (gdoi-local-server)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(4)M</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command enters GDOI local server ID configuration mode, which contains several subcommands for setting the KSSID:

- `default` (sets the values to their defaults)
- `exit` (saves the KSSID configuration and exits)
- `no` (negates a command)
- `range lowest-kssid - highest-kssid` (assigns a range of KSSIDs (unique in the entire group))
- `value kssid` (assigns a KSSID (unique in the entire group))

Each KS must be assigned at least one KSSID when using GCM or GMAC. The following table shows that the range of KSSIDs available depends on the group size configuration.

**Table 6: Ranges of Available KSSIDs Based on Group Size**

<table>
<thead>
<tr>
<th>Configured Group Size</th>
<th>Range of Available KSSIDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small (8 bits)</td>
<td>0 to 1</td>
</tr>
<tr>
<td>Small (12 bits)</td>
<td>0 to 3</td>
</tr>
<tr>
<td>Small (16 bits)</td>
<td>0 to 15</td>
</tr>
<tr>
<td>Medium</td>
<td>0 to 127</td>
</tr>
<tr>
<td>Large</td>
<td>0 to 511</td>
</tr>
</tbody>
</table>

Each KS must be assigned at least one KSSID when using GCM or GMAC. You can configure a single KSSID, a range of KSSIDs, or both. KSSID values are not assigned to (and usable by) the KS until you exit GDOI local server ID configuration mode.
If you remove KSSID that were previously used since the last reinitialization, the group reinitializes (without traffic loss), and KSSID that were used will be reset. You are prompted to confirm this before configuring the KSSID set. For example:

```
Device(gdoi-local-server-id)# no value 1
Device(gdoi-local-server-id)# exit

% The following Key Server SIDs being removed were previously used:
% 1
% Removing these KS SIDs will re-initialize the group (without traffic loss).
Are you sure you want to proceed? [yes/no]:
```

If the group is currently reinitializing, removal of KSSIDs that have been previously used since the last reinitialization is denied. For example:

```
Device(gdoi-local-server-id)# no value 0
Device(gdoi-local-server-id)# exit

% Key Server SID Configuration Denied:
% Please wait for group getvpn to finish re-initialization
% and try removing used KS SIDs again.
```

If cooperative KSs are configured and the secondary cooperative KS has configured a new group size, but the primary cooperative KS has not changed the group size so that the secondary cooperative KS is using the new group size, entering the `identifier` command on the secondary cooperative KS is denied. For example:

```
Device(gdoi-local-server-id)# identifier

% Key Server SID Configuration Denied:
% Need Primary COOP-KS to change Group Size from MEDIUM to LARGE, OR
% Need Local KS to change Group Size from LARGE to MEDIUM.
```

If cooperative KSs are is configured, the KSSID configured on each KS must be unique. No two KSs can have the same KSSID value configured, and if a cooperative KS tries to configure a KSSID that another cooperative KS peer has already assigned to itself, the configuration is denied. For example:

```
Device(gdoi-local-server-id)# range 0-127
Device(gdoi-local-server-id)# end

% Key Server SID Configuration Denied:
% The following Key Server SIDs being added overlap:
% 0-9, 20-29 (COOP-KS Peer: 10.0.7.1)
% 10-19, 30-39 (COOP-KS Peer: 10.0.9.1)
```

**Examples**

The following example shows how to configure a single KSSID and a range of KSSIDs. In this example, the `value` command allots the pool of SIDs to the KS that begin with KSSID value 0 (meaning that it is allotted the pool of SID values beginning with 0x0 and ending with 0x1FFFF):

```
Device# configure terminal
Device(config)# crypto gdoi group GETVPN
Device(config-gdoi-group)# server local
Device(gdoi-local-server-id)# identifier
Device(gdoi-local-server-id)# range 10 - 20
Device(gdoi-local-server-id)# value 0
Device(gdoi-local-server-id)# end
```
**identity local**

To specify the local Internet Key Exchange Version 2 (IKEv2) identity type, use the `identity local` command in IKEv2 profile configuration mode. To remove the identity, use the `no` form of this command.

```
identity local {address {ipv4-address | ipv6-address} | dn dn-string | fqdn fqdn-string | email email-string | key-id key-id-string} | opaque-string}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>address</code></td>
<td>Uses the IPv4 or IPv6 address as the local identity.</td>
</tr>
<tr>
<td><code>dn</code></td>
<td>Uses the distinguished name as the local identity.</td>
</tr>
<tr>
<td><code>fqdn</code></td>
<td>Uses the Fully Qualified Domain Name (FQDN) as the local identity.</td>
</tr>
<tr>
<td><code>email</code></td>
<td>Uses the e-mail ID as the local identity.</td>
</tr>
<tr>
<td><code>key-id</code></td>
<td>Uses the proprietary type opaque string as the local identity.</td>
</tr>
</tbody>
</table>

### Command Default

If the local authentication method is a preshared key, the default local identity is the IP address (IPv4 or IPv6).

If the local authentication method is an RSA signature, the default local identity is Distinguished Name.

### Command Modes

IKEv2 profile configuration (config-ikev2-profile)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(4)M</td>
<td>This command was modified. Support was added for IPv6 addresses.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to specify the local IKEv2 identity type as an IPv4 address or IPv6 address, a DN, an FQDN, an e-mail ID, or a key ID. The local IKEv2 identity is used by the local IKEv2 peer to identify itself to the remote IKEv2 peers in the AUTH exchange using the IDi field.

#### Note

You can configure one local IKEv2 identity type for a profile.

### Examples

The following example shows how to specify an IPv4 address as the local IKEv2 identity:

```
Router(config)# crypto ikev2 profile profile1
```
Router(config-ikev2-profile)# identity local address 10.0.0.1
The following example shows how to specify an IPv6 address as the local IKEv2 identity:
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# identity local address 2001:DB8:0::1

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>crypto ikev2 profile</td>
<td>Defines an IKEv2 profile,</td>
</tr>
</tbody>
</table>
identity (IKEv2 keyring)

To identify a peer with Internet Key Exchange Version 2 (IKEv2) types of identity, use the `identity` command in IKEv2 keyring peer configuration mode. To remove the identity, use the `no` form of this command.

```
identity {address {ipv4-address | ipv6-address} | fqdn domain domain-name | email domain domain-name | key-id domain-name} no identity {address {ipv4-address | ipv6-address} | fqdn domain domain-name | email domain domain-name | key-id key-id}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Uses the IPv4 or IPv6 address to identify the peer.</td>
</tr>
<tr>
<td>fqdn domain</td>
<td>Uses the Fully Qualified Domain Name (FQDN) to identify the peer.</td>
</tr>
<tr>
<td>email domain</td>
<td>Uses the e-mail ID to identify the peer.</td>
</tr>
<tr>
<td>key-id</td>
<td>Uses the proprietary types to identify the peer.</td>
</tr>
</tbody>
</table>

**Command Default**

Identity types are not specified to a peer.

**Command Modes**

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(4)M</td>
<td>This command was modified. Support was added for IPv6 addresses.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
<tr>
<td>15.3(3)M</td>
<td>This command was modified. The <code>domain domain-name</code> keyword-argument pair was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to identify the peer using IKEv2 types of identity such as an IPv4 or IPv6 address, an FQDN, an e-mail ID, or a key ID. Key lookup using IKEv2 identity is available only on the responder because the peer ID is not available on the initiator at the time of starting the IKEv2 session, and the initiator looks up keys during session startup.

**Examples**

The following example shows how to associate an FQDN to the peer:

```
Router(config)# crypto ikev2 keyring keyring-4
Router(config-keyring)# peer abc
Router(config-keyring-peer)# description abc domain
Router(config-keyring-peer)# identity fqdn example.com
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address (ikev2 keyring)</td>
<td>Specifies the IPv4 or IPv6 address or the range of the peers in an IKEv2 keyring.</td>
</tr>
<tr>
<td>crypto ikev2 keyring</td>
<td>Defines an IKEv2 keyring.</td>
</tr>
<tr>
<td>description (ikev2 keying)</td>
<td>Describes an IKEv2 peer or a peer group for the IKEv2 keyring.</td>
</tr>
<tr>
<td>hostname (ikev2 keyring)</td>
<td>Specifies the hostname for the peer in the IKEv2 keyring.</td>
</tr>
<tr>
<td>peer</td>
<td>Defines a peer or a peer group for the keyring.</td>
</tr>
<tr>
<td>pre-shared-key (ikev2 keyring)</td>
<td>Defines a preshared key for the IKEv2 peer.</td>
</tr>
</tbody>
</table>
identity (IKEv2 profile)

To specify how the local or remote router identifies itself to the peer and communicates with the peer in the Rivest, Shamir and Adleman (RSA) authentication exchange, use the identity command in IKEv2 profile configuration mode. To delete a match, use the no form of this command.

```plaintext
identity [{local {dn [trustpoint trustpoint-name [serial certificate-serial]]}address ip-address|fqdn string|email string}|remote {dn [ou=..., o=...]}address ip-address|fqdn string|email string}]
no identity [{local {dn [trustpoint trustpoint-name [serial certificate-serial]]}address ip-address|fqdn string|email string}|remote {dn [ou=..., o=...]}address ip-address|fqdn string|email string}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>local</th>
<th>Specifies the local router.</th>
</tr>
</thead>
<tbody>
<tr>
<td>dn</td>
<td>Specifies the distinguished name (DN) of the local or remote router.</td>
</tr>
<tr>
<td>trustpoint trustpoint-name</td>
<td>(Optional) Specifies the PKI trustpoint name to use with the RSA signature authentication method on the local router.</td>
</tr>
<tr>
<td>serial certificate-serial</td>
<td>(Optional) Specifies the serial number of the trustpoint certificate on the local router.</td>
</tr>
<tr>
<td>address ip-address</td>
<td>Specifies the IP address of the remote or local router.</td>
</tr>
<tr>
<td>fqdn fqdn-name</td>
<td>Specifies the Fully Qualified Domain Name (FQDN) of the remote or local router.</td>
</tr>
<tr>
<td>email e-mail ID</td>
<td>Specifies the email ID of the remote or local router.</td>
</tr>
<tr>
<td>ou= ..., o=...</td>
<td>(Optional) Specifies the organizational Unit (OU) field of the subject name in the trustpoint certificate.</td>
</tr>
</tbody>
</table>

### Command Default

An identity profile is not specified for a local or remote router regarding the RSA authentication exchange.

### Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)#

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(2)T</td>
<td>This command was modified. The local, dn, trustpoint, serial, and ou= keywords were added to this command.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `identity` command to identify the local or remote router by its DN, trustpoint, IP address, FQDN, or email address.

### Examples

The following example shows how an IKEv2 profile is matched on the remote identity. The following profile caters to peers that identify using `fqdn example.com` and authenticate with `rsa-signature` using `trustpoint-remote`. The local node authenticates with `pre-share` using `keyring-1`. 
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# match identity remote fqdn example.com
Router(config-ikev2-profile)# identity local email router2@example.com
Router(config-ikev2-profile)# authentication local pre-share
Router(config-ikev2-profile)# authentication remote rsa-sig
Router(config-ikev2-profile)# keyring keyring-1
Router(config-ikev2-profile)# pki trustpoint trustpoint-remote verify
Router(config-ikev2-profile)# lifetime 300
Router(config-ikev2-profile)# dpd 5 10 on-demand
Router(config-ikev2-profile)# virtual-template 1

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2 profile</td>
<td>Defines an IKEv2 profile.</td>
</tr>
<tr>
<td>match (IKEv2 profile)</td>
<td>Matches a profile on front-door VPN routing and forwarding (FVRF) or local parameters such as IP address or peer identity or peer certificate.</td>
</tr>
<tr>
<td>authentication (IKEv2 profile)</td>
<td>Specifies the local and remote authentication methods in an Internet Key Exchange Version 2 (IKEv2) profile.</td>
</tr>
<tr>
<td>keyring (IKEv2 profile)</td>
<td>Specifies a locally defined or accounting, authentication and authorization (AAA) based keyring.</td>
</tr>
<tr>
<td>pki trustpoint</td>
<td>Specifies the router to use the PKI trustpoints in the RSA signature authentication.</td>
</tr>
</tbody>
</table>
**identity address ipv4**

To identify a Group Domain of Interpretation (GDOI) group address, use the `identity address ipv4` command in GDOI group configuration mode. To remove the group address, use the `no` form of this command.

```
identity address ipv4 address
no identity address ipv4 address
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>address</code></td>
<td>IP address of the group.</td>
</tr>
</tbody>
</table>

**Command Default**

A group address is not identified.

**Command Modes**

GDOI group configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command or the `identity number` command is required for a GDOI configuration.

**Examples**

The following example shows that the identity address is 10.2.2.2:

```
identity address ipv4 10.2.2.2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto gdoi group</td>
<td>Identifies a GDOI group.</td>
</tr>
<tr>
<td><strong>identity number</strong></td>
<td>Identifies a GDOI group number.</td>
</tr>
</tbody>
</table>
identity number

To identify a Group Domain of Interpretation (GDOI) group number, use the `identity number` command in GDOI group configuration mode. To remove the group number, use the `no` form of this command.

```
identity number number
no identity number number
```

Syntax Description

| number | Number of the group. |

Command Default

A GDOI group number is not identified.

Command Modes

GDOI group configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command or the `identity address ipv4` command is required for a GDOI configuration.

Examples

The following example shows the group number is 3333:

```
identity number 3333
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto gdoi group</td>
<td>Identifies a GDOI group and enters GDOI group configuration mode.</td>
</tr>
<tr>
<td>identity address ipv4</td>
<td>Identifies a GDOI group address.</td>
</tr>
</tbody>
</table>
To create an identity policy and to enter identity policy configuration mode, use the `identity policy` command in global configuration mode. To remove the policy, use the `no` form of this command.

```
identity policy policy-name [{access-group group-name | description line-of-description | redirect url}]
no identity policy policy-name [{access-group group-name | description line-of-description | redirect url}]
```

### Syntax Description
- **policy-name**: Name of the policy.
- **access-group group-name**: (Optional) Access list to be applied.
- **description line-of-description**: (Optional) Description of the policy.
- **redirect url**: (Optional) Redirects clients to a particular URL.

### Command Default
An identity policy is not created.

### Command Modes
Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>15.2(1)E</td>
<td>This command was modified. The template keyword was removed.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
An identity policy has to be associated with an identity profile.

### Examples
The following example shows that an access policy named "policyname2" is being created. The access-group attribute is set to "allow-access". The redirect URL is set to "http://remediate-url.com". This access policy will be associated with a statically authorized device in the identity profile.

```
Device (config)# identity policy policyname2
Device (config-identity-policy)# access-group allow-access
Device (config-identity-policy)# redirect url http://remediate-url.com
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>identity profile</td>
<td>Creates an identity profile.</td>
</tr>
</tbody>
</table>
identity profile

To create an identity profile and to enter identity profile configuration mode, use the `identity profile` command in global configuration mode. To disable an identity profile, use the `no` form of this command.

```
identity profile {default|dot1x|eapoudp|auth-proxy}
no identity profile {default|dot1x|eapoudp|auth-proxy}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>default</th>
<th>Service type is default.</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x</td>
<td>Service type for 802.1X.</td>
<td></td>
</tr>
<tr>
<td>eapoudp</td>
<td>Service type for Extensible Authentication Protocol over UDP (EAPoUDP).</td>
<td></td>
</tr>
<tr>
<td>auth-proxy</td>
<td>Service type for authentication proxy.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

An identity profile is not created.

**Command Modes**

Global configuration (config)

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.3(2)XA</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.3(4)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(4)T.</td>
</tr>
<tr>
<td></td>
<td>12.3(8)T</td>
<td>The <code>eapoudp</code> keyword was added.</td>
</tr>
<tr>
<td></td>
<td>12.4(6)T</td>
<td>The <code>dot1x</code> keyword was removed.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td></td>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `identity profile` command and `default` keyword allow you to configure static MAC addresses of a client computer that does not support 802.1X and to authorize or unauthorize them statically. After you have issued the `identity profile` command and `default` keyword and the router is in identity profile configuration mode, you can specify the configuration of a template that can be used to create the virtual access interface to which unauthenticated supplicants (client computers) will be mapped.

The `identity profile` command and the `dot1x` keyword are used by the supplicant and authenticator. Using the `dot1x` keyword, you can set the username, password, or other identity-related information for an 802.1X authentication.

Using the `identity profile` command and the `eapoudp` keyword, you can statically authenticate or unauthenticate a device either on the basis of the device IP address or MAC address or on the type, and the corresponding network access policy can be specified using the `identity policy` command.
Examples

The following example shows that an identity profile and its description have been specified:

```
Router (config)# identity profile default
Router (config-identity-prof)# description description_entered_here
```

The following example shows that an EAPoUDP identity profile has been created:

```
Router (config)# identity policy eapoudp
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug dot1x</code></td>
<td>Displays 802.1X debugging information.</td>
</tr>
<tr>
<td><code>description</code></td>
<td>Specifies a description for an 802.1X profile.</td>
</tr>
<tr>
<td><code>device</code></td>
<td>Statically authorizes or rejects individual devices.</td>
</tr>
<tr>
<td><code>dot1x initialize</code></td>
<td>Initializes 802.1X state machines on all 802.1X-enabled interfaces.</td>
</tr>
<tr>
<td><code>dot1x max-req</code></td>
<td>Sets the maximum number of times that a router can send an EAP request/identity frame to a client PC.</td>
</tr>
<tr>
<td><code>dot1x max-start</code></td>
<td>Sets the maximum number of times the authenticator sends an EAP request/identity frame (assuming that no response is received) to the client.</td>
</tr>
<tr>
<td><code>dot1x pae</code></td>
<td>Sets the PAE type during 802.1X authentication.</td>
</tr>
<tr>
<td><code>dot1x port-control</code></td>
<td>Enables manual control of the authorization state of a controlled port.</td>
</tr>
<tr>
<td><code>dot1x re-authenticate</code></td>
<td>Manually initiates a reauthentication of the specified 802.1X-enabled ports.</td>
</tr>
<tr>
<td><code>dot1x re-authentication</code></td>
<td>Globally enables periodic reauthentication of the client PCs on the 802.1X interface.</td>
</tr>
<tr>
<td><code>dot1x system-auth-control</code></td>
<td>Enables 802.1X SystemAuthControl (port-based authentication).</td>
</tr>
<tr>
<td><code>dot1x timeout</code></td>
<td>Sets retry timeouts.</td>
</tr>
<tr>
<td><code>identity policy</code></td>
<td>Creates an identity policy.</td>
</tr>
<tr>
<td><code>show dot1x</code></td>
<td>Displays details for an identity profile.</td>
</tr>
<tr>
<td><code>template (identity profile)</code></td>
<td>Specifies a virtual template from which commands may be cloned.</td>
</tr>
</tbody>
</table>
identity profile eapoudp

To create an identity profile and to enter Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) profile configuration mode, use the identity profile eapoudp command in global configuration mode. To remove the policy, use the no form of this command.

```
identity profile eapoudp
no identity profile eapoudp
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
No EAPoUDP identity profile exists.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SX1</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SX1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Using this command, you can statically authenticate or unauthenticate a device either on the basis of the device IP address or MAC address or on the type, and the corresponding network access policy can be specified using the identity policy command.

**Examples**
The following example shows that an EAPoUDP identity profile has been created:

```
Router (config)# identity profile eapoudp
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>identity policy</td>
<td>Creates an identity policy.</td>
</tr>
</tbody>
</table>
idle-timeout (WebVPN)

Note
Effective with Cisco IOS Release 12.4(6)T, the **idle-timeout (WebVPN)** command is not available in Cisco IOS software.

To set the default idle timeout for a Secure Sockets Layer Virtual Private Network (SSLVPN) if no idle timeout has been defined or if the idle timeout is zero (0), use the **idle-timeout** command in Web VPN configuration mode. To revert to the default value, use the **no** form of this command.

 idle-timeout [{never;seconds}]
no idle-timeout [{never;seconds}]

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>never</strong></td>
<td>(Optional) The idle timeout function is disabled.</td>
</tr>
<tr>
<td><strong>seconds</strong></td>
<td>(Optional) Idle timeout in seconds. The values are from 180 seconds (3 minutes) to 86400 seconds (24 hours).</td>
</tr>
</tbody>
</table>

**Command Default**
If command is not configured, the default idle timeout is 1800 seconds (30 minutes).

**Command Modes**
Web VPN configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(6)T</td>
<td>This command was removed.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Configuring this command prevents stale sessions.

**Examples**
The following example shows that the idle timeout has been set for 1200 seconds:

```
Router (config)#
webvpn
Router (config-webvpn)# idle-timeout 1200
```

The following example shows that the idle timeout function is disabled:

```
Router (config)#
webvpn
Router (config-webvpn)# idle-timeout never
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>webvpn</td>
<td>Enters Web VPN configuration mode.</td>
</tr>
</tbody>
</table>
if-state nhrp

To enable the Next Hop Resolution Protocol (NHRP) to control the state of the tunnel interface, use the **if-state nhrp** command in interface configuration mode. To disable NHRP control of the tunnel interface state, use the **no** form of this command.

```
if-state nhrp
no if-state nhrp
```

### Syntax Description

This command has no arguments or keywords.

### Command Default

NHRP tunnel interface state control is disabled.

### Command Modes

Interface configuration (config-if)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If the system detects that one or more of the Next Hop Servers (NHSs) configured on the interface is up, then the tunnel interface state is also declared as ‘up’. If all NHSs configured on the interface are down, then the tunnel interface state is also declared as ‘down’.

The system does not consider NHSs configured with ‘no-reply’ when determining the interface state.

### Examples

The following example shows how to enable NHRP control of the tunnel interface state:

```
Router(config)# interface tunnel 1
Router(config-if)# if-state nhrp
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip interface</td>
<td>Displays the usability status of interfaces configured for IP.</td>
</tr>
<tr>
<td>show ip nhrp nhs</td>
<td>Displays NHRP NHS information.</td>
</tr>
</tbody>
</table>
**import**

To import a user-defined URL list into a webvpn context, use the `import` command in the webvpn URL list configuration mode. To disable the URL list, use the `no` form of this command.

```
import  device : file
no import device : file
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>device : file</code></td>
<td><code>device : file</code> -- Storage device on the system and the file name. The file name should include the directory location.</td>
</tr>
</tbody>
</table>

### Command Default

A user-defined URL list is not imported.

### Command Modes

Webvpn URL list configuration (config-webvpn-url)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(22)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If this command is used under the `url-list` command, the `url-text` command is not allowed. The `import` command and the `url-list` commands are mutually exclusive when used for a particular URL list. (If you use them together, you will receive this message: "Please remove the imported url-list.")

Also, if a URL list is configured using the `url-text` command, the `import` command is not allowed. (If you use them together, you will receive this message: "Please remove all the URLs before importing a file.")

### Examples

The following example shows that the URL list file "test-url.xml" is being imported from flash:

```
Router (config)# webvpn context
Router (config-webvpn-context)# url-list test
Router (config-webvpn-url)# import flash:test-url.xml
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>webvpn create template</code></td>
<td>Creates templates for multilanguage support for messages in an SSL VPN.</td>
</tr>
</tbody>
</table>
include-local-lan

To configure the Include-Local-LAN attribute to allow a nonsplit-tunneling connection to access the local subnetwork at the same time as the client, use the include-local-lan command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode or Internet Key Exchange Version 2 (IKEv2) authorization policy configuration mode. To disable the attribute that allows the nonsplit-tunneling connection, use the no form of this command.

include-local-lan
no include-local-lan

Syntax Description
This command has no arguments or keywords.

Command Default
A nonsplit-tunneling connection is not able to access the local subnet at the same time as the client.

Command Modes
ISAKMP group configuration (config-isakmp-group)
IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

Usage Guidelines
If split tunneling is not in use (that is, the SPLIT_INCLUDE attribute was not negotiated), you lose not only Internet access, but also access to resources on the local subnetworks. The Include-Local-LAN attribute allows the server to push the attribute to the client, which allows for a nonsplit-tunneling connection to access the local subnetwork at the same time as the client (that is, the connection is to the subnetwork to which the client is directly attached).

The Include-Local-LAN attribute is configured on a Cisco IOS router or in the RADIUS profile.

To configure the Include-Local-LAN attribute, use the include-local-lan command.

An example of an attribute-value (AV) pair for the Include-Local-LAN attribute is as follows:

ipsec:include-local-lan=1

You must enable the crypto isakmp client configuration group or crypto ikev2 authorization policy command, which specifies group policy information that has to be defined or changed, before enabling the include-local-lan command.

Note
The Include-Local-LAN attribute can be applied only by a RADIUS user.

- The attribute can be applied on a per-user basis after the user has been authenticated.
• The attribute can override any similar group attributes.
• User-based attributes are available only if RADIUS is used as the database.

## Examples

The following example shows that the Include-Local-LAN has been configured:

```
crypto isakmp client configuration group cisco
  include-local-lan
```

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>acl</code></td>
<td>Configures split tunneling.</td>
</tr>
<tr>
<td><code>crypto ikev2 authorization policy</code></td>
<td>Specifies an IKEv2 authorization policy.</td>
</tr>
<tr>
<td><code>crypto isakmp client configuration group</code></td>
<td>Specifies the DNS domain to which a group belongs.</td>
</tr>
</tbody>
</table>
incoming

To configure filtering for incoming IP traffic, use the incoming command in router IP traffic export (RITE) configuration mode. To disable filtering for incoming traffic, use the no form of this command.

incoming {access-list [standard|extended|named] | sample one-in-every packet-number}
no incoming {access-list [standard|extended|named] | sample one-in-every packet-number}

Syntax Description
- **access-list**: standard | extended | named
- **sample one-in-every packet-number**

| Command Default | If this command is not enabled, all incoming IP traffic will be filtered via sampling. |
| Command Modes | RITE configuration |
| Command History |

```
Release     Modification
12.3(4)T     This command was introduced.
12.2(25)S    This command was integrated into Cisco IOS Release 12.2(25)S.
```

Usage Guidelines
When configuring a network device for exporting IP traffic, you can issue the incoming command to filter unwanted traffic via the following methods:

- ACLs, which accept or deny an IP packet for export
- Sampling, which allows you to export one in every few packets in which you are interested. Use this option when it is not necessary to export all incoming traffic. Also, sampling is useful when a monitored ingress interface can send traffic faster than the egress interface can transmit it.

Examples
The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8a9b.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the ACL “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8a9b.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
```
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip traffic-export profile</td>
<td>Creates or edits an IP traffic export profile and enables the profile on an ingress interface.</td>
</tr>
<tr>
<td></td>
<td>outgoing</td>
<td>Configures filtering for outgoing export traffic.</td>
</tr>
</tbody>
</table>
initial-contact force

To process an initial contact notification in Internet Key Exchange Version 2 (IKEv2) IKE_AUTH exchange to an IKEv2 client by deleting unwanted security associations (SAs) and previous IKEv2 sessions, use the `initial-contact force` command in IKEv2 profile configuration mode. To not process the initial contact notification, use the `no` form of this command.

```
initial-contact force
no initial-contact
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
IKEv2 processes the initial contact notification received in an IKE_AUTH exchange after successful authentication and deletes the old IKEv2 SA and IPsec SAs for the same local and remote IKEv2 peer or identity.

**Command Modes**
IKEv2 profile configuration (config-ikev2-profile)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Before using the `initial-contact force` command, you must configure the `crypto ikev2 profile` command. Configuring this command in the IKEv2 profile enforces the default behavior of initial contact processing, even if initial contact notification is not received.

**Examples**
The following example shows how to configure the `initial-contact force` command:

```
Device(config)# crypto ikev2 profile profile1
Device(config-ikev2-profile)# initial-contact force
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2 profile</td>
<td>Defines an IKEv2 profile.</td>
</tr>
</tbody>
</table>
initiate mode

To configure the Phase 1 mode of an Internet Key Exchange (IKE), use the initiate mode command in ISAKMP profile configuration mode. To remove the mode that was configured, use the no form of this command.

initiate mode aggressive
no initiate mode aggressive

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggressive</td>
<td></td>
<td>Aggressive mode is initiated.</td>
</tr>
</tbody>
</table>

Command Default
IKE initiates main mode.

Command Modes
ISAKMP profile configuration (config-isa-prof)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.6</td>
<td>This command was integrated into Cisco IOS XE Release 2.6.</td>
</tr>
</tbody>
</table>

Usage Guidelines
Use this command if you want to initiate an IKE aggressive mode exchange instead of a main mode exchange.

Examples

The following example shows that aggressive mode has been configured:

crypto isakmp profile vpnprofile
initiate mode aggressive
inservice (WebVPN)

To enable a SSL VPN gateway or context process, use the `inservice` command in webvpn gateway configuration or webvpn context configuration mode. To disable a SSL VPN gateway or context process without removing the configuration from the router configuration file, use the `no` form of this command.

```
inservice
no inservice
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

A SSL VPN gateway or context process is not enabled.

**Command Modes**

Webvpn gateway configuration
Webvpn context configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The enable form of this command initializes required system data structures, initializes TCP sockets, and performs other start-up tasks related to the SSL VPN gateway or context process. The gateway and context processes must both be “inservice” to enable SSL VPN.

**Examples**

The following example enables the SSL VPN gateway process named SSL_GATEWAY:

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# inservice
```

The following example configures and activates the SSL VPN context configuration:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# inservice
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>webvpn context</td>
<td>Enters webvpn configuration mode to configure the SSL VPN context.</td>
</tr>
<tr>
<td>webvpn gateway</td>
<td>Defines a SSL VPN gateway and enters webvpn gateway configuration mode.</td>
</tr>
</tbody>
</table>
inspect

To enable Cisco IOS stateful packet inspection, use the `inspect` command in policy-map-class configuration mode. To disable stateful packet inspection, use the `no` form of this command.

```
inspect [{parameter-map-name}]  
no inspect[{parameter-map-name}]  
```

### Syntax Description

- `parameter-map-name` *(Optional)* Name of a previously configured inspect parameter map. If you do not specify a parameter map name, the software uses the default values for all the parameters.

### Command Default

Cisco IOS stateful packet inspection is disabled.

### Command Modes

Policy-map-class configuration (config-pmap-c)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(2)T</td>
<td>This command was modified. Support for IPv6 was added.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.4S</td>
<td>This command was integrated into Cisco IOS XE Release 3.4S.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

You can use this command after entering the `policy-map type inspect`, `class type inspect`, and `parameter-map type inspect` commands.

To enable Cisco IOS stateful packet inspection, enter the name of an inspect parameter map that was previously configured with the `parameter-map type inspect` command.

This command lets you specify the attributes that will be used for the inspection.

### Examples

The following example specifies inspection parameters for alert and audit-trail, and requests the `inspect` action with the specified inspect parameter:

```
    parameter-map type inspect insp-params  
    alert on  
    audit-trail on  
    policy-map type inspect mypolicy  
    class type inspect inspect-traffic  
    inspect inspect-params  
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class type inspect</td>
<td>Specifies the traffic (class) on which an action is to be performed.</td>
</tr>
<tr>
<td>parameter-map type inspect</td>
<td>Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the <code>inspect</code> action.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>policy-map type inspect</td>
<td>Creates a Layer 3 and Layer 4 or a Layer 7 (protocol-specific) inspect-type policy map.</td>
</tr>
</tbody>
</table>
inspect (config-profile)

To enable Cisco IOS stateful packet inspection, use the inspect command in parameter-map type inspect configuration mode. To disable stateful packet inspection, use the no form of this command.

```
inspect {parameter-map-name | vrf vrf-name parameter-map-name}
no inspect {parameter-map-name | vrf vrf-name parameter-map-name}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>parameter-map-name</td>
<td>Parameter map name.</td>
</tr>
<tr>
<td>vrf</td>
<td>Binds a VPN routing and forwarding (VRF) instance to a parameter map.</td>
</tr>
<tr>
<td>vrf-name</td>
<td>VRF name.</td>
</tr>
</tbody>
</table>

**Command Default**

VRF instances are not bound to parameter maps.

**Command Modes**

Parameter-map type inspect configuration (config-profile)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.5S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must configure the `parameter-map type inspect-global` command before you can configure the inspect command.

**Examples**

The following example shows how to enable Cisco IOS stateful packet inspection:

```
Router(config)# parameter-map type inspect-global
Router(config-profile)# inspect pmap1
```

The following example shows how to bind an inspect-VRF parameter map to the default VRF:

```
Router(config)# parameter-map type inspect-global
Router(config-profile)# inspect vrf vrf1 pmap1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>parameter-map type inspect-global</td>
<td>Configures a global parameter map.</td>
</tr>
</tbody>
</table>
integrity

To specify one or more integrity algorithms for an Internet Key Exchange Version 2 (IKEv2) proposal, use the `integrity` command in IKEv2 proposal configuration mode. To remove the configuration of the hash algorithm, use the `no` form of this command.

```
integrity integrity_type
no integrity
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>integrity_type</td>
<td>Specifies the hash algorithm.</td>
</tr>
</tbody>
</table>

**Command Default**

The default integrity algorithm is used.

**Command Modes**

IKEv2 proposal configuration (config-ikev2-proposal)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(2)T</td>
<td>This command was modified. The <code>sha256</code> and <code>sha384</code> keywords were added.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use this command to specify the integrity algorithm to be used in an IKEv2 proposal. The default integrity algorithms in the default proposal are SHA-1 and MD5. The integrity algorithms can be one of the following:

<table>
<thead>
<tr>
<th>Integrity Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sha1</td>
<td>Specifies Secure Hash Algorithm (SHA-1 - HMAC variant) as the hash algorithm (No longer recommended).</td>
</tr>
<tr>
<td>sha256</td>
<td>Specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm.</td>
</tr>
<tr>
<td>sha384</td>
<td>Specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.</td>
</tr>
<tr>
<td>sha512</td>
<td>Specifies SHA-2 family 512-bit (HMAC variant) as the hash algorithm.</td>
</tr>
</tbody>
</table>
**Integrity Type** | **Description**  
---|---  
**md5** | Specifies Message-Digest algorithm 5 (MD5 - HMAC variant) as the hash algorithm.  

**Note**  
You cannot selectively remove an integrity algorithm when multiple integrity algorithms are configured.

Suite-B adds support for the SHA-2 family (HMAC variant) hash algorithm used to authenticate packet data and verify the integrity verification mechanisms for the IKEv2 proposal configuration. HMAC is a variant that provides an additional level of hashing.

**Examples**

The following example configures an IKEv2 proposal with the MD5 integrity algorithm:

```
Device(config)# crypto ikev2 proposal proposal1  
Device(config-ikev2-proposal)# integrity md5
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2 proposal</td>
<td>Defines an IKEv2 proposal.</td>
</tr>
<tr>
<td>encryption (ikev2 proposal)</td>
<td>Specifies the encryption algorithm in an IKEv2 proposal.</td>
</tr>
<tr>
<td>group (ikev2 proposal)</td>
<td>Specifies the Diffie-Hellman group identifier in an IKEv2 proposal.</td>
</tr>
<tr>
<td>show crypto ikev2 proposal</td>
<td>Displays the parameters for each IKEv2 proposal.</td>
</tr>
</tbody>
</table>
**interface (RITE)**

To specify the outgoing interface for exporting traffic, use the `interface` command in router IP traffic export (RITE) configuration mode. To disable an interface, use the `no` form of this command.

```
interface interface-name
no interface interface-name
```

**Syntax Description**
- `interface-name` Name of interface in which IP packets are exported.

**Command Default**
If this command is not enabled, the exported IP traffic profile does not recognize an interface in which to send captured IP traffic.

**Command Modes**
RITE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>15.1(SY)</td>
<td>This command was integrated into Cisco IOS Release 15.1(SY).</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
After you configure an IP traffic export profile via the `ip traffic-export profile` global configuration command, you should issue the `interface` command; otherwise, the profile will be unable to export the captured IP packets. If you do not specify the `interface` command, you will receive a warning, which states that the profile is incomplete, when you attempt to apply the profile to an interface via the `ip traffic-export apply profile` interface configuration command.

**Note**
Currently, only Ethernet and Fast Ethernet interfaces are supported.

**Examples**
The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the access control list ACL “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip traffic-export apply profile</code></td>
<td>Applies an IP traffic export profile to a specific interface.</td>
</tr>
<tr>
<td><code>ip traffic-export profile</code></td>
<td>Creates or edits an IP traffic export profile and enables the profile on an ingress interface.</td>
</tr>
</tbody>
</table>
interface (VASI)

To configure a virtual routing and forwarding (VRF)-Aware Software Infrastructure (VASI) interface, use the `interface` command in global configuration mode. To remove a VASI configuration, use the `no` form of this command.

```
interface {vasileft | vasiright} number
no interface {vasileft | vasiright} number
```

**Syntax Description**

- **vasileft**: Configures the vasileft interface.
- **vasiright**: Configures the vasiright interface.
- **number**: Identifier of the VASI interface pair. The range is from 1 to 2000.

**Command Default**

The VASI interface is not configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 2.6</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.1S</td>
<td>This command was modified. The <code>number</code> argument was modified to accept 500 VASI interface pairs.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was modified. The <code>number</code> argument was modified to accept 1000 VASI interface pairs.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.10S</td>
<td>This command was modified. The <code>number</code> argument was modified to accept 2000 VASI interface pairs.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The vasileft and vasiright interfaces must be configured before the VASI interface becomes active. The two halves of the interface pair must be configured separately. If only one half of the interface is configured and not the other half, then the VASI interface does not become active.

**Examples**

The following example shows how to configure vasileft and vasiright interfaces:

```
Device(config)# interface vasileft 200
Device(config-if)# vrf forwarding table1
Device(config-if)# ip address 192.168.0.1 255.255.255.0
Device(config-if)# exit
Device(config)# interface vasiright 200
Device(config-if)# vrf forwarding table2
Device(config-if)# ip address 192.168.1.1 255.255.255.0
Device(config-if)# exit
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug adjacency (VASI)</td>
<td>Displays debugging information for VASI adjacency.</td>
</tr>
<tr>
<td>debug interface (VASI)</td>
<td>Displays debugging information for a VASI interface descriptor block.</td>
</tr>
<tr>
<td>debug vasi</td>
<td>Displays VASI debugging information.</td>
</tr>
<tr>
<td>ip address</td>
<td>Sets a primary or secondary IP address for an interface.</td>
</tr>
<tr>
<td>show vasi pair</td>
<td>Displays the status of a VASI pair.</td>
</tr>
<tr>
<td>vrf forwarding</td>
<td>Associates a VRF instance or a virtual network with an interface or subinterface.</td>
</tr>
</tbody>
</table>
interface virtual-template

To create a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces, use the interface virtual-template command in global configuration mode. To remove a virtual template interface, use the no form of this command.

```
interface virtual-template number [type virtual-template-type]
no interface virtual-template number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Number used to identify the virtual template interface. Up to 200 virtual template interfaces can be configured. On the Cisco 10000 series router, up to 4095 virtual template interfaces can be configured.</td>
</tr>
<tr>
<td>type virtual-template-type</td>
<td>(Optional) Specifies the type of virtual template.</td>
</tr>
</tbody>
</table>

**Command Default**

No virtual template interface is defined.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2F</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(4)T</td>
<td>This command was enhanced to increase the maximum number of virtual template interfaces from 25 to 200.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(31)SB2</td>
<td>This command was integrated into Cisco IOS Release 12.2(31)SB2.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SB</td>
<td>This command’s default configuration was modified for SNMP and implemented on the Cisco 10000 series router for the PRE3 and PRE4.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.5</td>
<td>This command was implemented on Cisco ASR 1000 series routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A virtual template interface is used to provide the configuration for dynamically created virtual access interfaces. It is created by users and can be saved in NVRAM.

After the virtual template interface is created, it can be configured in the same way as a serial interface.

Virtual template interfaces can be created and applied by various applications such as virtual profiles, virtual private dialup networks (VPDNs), PPP over ATM, protocol translation, and Multichassis Multilink PPP (MMP).

**Cisco 10000 Series Router**

You can configure up to 4095 total virtual template interfaces on the Cisco 10000 series router.
To ensure proper scaling and to minimize CPU utilization, we recommend the following virtual template interface settings:

- A keepalive timer of 30 seconds or greater using the `keepalive` command. The default is 10 seconds.
- Do not enable the Cisco Discovery Protocol (CDP). CDP is disabled by default. Use the `no cdp enable` command to disable CDP, if necessary.
- Disable link-status event messaging using the `no logging event link-status` command.
- To prevent the virtual-access subinterfaces from being registered with the SNMP functionality of the router and using memory, do not use the router’s SNMP management tools to monitor PPP sessions. Use the `no virtual-template snmp` command to disable the SNMP management tools.

When a virtual template interface is applied dynamically to an incoming user session, a virtual access interface (VAI) is created.

If you configure a virtual template interface with interface-specific commands, the Cisco 10000 series router does not achieve the highest possible scaling. To verify that the router does not have interface-specific commands within the virtual template interface configuration, use the `test virtual-template number subinterface` command.

In Cisco IOS Release 12.2(33)SB, the default configuration for the `virtual-template snmp` command was changed to `no virtual-template snmp`. This prevents large numbers of entries into the MIB ifTable, thereby avoiding CPU Hog messages as SNMP uses the interfaces MIB and other related MIBs. If you configure the `no virtual-template snmp` command, the router no longer accepts the `snmp trap link-status` command under a virtual-template interface. Instead, the router displays a configuration error message such as the following:

```
Router(config)# interface virtual-template 1
Router(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

If your configuration already has the `snmp trap link-status` command configured under a virtual-template interface and you upgrade to Cisco IOS Release 12.2(33)SB, the configuration error occurs when the router reloads even though the virtual template interface is already registered in the interfaces MIB.

### Examples

#### Cisco 10000 Series Router

The following example creates a virtual template interface called Virtual-Template1:

```
Router(config)# interface Virtual-Templatel
Router(config-if)# ip unnumbered Loopback1
Router(config-if)# keepalive 60
Router(config-if)# no peer default ip address
Router(config-if)# ppp authentication pap
Router(config-if)# ppp authorization vpn1
Router(config-if)# ppp accounting vpn1
Router(config-if)# no logging event link-status
Router(config-if)# no virtual-template snmp
```

#### Virtual Template with PPP Authentication Example

The following example creates and configures virtual template interface 1:

```
```
interface virtual-template 1 type ethernet
    ip unnumbered ethernet 0
    ppp multilink
    ppp authentication chap

**IPsec Virtual Template Example**

The following example shows how to configure a virtual template for an IPsec virtual tunnel interface.

interface virtual-template1 type tunnel
    ip unnumbered Loopback1
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile virtualtunnelinterface

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>cdp enable</td>
<td>Enables Cisco Discovery Protocol (CDP) on an interface.</td>
</tr>
<tr>
<td></td>
<td>clear interface virtual-access</td>
<td>Tears down the live sessions and frees the memory for other client uses.</td>
</tr>
<tr>
<td></td>
<td>keepalive</td>
<td>Enables keepalive packets and to specify the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface.</td>
</tr>
<tr>
<td></td>
<td>show interface virtual-access</td>
<td>Displays the configuration of the active VAI that was created using a virtual template interface.</td>
</tr>
<tr>
<td></td>
<td>tunnel protection</td>
<td>Associates a tunnel interface with an IPsec profile.</td>
</tr>
<tr>
<td></td>
<td>virtual interface</td>
<td>Sets the zone name for the connected AppleTalk network.</td>
</tr>
<tr>
<td></td>
<td>virtual-profile</td>
<td>Enables virtual profiles.</td>
</tr>
<tr>
<td></td>
<td>virtual template</td>
<td>Specifies the destination for a tunnel interface.</td>
</tr>
</tbody>
</table>
ip (webvpn url rewrite)

To configure the IP address of the site to be mangled on a Secure Socket Layer virtual private network (SSL VPN) gateway, use the `ip` command in webvpn url rewrite configuration mode. To deselect the IP address, use the `no` form of this command.

```
ip  ip-address
no  ip  ip-address
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the site to be mangled.</td>
</tr>
</tbody>
</table>

**Command Default**

A site is not selected for mangling.

**Command Modes**

Webvpn url rewrite (config-webvpn-url-rewrite)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows that the IP address 10.0.0.255.255.0.0 has been selected for mangling:

```
Router (config)# webvpn context
Router (config-webvpn-context)# url rewrite
Router (config-webvpn-url-rewrite)# ip 10.1.0.0 255.255.0.0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host (webvpn url rewrite)</td>
<td>Selects the host name of the site to be mangled on an SSL VPN gateway.</td>
</tr>
<tr>
<td>unmatched-action (webvpn url rewrite)</td>
<td>Defines the action when the user request does not match the IP address or host site configuration.</td>
</tr>
</tbody>
</table>

Cisco IOS Security Command Reference: Commands D to L
To apply an IP access list or object group access control list (OGACL) to an interface or a service policy map, use the **ip access-group** command in the appropriate configuration mode. To remove an IP access list or OGACL, use the **no** form of this command.

```plaintext
ip access-group {access-list-nameaccess-list-number} {in|out}
no ip access-group {access-list-numberaccess-list-name} {in|out}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>access-list-name</strong></td>
<td>Name of the existing IP access list or OGACL as specified by an <strong>ip access-list</strong> command.</td>
</tr>
<tr>
<td><strong>access-list-number</strong></td>
<td>Number of the existing access list.</td>
</tr>
<tr>
<td></td>
<td>• Integer from 1 to 199 for a standard or extended IP access list.</td>
</tr>
<tr>
<td></td>
<td>• Integer from 1300 to 2699 for a standard or extended IP expanded access list.</td>
</tr>
<tr>
<td><strong>in</strong></td>
<td>Filters on inbound packets.</td>
</tr>
<tr>
<td><strong>out</strong></td>
<td>Filters on outbound packets.</td>
</tr>
</tbody>
</table>

### Command Default

An access list is not applied.

### Command Modes

- Interface configuration (config-if)
- Service policy-map configuration (config-service-policymap)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>11.2</td>
<td>The <strong>access-list-name</strong> argument was added.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was made available in service policy-map configuration mode.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>The <strong>access-list-name</strong> keyword was modified to accept the name of an OGACL.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
<tr>
<td>15.2(02)SA</td>
<td>This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If the specified access list does not exist, all packets are passed (no warning message is issued).

#### Applying Access Lists to Interfaces

Access lists or OGACLs are applied on either outbound or inbound interfaces. For standard inbound access lists, after an interface receives a packet, the Cisco IOS software checks the source address of the packet...
against the access list. For extended access lists or OGACLs, the networking device also checks the destination access list or OGACL. If the access list or OGACL permits the address, the software continues to process the packet. If the access list or OGACL rejects the address, the software discards the packet and returns an Internet Control Management Protocol (ICMP) host unreachable message.

For extended outbound access lists, after a device receives and routes a packet to a controlled interface, the software checks the source address of the packet against the access list. For extended access lists or OGACLs, the networking device also checks the destination access list or OGACL. If the access list or OGACL permits the address, the software sends the packet. If the access list or OGACL rejects the address, the software discards the packet and returns an ICMP host unreachable message.

When you enable outbound access lists or OGACLs, you automatically disable autonomous switching for that interface. When you enable inbound access lists or OGACLs on any CBus or CxBus interface, you automatically disable autonomous switching for all interfaces (with one exception—a Storage Services Enabler (SSE) configured with simple access lists can still switch packets, on output only).

### Applying Access Lists or OGACLs to Service Policy Maps

You can use the `ip access-group` command to configure Intelligent Services Gateway (ISG) per-subscriber firewalls. Per-subscriber firewalls are Cisco IOS IP access lists or OGACLs that are used to prevent subscribers, services, and pass-through traffic from accessing specific IP addresses and ports.

ACLs and OGACLs can be configured in user profiles or service profiles on an authentication, authorization, and accounting (AAA) server or in service policy maps on an ISG. OGACLS or numbered or named IP access lists can be configured on the ISG, or the ACL or OGACL statements can be included in the profile configuration.

When an ACL or OGACL is added to a service, all subscribers of that service are prevented from accessing the specified IP address, subnet mask, and port combinations through the service.

### Examples

The following example applies list 101 on packets outbound from Ethernet interface 0:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 0
Router(config-if)# ip access-group 101 out
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>Sets conditions in a named IP access list or OGACL that will deny packets.</td>
</tr>
<tr>
<td>ip access-list</td>
<td>Defines an IP access list or OGACL by name or number.</td>
</tr>
<tr>
<td>object-group network</td>
<td>Defines network object groups for use in OGACLs.</td>
</tr>
<tr>
<td>object-group service</td>
<td>Defines service object groups for use in OGACLs.</td>
</tr>
<tr>
<td>permit</td>
<td>Sets conditions in a named IP access list or OGACL that will permit packets.</td>
</tr>
<tr>
<td>show ip access-list</td>
<td>Displays the contents of IP access lists or OGACLs.</td>
</tr>
<tr>
<td>show object-group</td>
<td>Displays information about object groups that are configured.</td>
</tr>
</tbody>
</table>
ip access-list

To define an IP access list or object-group access control list (ACL) by name or number or to enable filtering for packets with IP helper-address destinations, use the `ip access-list` command in global configuration mode. To remove the IP access list or object-group ACL or to disable filtering for packets with IP helper-address destinations, use the `no` form of this command.

```
ip access-list {{standard|extended} {access-list-name|access-list-number}|helper egress check}
no ip access-list {{standard|extended} {access-list-name|access-list-number}|helper egress check}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>standard</strong></td>
<td>Specifies a standard IP access list.</td>
</tr>
<tr>
<td><strong>extended</strong></td>
<td>Specifies an extended IP access list. Required for object-group ACLs.</td>
</tr>
<tr>
<td><strong>access-list-name</strong></td>
<td>Name of the IP access list or object-group ACL. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.</td>
</tr>
</tbody>
</table>
| **access-list-number** | Number of the access list.  
  - A standard IP access list is in the ranges 1-99 or 1300-1999.  
  - An extended IP access list is in the ranges 100-199 or 2000-2699. |
| **helper egress check** | Enables permit or deny matching capability for an outbound access list that is applied to an interface, for traffic that is relayed via the IP helper feature to a destination server address. |

**Command Default**

No IP access list or object-group ACL is defined, and outbound ACLs do not match and filter IP helper relayed traffic.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was modified. Object-group ACLs are now accepted when the <code>deny</code> and <code>permit</code> commands are used in standard IP access-list configuration mode or extended IP access-list configuration mode.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2S</td>
<td>This command was implemented on Cisco ASR 1000 series routers.</td>
</tr>
<tr>
<td>15.0(1)M5</td>
<td>This command was modified. The <code>helper</code>, <code>egress</code>, and <code>check</code> keywords were added.</td>
</tr>
</tbody>
</table>
This command was modified. The **helper**, **egress**, and **check** keywords were added.

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)SY</td>
<td>This command was modified. The <strong>helper</strong>, <strong>egress</strong>, and <strong>check</strong> keywords were added.</td>
</tr>
<tr>
<td>15.1(3)T3</td>
<td>This command was modified. The <strong>helper</strong>, <strong>egress</strong>, and <strong>check</strong> keywords were added.</td>
</tr>
<tr>
<td>15.1(2)SNG</td>
<td>This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to configure a named or numbered IP access list or an object-group ACL. This command places the router in access-list configuration mode, where you must define the denied or permitted access conditions by using the **deny** and **permit** commands.

Specifying the **standard** or **extended** keyword with the **ip access-list** command determines the prompt that appears when you enter access-list configuration mode. You must use the **extended** keyword when defining object-group ACLs.

You can create object groups and IP access lists or object-group ACLs independently, which means that you can use object-group names that do not yet exist.

Named access lists are not compatible with Cisco IOS software releases prior to Release 11.2.

Use the **ip access-group** command to apply the access list to an interface.

The **ip access-list helper egress check** command enables outbound ACL matching for permit or deny capability on packets with IP helper-address destinations. When you use an outbound extended ACL with this command, you can permit or deny IP helper relayed traffic based on source or destination User Datagram Protocol (UDP) ports. The **ip access-list helper egress check** command is disabled by default; outbound ACLs will not match and filter IP helper relayed traffic.

### Examples

The following example defines a standard access list named Internetfilter:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list standard Internetfilter
Router(config-nacl)# permit 192.168.255.0 0.0.0.255
Router(config-nacl)# permit 10.88.0.0 0.0.255.255
Router(config-nacl)# permit 10.0.0.0 0.255.255.255
```

The following example shows how to create an object-group ACL that permits packets from the users in **my_network_object_group** if the protocol ports match the ports specified in **my_service_object_group**:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended my_ogacl_policy
Router(config-ext-nacl)# permit tcp object-group my_network_object_group portgroup my_service_object_group any
Router(config-ext-nacl)# deny tcp any any
```

The following example shows how to enable outbound ACL filtering on packets with helper-address destinations:
Router> `enable`
Router# `configure terminal`
Router(config)# `ip access-list helper egress check`

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>deny</code></td>
<td>Sets conditions in a named IP access list or in an object-group ACL that will deny packets.</td>
</tr>
<tr>
<td><code>ip access-group</code></td>
<td>Applies an ACL or an object-group ACL to an interface or a service policy map.</td>
</tr>
<tr>
<td><code>object-group network</code></td>
<td>Defines network object groups for use in object-group ACLs.</td>
</tr>
<tr>
<td><code>object-group service</code></td>
<td>Defines service object groups for use in object-group ACLs.</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>Sets conditions in a named IP access list or in an object-group ACL that will permit packets.</td>
</tr>
<tr>
<td><code>show ip access-list</code></td>
<td>Displays the contents of IP access lists or object-group ACLs.</td>
</tr>
<tr>
<td><code>show object-group</code></td>
<td>Displays information about object groups that are configured.</td>
</tr>
</tbody>
</table>
ip access-list hardware permit fragments

To permit all noninitial fragments in the hardware, use the `ip access-list hardware permit fragments` command in global configuration mode. To return to the default settings, use the `no` form of this command.

```plaintext
ip access-list hardware permit fragments
no ip access-list hardware permit fragments
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
All fragments from flows that are received from an ACE with Layer 4 ports and permit action are permitted. All other fragments are dropped in the hardware. This action also applies to flows that are handled in the software regardless of this command setting.

**Command Modes**
Global configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(18)SXF5</td>
<td>This command was changed to affect all ACLs currently applied to interfaces and not just newly-applied ACLs. See the &quot;Usage Guidelines&quot; section for more information.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Flow fragments that match ACEs with Layer 4 ports and permit results are permitted in the hardware, and all other fragments are dropped. An entry is added in the TCAM for each ACE with Layer 4 ports and permit action. This action could cause large ACLs to not fit in the TCAM. If this is the case, use the `ip access-list hardware permit fragments` command to permit all noninitial fragments in the hardware.

- **Note**
  Configurations that you modify after you entered the `ip access-list hardware permit fragments` command will permit all noninitial fragments in the hardware. Hardware configurations that you modified before you entered the `ip access-list hardware permit fragments` command will not be changed.

- **Note**
  Hardware configurations that you modify after you entered the `no ip access-list hardware permit fragments` command will return to the default settings. Hardware configurations that you modified before you entered the `no ip access-list hardware permit fragments` command do not change.

The initial flow fragments that match the ACEs with Layer 4 ports and permit results are permitted in the hardware. All other initial fragments are dropped in the hardware.

**Catalyst 6500 Series Switches**

---

*icmp idle-timeout through ip http ezvpn*
The following restrictions apply to Cisco IOS releases before Cisco IOS Release 12.2(18)SX5:

**Note**
Configurations that you modify after you entered the `ip access-list hardware permit fragments` command will permit all noninitial fragments in the hardware. Hardware configurations that you modified before you entered the `ip access-list hardware permit fragments` command will not be changed.

**Note**
Hardware configurations that you modify after you entered the `no ip access-list hardware permit fragments` command will return to the default settings. Hardware configurations that you modified before you entered the `no ip access-list hardware permit fragments` command do not change.

In Cisco IOS releases after Cisco IOS Release 12.2(18)SX5, this command affects all ACLs currently applied to interfaces and not just newly-applied ACLs.

**Examples**

This example shows how to permit all noninitial fragments in the hardware:

```
Router(config)# ip access-list hardware permit fragments
```

This example shows how to return to the default settings:

```
Router(config)# no ip access-list hardware permit fragments
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip interface</code></td>
<td>Displays the usability status of interfaces that are configured for IP.</td>
</tr>
</tbody>
</table>
ip access-list logging interval

To configure the logging interval for access list entries, use the `ip access-list logging interval` command in global configuration mode. To disable the configuration, use the `no` form of this command.

```
ip access-list logging interval interval
no ip access-list logging interval
```

**Syntax Description**

- `interval` Access list logging interval, in milliseconds. The range is from 0 to 2147483647.

**Command Default**

Access list logging intervals are not configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the access list logging interval to 100 milliseconds:

```
Router# configure terminal
Router(config)# ip access-list logging interval 100
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip access-list logging hash-generation</code></td>
<td>Enables hash-value generation for ACE syslog entries.</td>
</tr>
</tbody>
</table>
ip access-list log-update

To set the threshold number of packets that generate a log message if they match an access list, use the ip access-list log-update command in global configuration mode. To remove the threshold, use the no form of this command.

```
ip access-list log-update threshold number-of-matches
no ip access-list log-update
```

**Syntax Description**

| number-of-matches | Threshold number of packets necessary to match an access list before a log message is generated. The range is 0 to 2147483647. There is no default number of matches. |

**Command Default**

Log messages are sent at the first matching packet and at 5-minute intervals after that.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Log messages are generated if you have specified the log keyword in the access-list (IP standard), access-list (IP extended), deny (IP), dynamic, or permit command.

Log messages provide information about the packets that are permitted or denied by an access list. By default, log messages appear at the console. (The level of messages logged to the console is controlled by the logging console command.) The log message includes the access list number, whether the packet was permitted or denied, and other information.

By default, the log messages are sent at the first matching packet and after that, identical messages are accumulated for 5-minute intervals, with a single message being sent with the number of packets permitted and denied during that interval. However, you can use the ip access-list log-update command to set the number of packets that, when match an access list (and are permitted or denied), cause the system to generate a log message. You might want to do this to receive log messages more frequently than at 5-minute intervals.

**Caution**

If you set the number-of-matches argument to 1, a log message is sent right away, rather than caching it; every packet that matches an access list causes a log message. A setting of 1 is not recommended because the volume of log messages could overwhelm the system.

Even if you use the ip access-list log-update command, the 5-minute timer remains in effect, so the cache is emptied at the end of 5 minutes, regardless of the count of messages in the cache. Regardless of when the log message is sent, the cache is flushed and the count reset to 0 for that message the same way it is when a threshold is not specified.
If the syslog server is not directly connected to a LAN that the router shares, any intermediate router might drop the log messages because they are UDP (unreliable) messages.

**Examples**

The following example enables logging whenever the 1000th packet matches an access list entry:

```
ip access-list log-update threshold 1000
```

<table>
<thead>
<tr>
<th><strong>Related Commands</strong></th>
<th><strong>Command</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>access-list (IP extended)</td>
<td>Defines an extended IP access list.</td>
</tr>
<tr>
<td></td>
<td>access-list (IP standard)</td>
<td>Defines a standard IP access list.</td>
</tr>
<tr>
<td></td>
<td>deny (IP)</td>
<td>Sets conditions under which a packet is denied by a named IP access list.</td>
</tr>
<tr>
<td></td>
<td>dynamic</td>
<td>Defines a named dynamic IP access list.</td>
</tr>
<tr>
<td></td>
<td>logging console</td>
<td>Limits messages logged to the console, based on severity.</td>
</tr>
<tr>
<td></td>
<td>permit</td>
<td>Sets conditions under which a packet passes a named IP access list.</td>
</tr>
</tbody>
</table>
ip access-list resequence

To apply sequence numbers to the access list entries in an access list, use the `ip access-list resequence` command in global configuration mode.

```
ip access-list resequence access-list-name starting-sequence-number increment
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>access-list-name</strong></td>
<td>Name of the access list. Names cannot contain a space or quotation mark.</td>
</tr>
<tr>
<td><strong>starting-sequence-number</strong></td>
<td>Access list entries will be resequenced using this initial value. The default value is 10. The range of possible sequence numbers is 1 through 2147483647.</td>
</tr>
<tr>
<td><strong>increment</strong></td>
<td>The number by which the sequence numbers change. The default value is 10. For example, if the increment value is 5 and the beginning sequence number is 20, the subsequent sequence numbers are 25, 30, 35, 40, and so on.</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(14)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command allows the `permit` and `deny` entries of a specified access list to be resequenced with an initial sequence number value determined by the `starting-sequence-number` argument, and continuing in increments determined by the `increment` argument. If the highest sequence number exceeds the maximum possible sequence number, then no sequencing occurs.

For backward compatibility with previous releases, if entries with no sequence numbers are applied, the first entry is assigned a sequence number of 10, and successive entries are incremented by 10. The maximum sequence number is 2147483647. If the generated sequence number exceeds this maximum number, the following message is displayed:

```
Exceeded maximum sequence number.
```

If the user enters an entry without a sequence number, it is assigned a sequence number that is 10 greater than the last sequence number in that access list and is placed at the end of the list.

If the user enters an entry that matches an already existing entry (except for the sequence number), then no changes are made.

If the user enters a sequence number that is already present, the following error message is generated:
Duplicate sequence number.

If a new access list is entered from global configuration mode, then sequence numbers for that access list are generated automatically.

Distributed support is provided so that the sequence numbers of entries in the Route Processor (RP) and line card (LC) are in synchronization at all times.

Sequence numbers are not saved in NVRAM. That is, the sequence numbers themselves are not saved. In the event that the system is reloaded, the configured sequence numbers revert to the default sequence starting number and increment.

This command works with named standard and extended IP access lists. Because the name of an access list can be designated as a number, numbers are acceptable as names as long as they are entered in named access list configuration mode.

Examples

The following example resequences an access list named kmd1. The starting sequence number is 100, and the increment value is 5:

```bash
ip access-list resequence kmd1 100 5
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny (IP)</td>
<td>Sets conditions under which a packet does not pass a named IP access list.</td>
</tr>
<tr>
<td>permit (IP)</td>
<td>Sets conditions under which a packet passes a named IP access list.</td>
</tr>
</tbody>
</table>
ip access-list logging hash-generation

To enable hash-value generation for access control entry (ACE) syslog entries, use the ip access-list logging hash-generation command in global configuration mode. To disable hash value generation, use the no form of this command.

```
no ip access-list logging hash-generation
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Hash value generation is disabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(22)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Cisco IOS routers generate syslog entries for log-enabled ACEs. The system appends a tag (either a user-defined cookie or a router-generated MD5 hash value) to ACE syslog entries. This tag uniquely identifies the ACE, within an access control list (ACL), that generated the syslog entry.

Use this command to generate an MD5 hash value for all the log enabled ACEs in the system that do not have a user-defined cookie. The system attaches the router-generated hash value to the corresponding ACE. The hash value is stored locally in the router’s NVRAM and persists through router reloads.

**Examples**

The following example shows how to enable hash value generation on the router, for IP access list syslog entries:

```
Router(config)# ip access-list logging hash-generation
```

```
*Aug 7 01:10:12.077: %IPACL-HASHGEN: ACL: 101 seq no : 20 Hash code is 0x75F079
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list (IP extended)</td>
<td>Defines an extended IP access list.</td>
</tr>
<tr>
<td>access-list (IP standard)</td>
<td>Defines a standard IP access list.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td><strong>debug ip access-list hash-generation</strong></td>
<td>Displays debugging information about ACL hash generation.</td>
</tr>
<tr>
<td><strong>show ip access-list</strong></td>
<td>Displays the contents of all current access lists.</td>
</tr>
</tbody>
</table>
ip-address (ca-trustpoint)

To specify an IPv4 or IPv6 address, or the interface that is included as “unstructuredAddress” in the certificate request, use the ip-address command in ca-trustpoint configuration mode. To restore the default behavior, use the no form of this command.

```
ip-address  {ip-addressinterface|none}
no  ip-address
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Specifies the IPv4 or IPv6 address that is included as “unstructuredAddress” in the certificate request.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface, from which the router can get an IP address, that is included as “unstructuredAddress” in the certificate request.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies that an IP address is not to be included in the certificate request.</td>
</tr>
</tbody>
</table>

**Command Default**

An IP address is not configured. You are prompted for the IP address during certificate enrollment.

**Command Modes**

Ca-trustpoint configuration (config-ca-trustpoint)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(1)T</td>
<td>This command was modified. Support for specifying the IPv6 address that is included as “unstructuredAddress” in the certificate request was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before you can issue this command, you must enable the `crypto ca pki trustpoint` command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode. The `ip-address` command allows a certificate enrollment parameter to be specified.

Use the `ip-address` command to include the IP address of the specified interface in the certificate request or to specify that an IP address should not be included in the certificate request.

If this command is enabled, you are not prompted for an IP address during certificate enrollment.

**Examples**

The following example shows how to include the IP address of the Ethernet-0 interface in the certificate request for the trustpoint “my_trustpoint”:

```
crypto ca trustpoint my_trustpoint
   enrollment url http://my_trustpoint.cisco.com/
   subject-name OU=Spiral Dept., O=tiedye.com
   ip-address ethernet-0
```

The following example shows how to include the IPv6 address that is included as “unstructuredAddress” in the certificate request for the trustpoint “my_trustpoint”:

```
crypto ca trustpoint my_trustpoint
```
The following example shows that an IPv4 address is not to be included in the certificate request:

crypto ca trustpoint my_trustpoint
enrollment url http://10.3.0.7:80
fqdn none
ip-address none
subject-name CN=subject1, OU=PKI, O=Cisco Systems, C=US

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>crypto ca trustpoint</td>
<td>Declares the CA that your router should use.</td>
</tr>
</tbody>
</table>
ip address dhcp

To acquire an IP address on an interface from the DHCP, use the `ip address dhcp` command in interface configuration mode. To remove any address that was acquired, use the `no` form of this command.

```
ip address dhcp [client-id interface-type number] [hostname hostname]
no ip address dhcp [client-id interface-type number] [hostname hostname]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client-id</td>
<td>(Optional) Specifies the client identifier. By default, the client identifier is an ASCII value. The <code>client-id interface-type number</code> option sets the client identifier to the hexadecimal MAC address of the named interface.</td>
</tr>
<tr>
<td>interface-type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>number</td>
<td>(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>hostname</td>
<td>(Optional) Specifies the hostname.</td>
</tr>
<tr>
<td>hostname</td>
<td>(Optional) Name of the host to be placed in the DHCP option 12 field. This name need not be the same as the hostname entered in global configuration mode.</td>
</tr>
</tbody>
</table>

**Command Default**

The hostname is the globally configured hostname of the router. The client identifier is an ASCII value.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(3)T</td>
<td>This command was modified. The <code>client-id</code> keyword and <code>interface-type number</code> argument were added.</td>
</tr>
<tr>
<td>12.2(3)</td>
<td>This command was modified. The <code>hostname</code> keyword and <code>hostname</code> argument were added. The behavior of the <code>client-id interface-type number</code> option changed. See the “Usage Guidelines” section for details.</td>
</tr>
<tr>
<td>12.2(8)T</td>
<td>This command was modified. The command was expanded for use on PPP over ATM (PPPoA) interfaces and certain ATM interfaces.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>15.1(3)T</td>
<td>This command was modified. Support was provided on the tunnel interface.</td>
</tr>
</tbody>
</table>
Prior to Cisco IOS Release 12.2(8)T, the `ip address dhcp` command could be used only on Ethernet interfaces.

The `ip address dhcp` command allows any interface to dynamically learn its IP address by using the DHCP protocol. It is especially useful on Ethernet interfaces that dynamically connect to an Internet service provider (ISP). Once assigned a dynamic address, the interface can be used with the Port Address Translation (PAT) of Cisco IOS Network Address Translation (NAT) to provide Internet access to a privately addressed network attached to the router.

The `ip address dhcp` command also works with ATM point-to-point interfaces and will accept any encapsulation type. However, for ATM multipoint interfaces you must specify Inverse ARP via the `protocol ip inarp` interface configuration command and use only the aa15snap encapsulation type.

Some ISPs require that the DHCPDISCOVER message have a specific hostname and client identifier that is the MAC address of the interface. The most typical usage of the `ip address dhcp client-id interface-type number hostname hostname` command is when `interface-type` is the Ethernet interface where the command is configured and `interface-type number` is the hostname provided by the ISP.

A client identifier (DHCP option 61) can be a hexadecimal or an ASCII value. By default, the client identifier is an ASCII value. The `client-id interface-type number` option overrides the default and forces the use of the hexadecimal MAC address of the named interface.

Between Cisco IOS Releases 12.1(3)T and 12.2(3), the `client-id` optional keyword allows the change of the fixed ASCII value for the client identifier. After Release 12.2(3), the optional `client-id` keyword forces the use of the hexadecimal MAC address of the named interface as the client identifier.

If a Cisco router is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If you use the `ip address dhcp` command with or without any of the optional keywords, the DHCP option 12 field (hostname option) is included in the DISCOVER message. By default, the hostname specified in option 12 will be the globally configured hostname of the router. However, you can use the `ip address dhcp hostname hostname` command to place a different name in the DHCP option 12 field than the globally configured hostname of the router.

The `no ip address dhcp` command removes any IP address that was acquired, thus sending a DHCPRELEASE message.

You might need to experiment with different configurations to determine the one required by your DHCP server. The table below shows the possible configuration methods and the information placed in the DISCOVER message for each method.

**Table 7: Configuration Method and Resulting Contents of the DISCOVER Message**

<table>
<thead>
<tr>
<th>Configuration Method</th>
<th>Contents of DISCOVER Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip address dhcp</code></td>
<td>The DISCOVER message contains “cisco- mac-address -Eth1” in the client ID field. The <code>mac-address</code> is the MAC address of the Ethernet 1 interface and contains the default hostname of the router in the option 12 field.</td>
</tr>
</tbody>
</table>
**Contents of DISCOVER Messages**

<table>
<thead>
<tr>
<th>Configuration Method</th>
<th>Contents of DISCOVER Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address dhcp hostname hostname</td>
<td>The DISCOVER message contains “cisco-mac-address-Eth1” in the client ID field. The mac-address is the MAC address of the Ethernet 1 interface, and contains hostname in the option 12 field.</td>
</tr>
<tr>
<td>ip address dhcp client-id ethernet 1</td>
<td>The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains the default hostname of the router in the option 12 field.</td>
</tr>
<tr>
<td>ip address dhcp client-id ethernet 1 hostname hostname</td>
<td>The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains hostname in the option 12 field.</td>
</tr>
</tbody>
</table>

**Examples**

In the examples that follow, the command `ip address dhcp` is entered for Ethernet interface 1. The DISCOVER message sent by a router configured as shown in the following example would contain “cisco-mac-address -Eth1” in the client-ID field, and the value abc in the option 12 field.

```
hostname abc
interface Ethernet 1
ip address dhcp
```

The DISCOVER message sent by a router configured as shown in the following example would contain “cisco-mac-address -Eth1” in the client-ID field, and the value def in the option 12 field.

```
hostname abc
interface Ethernet 1
ip address dhcp hostname def
```

The DISCOVER message sent by a router configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value abc in the option 12 field.

```
hostname abc
interface Ethernet 1
ip address dhcp client-id Ethernet 1
```

The DISCOVER message sent by a router configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value def in the option 12 field.

```
hostname abc
interface Ethernet 1
ip address dhcp client-id Ethernet 1 hostname def
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp pool</td>
<td>Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.</td>
</tr>
</tbody>
</table>
ip address (WebVPN)

To configure a proxy IP address on a Secure Socket Layer virtual private network (SSL VPN) gateway, use the `ip address` command in webvpn gateway configuration mode. To remove the proxy IP address from the SSL VPN gateway, use the `no` form of this command.

```plaintext
ip address ip-address [port port-number] [standby name]
no ip address
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IPv4 address.</td>
</tr>
<tr>
<td><code>port port-number</code></td>
<td>(Optional) Specifies the port number for proxy traffic. A number from 1 to 65535 can be entered for this argument. The default port number 443 is used if this command is configured without entering the <code>port</code> keyword.</td>
</tr>
</tbody>
</table>
| `standby name`  | • (Optional) Indicates that the IP address is a virtual address configured on one of the router interfaces using Hot Standby Routing Protocol (HSRP).  
• `name` --Must be the same as the HSRP group name that was configured on the router interface. |

Note: Note that the `name` argument is not an optional parameter when the `standby` keyword is used.

### Command Default

A proxy IP address is not configured.

### Command Modes

Webvpn gateway configuration (config-webvpn-gateway)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>The <code>standby</code> keyword and <code>name</code> arguments were added.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `ip address` command is used to configure a proxy IP address for an SSL VPN gateway. The IP address is the termination point for all SSL VPN client connections. This IP address can be any routable IP address assigned to a valid interface.

### Examples

The following example configures 192.168.1.1 as a proxy address on an SSL VPN gateway. Proxy traffic is directed over port 443.

```plaintext
Router(config) # webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway) # ip address 192.168.1.1 port 443
```

The following example shows that Router 1 and Router 2 are configured for HSRP on Gateway Webvpn:
Router 1 Configuration

Router# configure terminal
Router config)# interface g0/1
Router (config-if)# standby 0 ip 10.1.1.1
Router (config-if)# standby 0 name SSLVPN
Router (config-if)# exit
Router (config)# webvpn gateway Webvpn
Router (config-webvpn-gateway)# ip address 10.1.1.1 port 443 standby SSLVPN

Router 2 Configuration

Router# configure terminal
Router (config)# interface g0/0
Router (config-if)# standby 0 ip 10.1.1.1
Router (config-if)# standby 0 name SSLVPN2
Router (config-if)# exit
Router (config)# webvpn gateway Webvpn
Router (config-webvpn-gateway)# ip address 10.1.1.1 port 443 standby SSLVPN2

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>standby name</td>
<td>Configures the name of the standby group.</td>
</tr>
<tr>
<td>webvpn gateway</td>
<td>Defines an SSL VPN gateway and enters webvpn gateway configuration mode.</td>
</tr>
</tbody>
</table>
ip admission

To create a Layer 3 network admission control rule to be applied to the interface, or to create a policy that can be applied on an interface when the authentication, authorization and accounting (AAA) server is unreachable, use the `ip admission` command in interface configuration mode. To create a global policy that can be applied on a network access device, use the `ip admission command with the optional keywords and argument in global configuration mode. To remove the admission control rule, use the `no` form of this command.

```
ip admission admission-name [absolute-timer timeout | auth-proxy-audit | auth-proxy-banner
[file file-name | http http-banner-text] | init-state-time time | max-login-attempts login-attempts
| name authentication-name | proxy http[failure page file filename | page file filename] | refresh-all
| success[page file filename | redirect URL] | ratelimit sessions-limit | service-policy type tag
policy-name | source-interface interface-type | virtual-ip ip-address | watch-list[add-item address
| enable | expiry-time time]]
```

```
o ip admission admission-name [absolute-timer timeout | auth-proxy-audit | auth-proxy-banner
[file file-name | http http-banner-text] | init-state-time time | max-login-attempts login-attempts
| name authentication-name | proxy http[failure page file filename | page file filename] | refresh-all
| success[page file filename | redirect URL] | ratelimit sessions-limit | service-policy type tag
policy-name | source-interface interface-type | virtual-ip ip-address | watch-list[add-item address
| enable | expiry-time time]]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admission-name</td>
<td>Authentication or admission rule name.</td>
</tr>
<tr>
<td>absolute-timer</td>
<td>Configures the time in minutes for which the ip admission sessions can exist on the ISR irrespective of transactions. This is applicable for all the ip admission rules configured on the ISR.</td>
</tr>
<tr>
<td>auth-proxy-audit</td>
<td>Enables auditing for Authentication Proxy.</td>
</tr>
<tr>
<td>auth-proxy-banner</td>
<td>Configures banner for Authentication Proxy Login Page through file or text.</td>
</tr>
<tr>
<td>consent-banner</td>
<td>Configures banner for Authentication Proxy Consent Page through file or text.</td>
</tr>
<tr>
<td>event</td>
<td>Specify an authentication policy to be applied to ip admission sessions when the AAA server is unreachable.</td>
</tr>
<tr>
<td>http</td>
<td>Specify number of http processes ranging from 1 to 16.</td>
</tr>
<tr>
<td>inactivity-timer</td>
<td>Configures the time in minutes for which the ip admission sessions can exist on the ISR without any transactions. This is applicable for all the ip admission rules configured on the ISR.</td>
</tr>
<tr>
<td>init-state-time</td>
<td>Configures the time in minutes for which the ip admission sessions can exist on the ISR until authentication is succeeded. This is applicable for all the ip admission rules configured on the ISR.</td>
</tr>
<tr>
<td>max-http-conns</td>
<td>Configures maximum number of HTTP connections per client ranging from 1 to 200.</td>
</tr>
<tr>
<td>max-login-attempts</td>
<td>Configures maximum login attempts that are required before an ip admission session is moved to failed state.</td>
</tr>
</tbody>
</table>
**max-nodata-conns** Configures maximum TCP NODATA Connections to be allowed ranging from 1 to 1000

**max-nodata-conns** Configures an Authentication Proxy Rule

**proxy** Configures various pages for Authentication Proxy

**ratelimit** Configures session ratelimit ranging from 100 to 1000

**service-policy** Associates a tag based service-policy to ip admission

**source-interface** Specify source interface for ip admission

**virtual-ip** Configure web-based proxy authentication virtual IP address

**watch-list** Enables and configures ip admission watch-list functionality.

---

**Command Default**

A network admission control rule is not applied to the interface.

**Command Modes**

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was modified to include the <code>event timeout aaa policy identity</code> keywords and the <code>identity-policy-name</code> argument.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The admission rule defines how you apply admission control.

The optional keywords and argument define the network admission policy to be applied to a network access device or an interface when no AAA server is reachable. The command can be used to associate a default identity policy with Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) sessions.

**Examples**

The following example shows how to apply a network admission control rule named "nacrule1" to the interface:

```
Router (config-if)# ip admission nacrule1
```

The following example shows how to apply an identity policy named "example" to the device when the AAA server is unreachable:

```
Router (config)# ip admission nacrule1 event timeout aaa policy identity example
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>interface</td>
<td>Defines an interface.</td>
</tr>
</tbody>
</table>
ip admission consent banner

To display a banner on the authentication proxy consent webpage, use the `ip admission consent banner` command in global configuration mode. To disable the display of the banner, use the `no` form of this command.

```
ip admission consent banner {file file-name | text banner-text}
no ip admission consent banner
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>file file-name</td>
<td>Specifies a file that is to be shown as the consent webpage.</td>
</tr>
<tr>
<td>text banner-text</td>
<td>Specifies a text string to replace the default banner, which is the name of the router. The text string must be in the following format: “C banner-text C,” where “C” is a delimiting character.</td>
</tr>
</tbody>
</table>

**Command Default**

A banner is not displayed on the authentication proxy consent webpage.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 12.4(15)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to configure one of the following two scenarios:

- The `ip admission consent banner` command is configured using a filename.

  In this scenario, the administrator provides the location and name of the file that is to be used for the consent web page.

- The `ip admission consent banner` command is configured using a banner text.

  In this scenario, the administrator provides a multiline text that is converted into HTML. Only the multiline text is displayed on the authentication proxy login page.

**Note**

If the `ip admission consent banner` command is not enabled, nothing is displayed to the user on the consent login page, except two text boxes to enter the username and password, respectively.

**Note**

When HTTP authentication proxy is configured along with the IOS Consent feature, any HTTP authentication proxy-related configurations or policies will override the consent page-related configurations or policies. For example, if the `ip admission name admission-name consent` command is configured, the `ip admission consent banner` command is ignored, and only the banner that is configured by the `ip admission auth-proxy-banner` command is displayed.

**Examples**

The following example shows how to display the file “consent_page.html” located in flash:
The following example shows how to specify the custom banner “Consent-Page-Banner-Text” to be displayed in the authentication proxy consent webpage:

```
Device(config)# ip admission consent-banner file flash:consent_page.html
```

```
Device(config)# ip admission consent-banner text ^C Consent-Page-Banner-Text ^C
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip auth-proxy auth-proxy-banner</td>
<td>Displays a banner, such as the router name, in the authentication proxy login page.</td>
</tr>
</tbody>
</table>
ip admission name

To create an IP network admission control rule, use the `ip admission name` command in global configuration mode. To remove the network admission control rule, use the `no` form of this command.

```
ip admission name admission-name [{eapoudp [bypass] proxy {ftp|http|telnet} | service-policy type tag service-policy-name}] [list {acl acl-name}] [event] [timeout aaa] [policy identity identity-policy-name]
```

```
o ip admission name admission-name [{eapoudp [bypass] proxy {ftp|http|telnet} | service-policy type tag service-policy-name}] [list {acl acl-name}] [event] [timeout aaa] [policy identity identity-policy-name]
```

Syntax for Authentication Proxy Consent Webpage

```
ip admission name admission-name consent [[absolute-timer minutes] [event] [inactivity-time minutes] [list {acl acl-name}] [parameter-map consent-parameter-map-name]]
```

```
o ip admission name admission-name consent [[absolute-timer minutes] [event] [inactivity-time minutes] [list {acl acl-name}] [parameter-map consent-parameter-map-name]]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admission-name</td>
<td>Name of network admission control rule.</td>
</tr>
<tr>
<td>eapoudp</td>
<td>(Optional) Specifies IP network admission control using Extensible Authentication Protocol over UDP (EAPoUDP).</td>
</tr>
<tr>
<td>bypass</td>
<td>(Optional) Admission rule bypasses EAPoUDP communication.</td>
</tr>
<tr>
<td>proxy</td>
<td>(Optional) Specifies authentication proxy.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies that FTP is to be used to trigger the authentication proxy.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies that HTTP is to be used to trigger authentication proxy.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies that Telnet is to be used to trigger authentication proxy.</td>
</tr>
<tr>
<td>service-policy type tag</td>
<td>A control plane service policy is to be configured.</td>
</tr>
<tr>
<td>service-policy-name</td>
<td>Control plane tag service policy that is configured using the <code>policy-map type control tag {policy name}</code> command, keyword, and argument. This policy map is used to apply the actions on the host when a tag is received.</td>
</tr>
<tr>
<td>list</td>
<td>(Optional) Associates the named rule with an access control list (ACL).</td>
</tr>
<tr>
<td>acl</td>
<td>Applies a standard, extended list to a named admission control rule. The value ranges from 1 through 199.</td>
</tr>
<tr>
<td>acl-name</td>
<td>Applies a named access list to a named admission control rule.</td>
</tr>
<tr>
<td>event</td>
<td>(Optional) Identifies the condition that triggered the application of the policy.</td>
</tr>
<tr>
<td>timeout aaa</td>
<td>(Optional) Specifies that the AAA server is unreachable.</td>
</tr>
</tbody>
</table>
**policy identity**

Configure the application of an identity policy to be used while the AAA server is unreachable.

*identity-policy-name*

Specifies the identity policy to apply.

**consent**

Associates an authentication proxy consent webpage with the IP admission rule specified via the *admission-name* argument.

**absolute-timer minutes**

(Optional) Elapsed time, in minutes, before the external server times out.

**inactivity-time minutes**

(Optional) Elapsed time, in minutes, before the external file server is deemed unreachable.

**parameter-map**

(Optional) A parameter map policy is to be associated with consent profile.

**consent-parameter-map-name**

Specifies the consent profile parameters to apply.

---

**Command Default**

An IP network admission control rule is not created.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(6)T</td>
<td>The <strong>bypass</strong> and <strong>service-policy type tag</strong> keywords and <strong>service-policy-name</strong> argument were added.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>The <strong>event</strong>, <strong>timeout aaa</strong>, and <strong>policy identity</strong> keywords and the <strong>identity-policy-name</strong> argument were added.</td>
</tr>
<tr>
<td>12.4(15)T</td>
<td>The following keywords and arguments were added: <strong>consent</strong>, <strong>absolute-timer</strong>, <strong>minutes</strong>, <strong>inactivity-time</strong>, <strong>minutes</strong>, <strong>parameter-map</strong>, and <strong>consent-parameter-map-name</strong>.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The admission rule defines how you apply admission control.

You can associate the named rule with an ACL, providing control over which hosts use the admission control feature. If no standard access list is defined, the named admission rule intercepts IP traffic from all hosts whose connection-initiating packets are received at the configured interface.

The **bypass** keyword allows an administrator the choice of not having to use the EAPoUDP-based posture validation for the hosts that are trying to connect on the port. The bypass can be used if an administrator knows that the hosts that are connected on the port do not have the Cisco Trust Agent client installed.

The **service-policy type tag** {**service-policy-name**} keywords and argument allow you to associate the service policy of the type tag with the IP admission rule. On the network access device (NAD), a set of policies can be associated with an arbitrary tag string, and if the AAA server sends the same tag in response to the posture validation or authentication response, the policies that are associated with the tag can be applied on the host. The **service policy** keyword is an optional keyword, and if the service policy is not associated with the IP admission name, the policies that are received from the AAA server are applied on the host.
The **list** keyword option allows you to apply a standard, extended (1 through 199) or named access list to a named admission control rule. IP connections that are initiated by hosts in the access list are intercepted by the admission control feature.

The **event** keyword option allows you to specify the condition that triggered application of an identity policy.

The **timeout aaa** keyword option specifies that the AAA server is unreachable, and this condition is triggering the application of an identity policy.

The **policy identity** keyword and the **identity-policy-name argument** allow you to configure application of an identity policy and specify the policy type to be applied while the AAA server is unreachable.

The **consent** keyword and the **parameter-map consent-parameter-map-name** keyword and argument allow you to associate the authentication proxy consent feature with an IP admission rule. The consent feature enables customers to display a consent webpage to an end user, providing access to wireless services only after the end user accepts the agreement.

### Examples

#### Tag and Template Feature Examples

The following example shows that an IP admission control rule is named "greentree" and that it is associated with ACL "101." Any IP traffic that is destined to a previously configured network (using the **access-list** command) will be subjected to antivirus state validation using EAPoUDP.

```
Router (config)# ip admission name greentree eapoudp list 101
```

The following example shows that EAPoUDP bypass has been configured:

```
Router (config)# ip admission name greentree eapoudp bypass list 101
```

In the following service policy example, tags named "healthy" and "non_healthy" can be received from an AAA server, the policy map is defined on the NAD, and the tag policy type is associated with the IP admission name "greentree."

```
Class Map Definition for the healthy class Type Tag

Router (config)# class-map type tag healthy_class
Router(config-cmap)# match tag healthy
Router(config-cmap)# end

Class Map Definition for the non_healthy_class Type Tag

Router (config)# class-map type tag non_healthy_class
Router (config-cmap)# match tag non_healthy
Router (config-cmap)# end

Policy Map Definition

! The following line will be associated with the IP admission name.
Router (config)# policy-map type control tag global_class
```
The following line refers to the healthy class map that was defined above.
Router (config-pmap)# class healthy_class
Router (config-pmap-c)# identity policy healthy_policy
Router (config-pmap-c)# exit

The following line refers to the non_healthy class that was defined above.
Router (config-pmap)# class non_healthy_class
Router (config-pmap-c)# identity policy non_healthy_policy
Router (config-pmap-c)# end

Identity Policy Definition

Router (config)# identity policy healthy_policy
! The following line is the IP access list for healthy users.
Router (config-identity-policy)# access-group healthy
Router (config-identity-policy)# end
Router (config)# identity policy non_healthy_policy
Router (config-identity-policy)# access-group non_healthy
Router (config-identity-policy)# end

Defining Access Lists

Router (config)# ip access-list extended healthy_class
! The following line can be anything, but as an example, traffic is being allowed.
Router (config-ext-nacl)# permit ip any any
Router (config-ext-nac)# end
Router (config)# ip access-list extended non_healthy_class
! The following line is only an example. In practical cases, you could prevent a user from accessing specific networks.
Router (config-ext-nacl)# deny ip any any
Router (config-ext-nac)# end

Associating the Policy Map with the IP Admission Name

Router (config)# ip admission name greentree service-policy type tag global_class
! In the next line, the admission name can be associated with the interface.
Router (config)# interface fastethernet 1/0
Router (config-if)# ip admission greentree

In the above configuration, if the AAA server sends a tag named "healthy" or "non_healthy" for any host, the policies that are associated with the appropriate identity policy will be applied on the host.

NAC--Auth Fail Open Feature Examples

The following example shows how to define an IP admission control rule named "samplerule" and attach it to a specific interface:

Router (config)# ip admission name samplerule eapoudp list 101 event timeout aaa policy identity aaa_fail_policy
Router (config)# interface fastethernet 1/1
Router (config-if)# ip admission samplerule
Router (config-if)# end

In the above configuration, if the specified interface is not already authorized when the AAA server becomes unreachable, it will operate under the specified policy until revalidation is possible.

**Authentication Proxy Consent Webpage Example**

The following example shows how to configure an IP admission consent rule and associate the consent rule with the definitions of the parameter map "consent_parameter_map":

```
ip admission name consent-rule consent inactivity-time 204 absolute-timer 304 parameter-map consent_parameter_map list 103
ip admission consent-banner file flash:consent_page.html
ip admission consent-banner text ^C Consen-Page-Banner-Text ^C
ip admission max-login-attempts 5
ip admission init-state-timer 15
ip admission auth-proxy-audit
ip admission inactivity-timer 205
ip admission absolute-timer 305
ip admission ratelimit 100
ip http server
ip http secure-server
!
```

```
interface FastEthernet 0/0
description ### CLIENT-N/W ###
ip address 192.168.100.170 255.255.255.0
ip access-group 102 in
ip admission consent-rule
no shut
exit
!
interface FastEthernet 0/1
description ### AAA-DHCP-AUDIT-SERVER-N/W ###
ip address 192.168.104.170 255.255.255.0
no shut
exit
!
line con 0
exec-timeout 0 0
login authentication noAAA
exit
!
line vty 0 15
exec-timeout 0 0
login authentication noAAA
exit
!
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Sets a primary or secondary IP address for an interface.</td>
</tr>
<tr>
<td>ip admission event timeout aaa policy identity</td>
<td>Defines a policy to be applied when the AAA server is unreachable.</td>
</tr>
</tbody>
</table>
**ip admission name bypass regex**

To configure browser-based authentication bypass on a Network Admission Control (NAC) rule, use the `ip admission name bypass regex` command in global configuration mode. To remove browser-based authentication bypass, use the `no` form of this command.

```
ip admission name administration-name bypass regex regex-map [absolute-timer minutes]
no ip admission name administration-name bypass
```

**Syntax Description**

- `administration-name`: Name of a NAC rule.
- `regex-map`: Regular expression (regex) parameter map with a regex pattern to enable bypass authentication for a web browser.
- `absolute-timer minutes`: (Optional) Specifies the maximum time, in minutes, before a browser session times out. The maximum time ranges from 0 to 35791. Default value for an authentication session is 0. Default value for an authentication bypass session is 60.

**Command Default**

Authentication is required for all browsers.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3(3)M</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `bypass regex regex-map` keyword and argument configures a regex pattern that can be compared to the user-agent field in the HTTP Get request to bypass authentication for a configured browser. This command defines the NAC policy to be applied to a network access device to bypass browser authentication.

The following example shows how to bypass browser authentication:

```
Device> enable
Device# configure terminal
Device(config)# ip admission name rule1 bypass regex regex-map1 absolute-timer 10
```
ip admission name http-basic

To create a basic HTTP authentication network admission control rule, use the `ip admission name http-basic` command in global configuration mode. To remove the network admission control rule, use the `no` form of this command.

```
ip admission name admission-name http-basic [passive] [absolute-timer minutes] [event timeout]
aaa policy identity identity-policy-name] [inactivity-time minutes] [list acl-list extended-acl-list acl-name]
{service-policy type tag service-policy-name]
```

no ip admission name admission-name http-basic

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admission-name</td>
<td>Name of the network admission control rule.</td>
</tr>
<tr>
<td>passive</td>
<td>(Optional) Specifies passive mode.</td>
</tr>
<tr>
<td>absolute-timer minutes</td>
<td>(Optional) Specifies the elapsed time, in minutes, before the external server time out. Valid values are from 0 to 35791. The default is 0.</td>
</tr>
<tr>
<td>event</td>
<td>(Optional) Specifies the event to be associated with a policy.</td>
</tr>
<tr>
<td>timeout</td>
<td>(Optional) Specifies timeout-based events.</td>
</tr>
<tr>
<td>aaa</td>
<td>(Optional) Specifies that the authentication, authorization, and accounting (AAA) server is unreachable.</td>
</tr>
<tr>
<td>policy identity</td>
<td>(Optional) Applies an identity policy to be used while the AAA server is unreachable.</td>
</tr>
<tr>
<td>identity-policy-name</td>
<td>(Optional) Name of the identity policy to be applied.</td>
</tr>
<tr>
<td>inactivity-time minutes</td>
<td>(Optional) Specifies the lapsed time, in minutes, before the external file server is deemed unreachable. Valid values are from 1 to 35791.</td>
</tr>
<tr>
<td>list</td>
<td>(Optional) Specifies an access control list (ACL) to apply to an authentication proxy.</td>
</tr>
<tr>
<td>acl-list</td>
<td>(Optional) Standard ACL number. Valid values are from 1 to 199.</td>
</tr>
<tr>
<td>extended-acl-list</td>
<td>(Optional) Expanded range of ACL numbers. Valid values are from 1300 to 2699.</td>
</tr>
<tr>
<td>acl-name</td>
<td>(Optional) ACL name.</td>
</tr>
<tr>
<td>service-policy</td>
<td>(Optional) Specifies a control plane service policy is to be configured.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Specifies the type of the service policy.</td>
</tr>
<tr>
<td>tag</td>
<td>(Optional) Specifies the tag-based service policy type.</td>
</tr>
<tr>
<td>service-policy-name</td>
<td>(Optional) Name of the control plane service policy. This service policy is used to apply actions on the host when a tag is received.</td>
</tr>
</tbody>
</table>

### Command Default

A basic HTTP authentication network admission control rule is not configured.
Command Modes
Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(1)T1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
When you configure the `ip admission name http-basic` command, client applications always prompt users to enter their credentials.

The absolute timeout value allows you to configure a time duration during which the authentication proxy on the enabled interface is active. After the absolute timer expires, the authentication proxy is disabled regardless of any activity. The absolute timeout value can be configured per protocol or globally. The default value of the absolute timeout is zero. Hence the absolute timer is disabled by default and the authentication proxy is enabled indefinitely.

The `timeout aaa` keywords specify that the AAA server is unreachable, and this condition triggers the application of an identity policy.

The `service-policy type tag service-policy-name` keywords and argument allow you to associate a service policy of the type tag with the IP admission rule. On the network access device (NAD), a set of policies can be associated with an arbitrary tag string, and if the AAA server sends the same tag in response to the posture validation or authentication response, the policies that are associated with the tag can be applied on the host. The `service policy` keyword is an optional keyword, and if the service policy is not associated with the IP admission name, the policies that are received from the AAA server are applied on the host.

Examples
The following example shows how to configure a basic HTTP network admission control rule:

```
Router(config)# ip admission name admission1 http-basic
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip address</code></td>
<td>Sets a primary or secondary IP address for an interface.</td>
</tr>
<tr>
<td><code>ip admission event timeout aaa policy</code></td>
<td>Defines a policy to be applied when the AAA server is unreachable.</td>
</tr>
<tr>
<td><code>ip admission event timeout aaa policy</code></td>
<td></td>
</tr>
</tbody>
</table>
**ip admission name method-list**

To create a list of authentication, authorization, and accounting (AAA) method network admission control rules, use the `ip admission name method-list` command in global configuration mode. To remove the network admission control rules, use the `no` form of this command.

```
ip admission name admission-name method-list [{accounting} [{authentication} [{authorization}]] [list-name|default]]
no ip admission name admission-name method-list
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admission-name</td>
<td>Name of the network admission control rule.</td>
</tr>
<tr>
<td>accounting</td>
<td>(Optional) Specifies the accounting method.</td>
</tr>
<tr>
<td>authentication</td>
<td>(Optional) Specifies the authentication method.</td>
</tr>
<tr>
<td>authorization</td>
<td>(Optional) Specifies the authorization method.</td>
</tr>
<tr>
<td>list-name</td>
<td>Method list name.</td>
</tr>
<tr>
<td>default</td>
<td>Specifies the default method list.</td>
</tr>
</tbody>
</table>

**Command Default**

A list of AAA method network admission control rules is not configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(T)1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ip admission name method-list accounting` command defines the reference to the accounting method list of service type auth-proxy or the network that is configured using the `aaa accounting auth-proxy` and `aaa accounting network` commands respectively.

The `ip admission name method-list authentication` command defines the reference to the authentication method list of service type login that is configured using the `aaa authentication login` command.

The `ip admission name method-list authorization` command defines the reference to the authorization method list of service type auth-proxy or the network that is configured using the `aaa authorization auth-proxy` and `aaa authorization network` commands respectively.

**Examples**

The following example shows how to create an accounting method network admission control rule:

```
Router(config)# ip admission name admission1 method-list accounting accounting-method
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>aaa accounting</strong></td>
<td>Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.</td>
</tr>
<tr>
<td><strong>aaa authentication login</strong></td>
<td>Sets AAA authentication at login.</td>
</tr>
<tr>
<td><strong>aaa authorization network</strong></td>
<td>Sets the parameters that restrict user access to a network.</td>
</tr>
<tr>
<td><strong>ip address</strong></td>
<td>Sets a primary or secondary IP address for an interface.</td>
</tr>
<tr>
<td><strong>ip admission event timeout aaa policy identity</strong></td>
<td>Defines a policy to be applied when the AAA server is unreachable.</td>
</tr>
</tbody>
</table>
To create a Windows network, NT LAN Manager (NTLM) authentication network admission control rule, use the `ip admission name ntlm` command in global configuration mode. To remove the network admission control rule, use the `no` form of this command.

```
ip admission name admission-name ntlm [{absolute-timer minutes}] [{event timeout aaa policy identity identity-policy-name}] [{list {acl-list extended-acl-list acl-name}}] [{service-policy type tag service-policy-name}] no ip admission name admission-name ntlm
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admission-name</td>
<td>Name of the network admission control rule.</td>
</tr>
<tr>
<td>absolute-timer minutes</td>
<td>(Optional) Specifies the elapsed time, in minutes, before the external server times out. Valid values are from 0 to 35791.</td>
</tr>
<tr>
<td>event</td>
<td>(Optional) Specifies the event to be associated with a policy.</td>
</tr>
<tr>
<td>timeout</td>
<td>(Optional) Specifies timeout-based events.</td>
</tr>
<tr>
<td>aaa</td>
<td>(Optional) Specifies that the authentication, authorization, and accounting (AAA) server is unreachable.</td>
</tr>
<tr>
<td>policy identity</td>
<td>(Optional) Applies an identity policy to be used while the AAA server is unreachable.</td>
</tr>
<tr>
<td>identity-policy-name</td>
<td>(Optional) Name of the identity policy to be applied.</td>
</tr>
<tr>
<td>list</td>
<td>(Optional) Specifies an access control list (ACL) to apply to an authentication proxy.</td>
</tr>
<tr>
<td>acl-list</td>
<td>(Optional) Standard ACL number. Valid values are from 1 to 199.</td>
</tr>
<tr>
<td>extended-acl-list</td>
<td>(Optional) Expanded range of ACL numbers. Valid values are from 1300 to 2699.</td>
</tr>
<tr>
<td>acl-name</td>
<td>(Optional) ACL name.</td>
</tr>
<tr>
<td>service-policy</td>
<td>(Optional) Specifies a control plane service policy is to be configured.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Specifies the type of the service policy.</td>
</tr>
<tr>
<td>tag</td>
<td>(Optional) Specifies the tag-based service policy type.</td>
</tr>
<tr>
<td>service-policy-name</td>
<td>(Optional) Name of the control plane service policy. This service policy is used to apply actions on the host when a tag is received.</td>
</tr>
</tbody>
</table>

**Command Default**

An NTLM Authentication network admission control rule is not configured.

**Command Modes**

Global configuration (config)
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(1)T1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

When you use the NTLM authentication method, the router tries to retrieve the user credentials transparently from the client application without prompting end users. If the client application cannot send user credentials transparently, it prompts users to enter their username and password.

The absolute timeout value allows you to configure a time duration during which the authentication proxy on the enabled interface is active. After the absolute timer expires, the authentication proxy is disabled regardless of any activity. The absolute timeout value can be configured per protocol or globally. The default value of the absolute timeout is zero. Hence the absolute timer is disabled by default and the authentication proxy is enabled indefinitely.

The `timeout aaa` keyword specifies that the AAA server is unreachable, and this condition triggers the application of an identity policy.

The `service-policy type tag service-policy-name` keywords and argument allow you to associate a service policy of the type tag with the IP admission rule. On the network access device (NAD), a set of policies can be associated with an arbitrary tag string, and if the AAA server sends the same tag in response to the posture validation or authentication response, the policies that are associated with the tag can be applied on the host. The `service policy` keyword is an optional keyword, and if the service policy is not associated with the IP admission name, the policies that are received from the AAA server are applied on the host.

Examples

The following example shows how to create an NTLM network admission control rule:

```
Router(config)# ip admission name admission1 ntlm
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Sets a primary or secondary IP address for an interface.</td>
</tr>
<tr>
<td>ip admission event timeout aaa policy identity</td>
<td>Defines a policy to be applied when the AAA server is unreachable.</td>
</tr>
</tbody>
</table>
**ip admission name order**

To create a fallback authentication order for the network admission control rule, use the `ip admission name order` command in global configuration mode. To remove the authentication order for the network admission control rule, use the `no` form of this command.

```
ip admission name admission-name order [{http-basic}] [{ntlm}] [{proxy-http}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admission-name</td>
<td>Name of the network admission control rule.</td>
</tr>
<tr>
<td>http-basic</td>
<td>(Optional) Specifies HTTP basic authentication.</td>
</tr>
<tr>
<td>ntlm</td>
<td>(Optional) Specifies Windows network, NT LAN Manager (NTLM) authentication.</td>
</tr>
<tr>
<td>proxy-http</td>
<td>(Optional) Specifies proxy HTTP authentication.</td>
</tr>
</tbody>
</table>

**Command Default**

A fallback authentication order for the network admission control rule is not configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(1)T1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to create an authentication order for a network admission control rule:

```
Router(config)# ip admission name admission1 order http-basic
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip admission name</code></td>
<td>Creates an authentication network admission control rule.</td>
</tr>
<tr>
<td><code>ip admission name http-basic</code></td>
<td>Creates a basic HTTP authentication network admission control rule.</td>
</tr>
<tr>
<td><code>ip admission name ntlm</code></td>
<td>Creates an NTLM authentication network admission control rule.</td>
</tr>
</tbody>
</table>
ip admission proxy http

To specify the display of custom authentication proxy web pages during web-based authentication, use the `ip admission proxy http` command in global configuration mode. To specify the use of the default web page, use the `no` form of this command.

```
ip admission proxy http {{login|success|failure|login expired} page file device:file-name|success redirect url}
no ip admission proxy http {{login|success|failure|login expired} page file device:file-name|success redirect url}
```

Cisco IOS Release 12.2(52)SG, 12.2SE, 15.2(1)E, and later releases

```
ip admission proxy http {{login|success|failure|login expired} page file device:file-name|success redirect url|refresh-all}
no ip admission proxy http {{login|success|failure|login expired} page file device:file-name|success redirect url|refresh-all}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>login</td>
<td>Specifies a locally stored web page to be displayed during login.</td>
</tr>
<tr>
<td>success</td>
<td>Specifies a locally stored web page to be displayed when the login is successful.</td>
</tr>
<tr>
<td>failure</td>
<td>Specifies a locally stored web page to be displayed when the login has failed.</td>
</tr>
<tr>
<td>login expired</td>
<td>Specifies a locally stored web page to be displayed when the login has expired.</td>
</tr>
<tr>
<td>device</td>
<td>Specifies a disk or flash memory in the switch memory file system where the custom HTML file is stored.</td>
</tr>
<tr>
<td>file-name</td>
<td>Specifies the name of the custom HTML file to be used in place of the default HTML file for the specified condition.</td>
</tr>
<tr>
<td><strong>success redirect url</strong></td>
<td>Specifies an external web page to be displayed when the login is successful.</td>
</tr>
<tr>
<td><strong>refresh-all</strong></td>
<td>Specifies the refresh of all custom HTML pages to reflect the updates made to the pages in the disk or flash memory in the switch memory file system.</td>
</tr>
</tbody>
</table>

**Note**: Effective with CSCt25327, the `refresh-all` keyword was introduced for Cisco IOS Release 12.2(52)SG, 12.2SE, 15.2(1)E, and later releases.

**Command Default**
The internal default authentication proxy web pages are displayed during web-based authentication.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SXI</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(52)SG</td>
<td>The <code>refresh-all</code> keyword was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

When configuring the use of customized authentication proxy web pages, consider the following guidelines:

• To enable the custom web pages feature, you must specify all four custom HTML files. If fewer than four files are specified, the internal default HTML pages will be used.

• The four custom HTML files must be present on the disk or flash of the switch. The maximum size of each HTML file is 8 KB.

• Any images on the custom pages must be located on an accessible HTTP server. An intercept ACL must be configured within the admission rule to allow access to the HTTP server.

• Any external link from a custom page will require configuration of an intercept ACL within the admission rule.

• Any name resolution required for external links or images will require configuration of an intercept ACL within the admission rule to access a valid DNS server.

• If the custom web pages feature is enabled, a configured auth-proxy-banner will not be used.

• If the custom web pages feature is enabled, the redirection URL for successful login feature will not be available.

• Because the custom login page is a public web form, consider the following guidelines for this page:
  • The login form must accept user input for the username and password and must POST the data as uname and pwd.
  • The custom login page should follow best practices for a web form, such as page timeout, hidden password, and prevention of redundant submissions.

• When configuring a redirection URL for successful login, consider the following guidelines:
  • If the custom authentication proxy web pages feature is enabled, the redirection URL feature is disabled and will not be available in the CLI. You can perform redirection in the custom login success page.
  • If the redirection URL feature is enabled, a configured auth-proxy-banner will not be used.

• Effective with CSCtj25327, when a custom HTML page is replaced with a new page with the exact same name in the disk or flash memory in the switch memory file system, use the ip admission proxy http refresh-all command to refresh the custom HTML pages and view the new pages.

Examples

The following example shows how to configure custom authentication proxy web pages:

Device(config)# ip admission proxy http login page file disk1:login.htm
Device(config)# ip admission proxy http success page file disk1:success.htm
Device(config)# ip admission proxy http fail page file disk1:fail.htm
Device(config)# ip admission proxy http login expired page file disk1:expired.htm

The following example shows how to verify the configuration of custom authentication proxy web pages:

Device# show ip admission configuration

Authentication proxy webpage
 Login page : disk1:login.htm
 Success page : disk1:success.htm
 Fail Page : disk1:fail.htm
The following example shows how to configure a redirection URL for successful login:

```
Device(config)# ip admission proxy http success redirect www.example.com
```

The following example shows how to verify the redirection URL for successful login:

```
Device# show ip admission configuration
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip http server ip https server</td>
<td>Enables the HTTP server within the switch.</td>
</tr>
<tr>
<td></td>
<td>show ip admission configuration</td>
<td>Displays the configuration of web-based authentication ip admission.</td>
</tr>
</tbody>
</table>
ip admission virtual-ip

To configure a web-based proxy authentication virtual IP address, use the `ip admission virtual-ip` command in global configuration mode. To remove the address, use the `no` form of this command.

```
ip admission virtual-ip ip-address [virtual-host host-name]
oip admission virtual-ip ip-address [virtual-host host-name]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>Virtual IP address.</td>
</tr>
<tr>
<td><code>virtual-host ip-address</code></td>
<td>(Optional) Specifies the name of the virtual host to connect to.</td>
</tr>
</tbody>
</table>

**Command Default**

A web-based proxy authentication virtual IP address is not configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.4(2)T</td>
<td>This command was modified. The <code>virtual-host host-name</code> keyword and argument pair was added in a release prior to Cisco IOS Release 15.4(2)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A virtual IP address is used only in communication between the Cisco IOS HTTP authentication and clients. For the web-based proxy authentication to operate you must set the virtual IP address, and no other device on the network can have the same IP address as the virtual IP address.

**Examples**

The following example shows how to configure the web-based proxy authentication virtual IP address:

```
Device(config)# ip admission virtual-ip 10.1.1.1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>content-scan out</td>
<td>Enables content scanning on an egress interface.</td>
</tr>
</tbody>
</table>
ip audit

To apply an audit specification created with the `ip audit` command to a specific interface and for a specific direction, use the `ip audit` command in interface configuration mode. To disable auditing of the interface for the specified direction, use the `no` version of this command.

```
ip audit audit-name {in|out}
no ip audit audit-name {in|out}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>audit-name</code></td>
<td>Name of an audit specification.</td>
</tr>
<tr>
<td><code>in</code></td>
<td>Inbound traffic.</td>
</tr>
<tr>
<td><code>out</code></td>
<td>Outbound traffic.</td>
</tr>
</tbody>
</table>

**Command Default**

No audit specifications are applied to an interface or direction.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.28(SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ip audit` interface configuration command to apply an audit specification created with the `ip audit` command to a specific interface and for a specific direction.

**Examples**

In the following example, the audit specification MARCUS is applied to an interface and direction:

```
interface e0
  ip audit MARCUS in
```

In the following example, the audit specification MARCUS is removed from the interface on which it was previously added:

```
interface e0
  no ip audit MARCUS in
```
ip audit attack

To specify the default actions for attack signatures, use the `ip audit attack` command in global configuration mode. To set the default action for attack signatures, use the `no` form of this command.

```
ip audit attack action [alarm] [drop] [reset]
no ip audit attack
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>Specifies an action for the attack signature to take in response to a match.</td>
</tr>
<tr>
<td>alarm</td>
<td>(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Used with the <code>action</code> keyword.</td>
</tr>
<tr>
<td>drop</td>
<td>(Optional) Drops the packet. Used with the <code>action</code> keyword.</td>
</tr>
<tr>
<td>reset</td>
<td>(Optional) Resets the TCP session. Used with the <code>action</code> keyword.</td>
</tr>
</tbody>
</table>

### Command Default

The default action is `alarm`.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `ip audit attack` global configuration command to specify the default actions for attack signatures.

### Examples

In the following example, the default action for attack signatures is set to all three actions:

```
ip audit attack action alarm drop reset
```
ip audit info

To specify the default actions for info signatures, use the ip audit info command in global configuration mode. To set the default action for info signatures, use the no form of this command.

```
ip audit info action [alarm] [drop] [reset]
no ip audit info
```

**Syntax Description**

<table>
<thead>
<tr>
<th>action</th>
<th>Sets an action for the info signature to take in response to a match.</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarm</td>
<td>(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Used with the action keyword.</td>
</tr>
<tr>
<td>drop</td>
<td>(Optional) Drops the packet. Used with the action keyword.</td>
</tr>
<tr>
<td>reset</td>
<td>(Optional) Resets the TCP session. Used with the action keyword.</td>
</tr>
</tbody>
</table>

**Command Default**

The default action is alarm.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the ip audit info global configuration command to specify the default actions for info signatures.

**Examples**

In the following example, the default action for info signatures is set to all three actions:

```
ip audit info action alarm drop reset
```
# ip audit name

To create audit rules for info and attack signature types, use the `ip audit name` command in global configuration mode. To delete an audit rule, use the `no` form of this command.

```
ip audit name audit-name {info|attack} [list standard-acl] [action [alarm] [drop] [reset]]
o no ip audit name audit-name {info|attack}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>audit-name</td>
<td>Name for an audit specification.</td>
</tr>
<tr>
<td>info</td>
<td>Specifies that the audit rule is for info signatures.</td>
</tr>
<tr>
<td>attack</td>
<td>Specifies that the audit rule is for attack signatures.</td>
</tr>
<tr>
<td>list</td>
<td>(Optional) Specifies an ACL to attach to the audit rule.</td>
</tr>
<tr>
<td>standard-acl</td>
<td>(Optional) Integer representing an access control list. Use with the <code>list</code> keyword.</td>
</tr>
<tr>
<td>action</td>
<td>(Optional) Specifies an action or actions to take in response to a match.</td>
</tr>
<tr>
<td>alarm</td>
<td>(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Use with the <code>action</code> keyword.</td>
</tr>
<tr>
<td>drop</td>
<td>(Optional) Drops the packet. Use with the <code>action</code> keyword.</td>
</tr>
<tr>
<td>reset</td>
<td>(Optional) Resets the TCP session. Use with the <code>action</code> keyword.</td>
</tr>
</tbody>
</table>

## Command Default

If an action is not specified, the default action is `alarm`.

## Command Modes

Global configuration

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

Any signatures disabled with the `ip audit signature` command do not become a part of the audit rule created with the `ip audit name` command.

## Examples

In the following example, an audit rule called INFO.2 is created, and configured with all three actions:

```
ip audit name INFO.2 info action alarm drop reset
```

In the following example, an info signature is disabled and an audit rule called INFO.3 is created:
ip audit signature 1000 disable
ip audit name INFO.3 info action alarm drop reset

In the following example, an audit rule called ATTACK.2 is created with an attached ACL 91, and the ACL is created:

ip audit name ATTACK.2 list 91
access-list 91 deny 10.1.0.0 0.0.255.255
access-list 91 permit any
To specify the method of event notification, use the `ip audit notify` command in global configuration mode. To disable event notifications, use the `no` form of this command.

```
ip audit notify {nr-director|log}
no ip audit notify {nr-director|log}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>nr-director</code></td>
<td>Send messages in NetRanger format to the NetRanger Director or Sensor.</td>
</tr>
<tr>
<td><code>log</code></td>
<td>Send messages in syslog format.</td>
</tr>
</tbody>
</table>

### Command Default

The default is to send messages in syslog format.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If messages are sent to the NetRanger Director, then you must also configure the NetRanger Director’s Post Office transport parameters using the `ip audit po remote` command.

### Examples

In the following example, event notifications are specified to be sent in NetRanger format:

```
ip audit notify nr-director
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip audit po local</code></td>
<td>Specifies the local Post Office parameters used when sending event notifications to the NetRanger Director.</td>
</tr>
<tr>
<td><code>ip audit po remote</code></td>
<td>Specifies one or more sets of Post Office parameters for NetRanger Directors receiving event notifications from the router.</td>
</tr>
</tbody>
</table>
**ip audit po local**

To specify the local Post Office parameters used when sending event notifications to the NetRanger Director, use the `ip audit po local` command in global configuration mode. To set the local Post Office parameters to their default settings, use the `no` form of this command.

```
ip audit po local hostid id-number orgid id-number
no ip audit po local [hostid id-number orgid id-number]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostid</td>
<td>Specifies a NetRanger host ID.</td>
</tr>
<tr>
<td>id-number</td>
<td>Unique integer in the range 1 to 65535 used in NetRanger communications to identify the local host. The default host ID is 1.</td>
</tr>
<tr>
<td>orgid</td>
<td>Specifies a NetRanger organization ID.</td>
</tr>
<tr>
<td>id-number</td>
<td>Unique integer in the range 1 to 65535 used in NetRanger communications to identify the group to which the local host belongs. The default organization ID is 1.</td>
</tr>
</tbody>
</table>

**Command Default**
The default organization ID is 1. The default host ID is 1.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `ip audit po local` global configuration command to specify the local Post Office parameters used when sending event notifications to the NetRanger Director.

**Examples**

In the following example, the local host is assigned a host ID of 10 and an organization ID of 500:

```
ip audit po local hostid 10 orgid 500
```
**ip audit po max-events**

To specify the maximum number of event notifications that are placed in the router’s event queue, use the `ip audit po max-events` command in global configuration mode. To set the number of recipients to the default setting, use the `no` version of this command.

```
ip audit po max-events number-of-events
no ip audit po max-events
```

**Syntax Description**

| number-of-events | Integer in the range from 1 to 65535 that designates the maximum number of events allowable in the event queue. The default is 100 events. |

**Command Default**
The default number of events is 100.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Raising the number of events past 100 may cause memory and performance impacts because each event in the event queue requires 32 KB of memory.

**Examples**

In the following example, the number of events in the event queue is set to 250:

```
ip audit po max-events 250
```
**ip audit po protected**

To specify whether an address is on a protected network, use the `ip audit po protected` command in global configuration mode. To remove network addresses from the protected network list, use the `no` form of this command.

```
ip audit po protected ip-addr [to ip-addr]
no ip audit po protected [ip-addr]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-addr</td>
<td>IP address of a network host.</td>
</tr>
<tr>
<td>to ip-addr</td>
<td>(Optional) Specifies a range of IP addresses.</td>
</tr>
</tbody>
</table>

**Command Default**

If no addresses are defined as protected, then all addresses are considered outside the protected network.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.33SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can enter a single address at a time or a range of addresses at a time. You can also make as many entries to the protected networks list as you want. When an attack is detected, the corresponding event contains a flag that denotes whether the source or destination of the packet belongs to a protected network or not. If you specify an IP address for removal, that address is removed from the list. If you do not specify an address, then all IP addresses are removed from the list.

**Examples**

In the following example, a range of addresses is added to the protected network list:

```
ip audit po protected 10.1.1.0 to 10.1.1.255
```

In the following example, three individual addresses are added to the protected network list:

```
ip audit po protected 10.4.1.1
ip audit po protected 10.4.1.8
ip audit po protected 10.4.1.25
```

In the following example, an address is removed from the protected network list:

```
no ip audit po protected 10.4.1.1
```
ip audit po remote

To specify one or more set of Post Office parameters for NetRanger Directors receiving event notifications from the router, use the **ip audit po remote** global configuration command. To remove a NetRanger Director’s Post Office parameters as defined by host ID, organization ID, and IP address, use the *no* form of this command.

**ip audit po remote hostid** host-id **orgid** org-id **rmtaddress** ip-address **localaddress** ip-address 
[**port** port-number] [**preference** preference-number] [**timeout** seconds] [**application** {director|logger;] 
**no ip audit po remote hostid** host-id **orgid** org-id **rmtaddress** ip-address

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host-id</td>
<td>Unique integer in the range from 1 to 65535 used in NetRanger communications to identify the local host. Use with the <strong>hostid</strong> keyword.</td>
</tr>
<tr>
<td>hostid</td>
<td>Specifies a NetRanger host ID.</td>
</tr>
<tr>
<td>org-id</td>
<td>Unique integer in the range from 1 to 65535 used in NetRanger communications to identify the group in which the local host belongs. Use with the <strong>orgid</strong> keyword.</td>
</tr>
<tr>
<td>orgid</td>
<td>Specifies a NetRanger organization ID.</td>
</tr>
<tr>
<td>rmtaddress</td>
<td>Specifies the IP address of the NetRanger Director.</td>
</tr>
<tr>
<td>localaddress</td>
<td>Specifies the IP address of the Cisco IOS Firewall IDS router.</td>
</tr>
<tr>
<td>ip-address</td>
<td>IP address of the NetRanger Director or Cisco IOS Firewall IDS router’s interface. Use with the <strong>rmtaddress</strong> and <strong>localaddress</strong> keywords.</td>
</tr>
<tr>
<td>port-number</td>
<td>(Optional) Integer representing the UDP port on which the NetRanger Director is listening for event notifications. Use with the <strong>port</strong> keyword.</td>
</tr>
<tr>
<td>port</td>
<td>(Optional) Specifies a User Datagram Protocol port through which to send messages.</td>
</tr>
<tr>
<td>preference</td>
<td>(Optional) Specifies a route preference for communication.</td>
</tr>
<tr>
<td>preference-number</td>
<td>(Optional) Integer representing the relative priority of a route to a NetRanger Director, if more than one route exists. Use with the <strong>preference</strong> keyword.</td>
</tr>
<tr>
<td>seconds</td>
<td>(Optional) Integer representing the heartbeat timeout value for Post Office communications. Use with the <strong>timeout</strong> keyword.</td>
</tr>
<tr>
<td>timeout</td>
<td>(Optional) Specifies a timeout value for Post Office communications.</td>
</tr>
<tr>
<td>application</td>
<td>(Optional) Specifies the type of application that is receiving the Cisco IOS Firewall IDS messages.</td>
</tr>
<tr>
<td>director</td>
<td>(Optional) Specifies that the receiving application is the NetRanger Director interface.</td>
</tr>
<tr>
<td>logger</td>
<td>(Optional) Specifies that the receiving application is a NetRanger Sensor.</td>
</tr>
</tbody>
</table>

### Command Default

The default organization ID is 1.
The default host ID is 1.
The default UDP port number is 45000.
The default preference is 1.
The default heartbeat timeout is 5 seconds.
The default application is director.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.33SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A router can report to more than one NetRanger Director. In this case, use the **ip audit po remote** command to add each NetRanger Director to which the router sends notifications.

More than one route can be established to the same NetRanger Director. In this case, you must give each route a preference number that establishes the relative priority of routes. The router always attempts to use the lowest numbered route, switching automatically to the next higher number when a route fails, and then switching back when the route begins functioning again.

A router can also report to a NetRanger Sensor. In this case, use the **ip audit po remote** command and specify **logger** as the application.

**Examples**

In the following example, two communication routes for the same dual-homed NetRanger Director are defined:

```
ip audit po remote hostid 30 orgid 500 rmtaddress 10.1.99.100 localaddress 10.1.99.1 preference 1
ip audit po remote hostid 30 orgid 500 rmtaddress 10.1.4.30 localaddress 10.1.4.1 preference 2
```

The router uses the first entry to establish communication with the NetRanger Director defined with host ID 30 and organization ID 500. If this route fails, then the router will switch to the secondary communications route. As soon as the first route begins functioning again, the router switches back to the primary route and closes the secondary route.

In the following example, a different Director is assigned a longer heartbeat timeout value because of network congestion, and is designated as a logger application:

```
ip audit po remote hostid 70 orgid 500 rmtaddress 10.1.8.1 localaddress 10.1.8.100 timeout 10 application director
```
**ip audit signature**

To attach a policy to a signature, use the `ip audit signature` command in global configuration mode. To remove the policy, use the `no` form of this command. If the policy disabled a signature, then the `no` form of this command reenables the signature. If the policy attached an access list to the signature, the `no` form of this command removes the access list.

```
ip audit signature signature-id {disable|list acl-list}
no ip audit signature signature-id
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>signature-id</td>
<td>Unique integer specifying a signature as defined in the NetRanger Network Security Database.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the ACL associated with the signature.</td>
</tr>
<tr>
<td>list</td>
<td>Specifies an ACL to associate with the signature.</td>
</tr>
<tr>
<td>acl-list</td>
<td>Unique integer specifying a configured ACL on the router. Use with the <code>list</code> keyword.</td>
</tr>
</tbody>
</table>

**Command Default**

No policy is attached to a signature.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command allow you to set two policies: disable the audit of a signature or qualify the audit of a signature with an access list.

If you are attaching an access control list to a signature, then you also need to create an audit rule with the `ip audit name` command and apply it to an interface with the `ip audit` command.

**Examples**

In the following example, a signature is disabled, another signature has ACL 99 attached to it, and ACL 99 is defined:

```
ip audit signature 6150 disable
ip audit signature 1000 list 99
access-list 99 deny 10.1.10.0 0.0.0.255
access-list 99 permit any
```
ip audit smtp

To specify the number of recipients in a mail message over which a spam attack is suspected, use the ip audit smtp command in global configuration mode. To set the number of recipients to the default setting, use the no form of this command.

```
ip audit smtp spam number-of-recipients
no ip audit smtp spam
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spam</td>
<td>Specifies a threshold beyond which the Cisco IOS Firewall IDS alarms on spam e-mail.</td>
</tr>
<tr>
<td>number-of-recipients</td>
<td>Integer in the range of 1 to 65535 that designates the maximum number of recipients in a mail message before a spam attack is suspected. Use with the spam keyword. The default is 250 recipients.</td>
</tr>
</tbody>
</table>

**Command Default**

The default number of recipients is 250.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the ip audit smtp global configuration command to specify the number of recipients in a mail message over which a spam attack is suspected.

**Examples**

In the following example, the number of recipients is set to 300:

```
ip audit smtp spam 300
```
**ip auth-proxy (global configuration)**

To set the the authentication proxy idle timeout or maximum number of idle connections, use the `ip auth-proxy` command in global configuration mode. To return the idle timeout or maximum number of idle connections to their default values, use the `no` form of this command.

**ip auth-proxy** `{absolute-timer min|inactivity-timer min|init-state-timer min|max-nodata-conns number}`

**no ip auth-proxy** `{absolute-timer|inactivity-timer|init-state-timer|max-nodata-conns}`

| Syntax Description | absolute-timer min | Length of time in minutes that an ingress IP authentication proxy session can remain active. After this timer expires, each session must go through the entire process of establishing its connection as if it was a new request.

The range is 0 to 35,791. The default is 0.

| | inactivity-timer min | Length of time in minutes that an active ingress session can be present with no activity or data from the end client. If this timer expires without activity or data, the session is cleared.

The range is 1 to 2,147,483,647. The default is 60.

**Note** This keyword and argument pair replaces the auth-cache-time min keyword and argument pair.

| | init-state-timer min | Length of time in minutes that an ingress authentication proxy session can stay in the INIT state. An ingress session is first registered in the INIT state until the user enters their username and password credentials. If the timer expires before the credentials are entered, the session is removed.

The range is 1 to 15. The default is 2.

| | max-nodata-conns number | Maximum number of idle ("no data") TCP connections that can exist globally for the IP authentication feature.

The range is 1 to 1,000. The default is 3.

**Command Default**

The absolute timer is enabled indefinitely. The inactivity timer, and the INIT state timer are enabled. The limit on the number of global idle TCP connections is enabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(1)</td>
<td>The <em>inactivity-timer</em> and <em>absolute-timer</em> keywords were added.</td>
</tr>
<tr>
<td>12.4(6)T</td>
<td>The <em>init-state-timer</em> keyword was added</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
**Modification/Release**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You use the `ip auth-proxy` command to set the global idle timeout value for the authentication proxy. The idle timeout value is the length of time an authentication cache entry, along with its associated dynamic user access control list, is cleared after a period of inactivity.

You use the `absolute-timer` keyword to configure the length of time during which the authentication proxy on the enabled interface is active. After the absolute timer expires, the authentication proxy is disabled regardless of any activity. You can override the global absolute timeout value with the local (per protocol) value, which you can enable by using the `ip auth-proxy name` command. The absolute timer is turned off by default, and the authentication proxy is enabled indefinitely.

You must set the value of the `inactivity-timer` keyword to a higher value than the idle timeout of any Context-Based Access Control (CBAC) protocols. Otherwise, when the authentication proxy removes the user profile (and its associated dynamic user ACLs), there might be idle connections monitored by CBAC. Removing these user-specific ACLs could cause those idle connections to hang. If the CBAC idle timeout value is shorter, CBAC resets these connections when the CBAC idle timeout expires, which is before the authentication proxy removes the user profile.

You use the `init-state-timer` keyword to configure the amount of time that the authentication proxy is allowed to clear connections that are in the INIT state. Authentication attempts can remain in the INIT state when the router is loaded heavily and the authentication is not completed in two minutes. This problem is more likely if HTTPS is used for authenticating users. The default value of two minutes is usually sufficient to handle most cases, but if not, you should use the `init-state-timer` keyword to increase this value.

You use the `max-nodata-conns` keyword to limit the number of idle TCP connections (TCP sessions that are active but do not transmit data for a long period of time). There is no timer associated with this number.

**Examples**

The following example sets the inactivity timer to 30 minutes:

```shell
Router> enable
Router# configure terminal
Router(config)# ip auth-proxy inactivity-timer 30
```

The following example sets the INIT state timer to 15 minutes:

```shell
Router> enable
Router# configure terminal
Router(config)# ip auth-proxy init-state-timer 15
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip auth-proxy name</code></td>
<td>Creates an authentication proxy rule.</td>
</tr>
<tr>
<td><code>show ip auth-proxy configuration</code></td>
<td>Displays the authentication proxy entries or the running authentication proxy configuration.</td>
</tr>
</tbody>
</table>
ip auth-proxy (interface configuration)

To apply an authentication proxy rule at a firewall interface, use the `ip auth-proxy` command in interface configuration mode. To remove the authentication proxy rules, use the `no` form of this command.

```
ip auth-proxy auth-proxy-name
no ip auth-proxy auth-proxy-name
```

**Syntax Description**

| auth-proxy-name | Specifies the name of the authentication proxy rule to apply to the interface configuration. The authentication proxy rule is established with the `ip auth-proxy name` command. |

**Command Default**

No default behavior or values.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ip auth-proxy` command to enable the named authentication proxy rule at the firewall interface. Traffic passing through the interface from hosts with an IP address matching the standard access list and protocol type (HTTP) is intercepted for authentication if no corresponding authentication cache entry exists. If no access list is defined, the authentication proxy intercepts traffic from all hosts whose connection initiating packets are received at the configured interface.

Use the `no` form of this command with a rule name to disable the authentication proxy for a given rule on a specific interface. If a rule is not specified, the `no` form of this command disables the authentication proxy on the interface.

**Examples**

The following example configures interface Ethernet0 with the HQ_users rule:

```
interface e0
ip address 172.21.127.210 255.255.255.0
ip access-group 111 in
ip auth-proxy HQ_users
ip nat inside
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip auth-proxy name</code></td>
<td>Creates an authentication proxy rule.</td>
</tr>
</tbody>
</table>
ip auth-proxy auth-proxy-banner

To display a banner, such as the router name, in the authentication proxy login page, use the `ip auth-proxy auth-proxy-banner` command in global configuration mode. To disable display of the banner, use the `no` form of this command.

```
ip auth-proxy auth-proxy-banner {ftp|http|telnet} [banner-text]
no ip auth-proxy auth-proxy-banner {ftp|http|telnet}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp</td>
<td>Specifies the FTP protocol.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies the HTTP protocol.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies the Telnet protocol.</td>
</tr>
<tr>
<td>banner-text</td>
<td>(Optional) Specifies a text string to replace the default banner, which is the name of the router. The text string should be written in the following format: “C banner-text C,” where “C” is a delimiting character.</td>
</tr>
</tbody>
</table>

**Command Default**

This command is not enabled, and a banner is not displayed on the authentication proxy login page.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(1)</td>
<td>The following keywords were added: ftp, http, and telnet.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ip auth-proxy auth-proxy-banner` command allows users to configure one of two possible scenarios:

- The `ip auth-proxy auth-proxy-banner` command is enabled.
  
  In this scenario, the administrator has not supplied any text. Thus, a default banner that states the following: “Cisco Systems, <router’s hostname> Authentication” will be displayed in the authentication proxy login page. This scenario is most commonly used.

- The `ip auth-proxy auth-proxy-banner` command with the `banner-text` argument is enabled.
  
  In this scenario, the administrator can supply multiline text that will be converted to HTML by the auth-proxy parser code. Thus, only the multiline text will displayed in the authentication proxy login page. You will not see the default banner, “Cisco Systems, <router’s hostname> Authentication.”
If the `ip auth-proxy auth-proxy-banner` command is not enabled, there will not be any banner configuration. Thus, nothing will be displayed to the user on authentication proxy login page except a text box to enter the username and a text box to enter the password.

### Examples

The following example causes the router name to be displayed in the authentication proxy login page:

```
ip auth-proxy auth-proxy-banner ftp
```

The following example shows how to specify the custom banner “whozat” to be displayed in the authentication proxy login page:

```
ip auth-proxy auth-proxy-banner telnet CwhozatC
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip auth-proxy name</td>
<td>Creates an authentication proxy rule.</td>
</tr>
</tbody>
</table>
**ip auth-proxy max-login-attempts**

To limit the number of login attempts at a firewall interface in the interface configuration command mode, use the `ip auth-proxy max-login-attempts` command. Use the `no` form of this command to return to the default settings.

```
ip auth-proxy max-login-attempts number
no ip auth-proxy max-login-attempts
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Maximum number of login attempts. The range is 1 to 100. The default value depends on the authentication mechanism:</td>
</tr>
<tr>
<td></td>
<td>• FTP: 5</td>
</tr>
<tr>
<td></td>
<td>• HTTP: 30</td>
</tr>
<tr>
<td></td>
<td>• Telnet: 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Enabled</th>
</tr>
</thead>
</table>

| Command Modes     | Interface configuration |

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td></td>
<td>12.2SE</td>
<td>This command was modified. The maximum number of login attempts was changed to 100.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only. This command is supported on the firewall interfaces only.

The maximum login attempt functionality is independent of the watch-list feature (you create a watch list with the `ip access-list hardware permit fragments` command). If you do not configure a watch list, the existing authentication proxy behavior occurs, but it displays the new number for retries. If you configure a watch list, when the maximum is reached, the session is blocked and the IP address is put in the watch list.

**Examples**

This example shows how to set a limit to the number of login attempts at a firewall interface:

```
Router> enable
Router# configure terminal
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip auth-proxy max-login-attempts 4
Router(config-if)# end
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip auth-proxy watch-list</td>
<td>Deletes a single watch-list entry or all watch-list entries.</td>
</tr>
<tr>
<td>ip auth-proxy watch-list</td>
<td>Enables and configures an authentication proxy watch list.</td>
</tr>
<tr>
<td>show ip auth-proxy watch-list</td>
<td>Displays the information about the authentication proxy watch list.</td>
</tr>
</tbody>
</table>
**ip auth-proxy name**

To create an authentication proxy rule, use the ip auth-proxy name command in global configuration mode. To remove the authentication proxy rules, use the no form of this command.

**Cisco IOS 12.4(6)T and Later Releases**

```
ip auth-proxy name auth-proxy-name {ftp|http|telnet} [event timeout aaa policy identity id-policy-name] [absolute-timer timeout] [auth-cache-time timeout] [inactivity-time timeout] [list {list-num [service-policy type tag policy-name|std-list-num list-name]}] [service-policy type tag service-policy-name]
```

```
no ip auth-proxy name auth-proxy-name {ftp|http|telnet}
```

**Cisco IOS Release 12.2(33)SRA, 12.2SX, and Later Releases**

```
ip auth-proxy name auth-proxy-name {ftp|http|telnet} [event timeout aaa policy identity id-policy-name] [absolute-timer timeout] [auth-cache-time timeout] [inactivity-time timeout] [list {list-num [service-policy type tag policy-name|std-list-num list-name]}]
```

```
no ip auth-proxy name auth-proxy-name {ftp|http|telnet}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>auth-proxy-name</strong></td>
<td>A name of up to 16 alphanumeric characters to be associated with an authentication proxy rule.</td>
</tr>
<tr>
<td><strong>ftp</strong></td>
<td>Specifies FTP to trigger the authentication proxy.</td>
</tr>
<tr>
<td><strong>http</strong></td>
<td>Specifies HTTP to trigger the authentication proxy.</td>
</tr>
<tr>
<td><strong>telnet</strong></td>
<td>Specifies Telnet to trigger the authentication proxy.</td>
</tr>
<tr>
<td><strong>event timeout aaa policy identity id-policy-name</strong></td>
<td>(Optional) Specifies the event to be associated with the policy, timeout of the based event, AAA fail policy to be applied, Identity fail policy to be applied, and Identity policy name.</td>
</tr>
<tr>
<td><strong>absolute-timer timeout</strong></td>
<td>(Optional) Specifies a window in which the authentication proxy on the enabled interface is active. Enter a value in the range 0 to 35791 minutes. The default value is 0 minutes.</td>
</tr>
<tr>
<td><strong>auth-cache-time timeout</strong></td>
<td>(Optional) Alias of inactivity timeout in minutes. Enter a value in the range 1 to 35791 minutes.</td>
</tr>
<tr>
<td><strong>inactivity-time min</strong></td>
<td>(Optional) Overrides the global authentication proxy cache timer for a specific authentication proxy name, offering more control over timeout values. Enter a value in the range 1 to 35791 minutes. The default value is equal to the value set with the ip auth-proxy command.</td>
</tr>
<tr>
<td>**list {list-num</td>
<td>std-list-num</td>
</tr>
</tbody>
</table>

**Note**: This option deprecates the auth-cache-time timeout option.
A control plane service policy is to be configured.

Control plane tags service policy that is configured using the policy-map type control tag policy-map-name command. This policy map is used to apply the actions on the host when a tag is received.

Command Default

The default value is equal to the value set with the `ip auth-proxy auth-cache-time` command.

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2</td>
<td>Support for named and extend access lists was introduced.</td>
</tr>
<tr>
<td>12.3(1)</td>
<td>The following keywords were introduced:</td>
</tr>
<tr>
<td></td>
<td>• <code>ftp</code></td>
</tr>
<tr>
<td></td>
<td>• <code>telnet</code></td>
</tr>
<tr>
<td></td>
<td>• <code>inactivity-time timeout</code></td>
</tr>
<tr>
<td></td>
<td>• <code>absolute-timer timeout</code></td>
</tr>
<tr>
<td>12.4(6)T</td>
<td>The <code>service-policy type tag</code> keywords and <code>service-policy-name</code> argument were added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The <code>event</code>, <code>timeout</code>, <code>aaa</code>, <code>policy</code>, <code>identity</code> keywords and the <code>id-policy-name</code> argument were added.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command creates a named authentication proxy rule, and it allows you to associate that rule with an access control list (ACL), providing control over which hosts use the authentication proxy. The rule is applied to an interface on a router using the `ip auth-proxy` command.

Use the `inactivity-time timeout` option to override the global the authentication proxy cache timer. This option provides control over timeout values for specific authentication proxy rules. The authentication proxy cache timer monitors the length of time (in minutes) that an authentication cache entry, along with its associated dynamic user access control list, is managed after a period of inactivity. When that period of inactivity (idle time) expires, the authentication entry and the associated dynamic access lists are deleted.

Use the `list` option to associate a set of specific IP addresses or a named ACL with the `ip auth-proxy name` command.

Use the `no` form of this command with a rule name to remove the authentication proxy rules. If no rule is specified, the `no` form of this command removes all the authentication rules on the router, and disables the proxy at all interfaces.
You must use the `aaa authorization auth-proxy` command with the `ip auth-proxy name` command. Together these commands set up the authorization policy to be retrieved by the firewall. Refer to the `aaa authorization auth-proxy` command for more information.

### Examples

The following example shows how to create the HQ_users authentication proxy rule. Because an access list is not specified in the rule, all connection-initiating HTTP traffic is subjected to authentication.

```bash
ip auth-proxy name HQ_users http
```

The following example shows how to create the Mfg_users authentication proxy rule and apply it to hosts specified in ACL 10:

```bash
access-list 10 192.168.7.0 0.0.0.255
ip auth-proxy name Mfg_users http list 10
```

The following example shows how to set the timeout value for Mfg_users to 30 minutes:

```bash
access-list 15 any
ip auth-proxy name Mfg_users http inactivity-timer 30 list 15
```

The following example shows how to disable the Mfg_users rule:

```bash
no ip auth-proxy name Mfg_users
```

The following example shows how to disable the authentication proxy at all interfaces and remove all the rules from the router configuration:

```bash
no ip auth-proxy xyz ftp
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa authorization</code></td>
<td>Sets parameters that restrict network access to a user.</td>
</tr>
<tr>
<td><code>ip auth-proxy (global)</code></td>
<td>Sets the authentication proxy idle timeout value (that is, the length of time an authentication cache entry, along with its associated dynamic user ACL, is managed after a period of inactivity).</td>
</tr>
<tr>
<td><code>ip auth-proxy (interface)</code></td>
<td>Applies an authentication proxy rule at a firewall interface.</td>
</tr>
<tr>
<td><code>show ip auth-proxy configuration</code></td>
<td>Displays the authentication proxy entries or the running authentication proxy configuration.</td>
</tr>
</tbody>
</table>
ip auth-proxy watch-list

To enable and configure an authentication proxy watch list in the interface configuration command mode, use the `ip auth-proxy watch-list` command. To disable the watch-list functionality, remove an IP address from the watch list. Or, to return to the default setting, use the `no` form of this command.

```
ip auth-proxy watch-list {add-item ip-addr|enable|expiry-time minutes}
no ip auth-proxy watch-list [{add-item ip-addr|expiry-time}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add-item ip-addr</td>
<td>Adds an IP address to the watch list.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables a watch list.</td>
</tr>
<tr>
<td>expiry-time minutes</td>
<td>Specifies the duration of time that an entry is in the watch list; see the “Usage Guidelines” section for valid values.</td>
</tr>
</tbody>
</table>

**Command Default**

The defaults are as follows:

- `minutes` is 30 minutes.
- The watch-list functionality is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

The valid values for minutes are from 0 to the largest 32-bit positive number (0x7FFFFFFF or 2147483647 in decimal). Setting the `minutes` to 0 (zero) places the entries in the list permanently.

This command is supported on the firewall interfaces only.

Use the `no` form of this command to do the following:

- `no ip auth-proxy watch-list` --Disables the watch-list functionality.
- `no ip auth-proxy watch-list add-item ip-addr`--Removes the IP address from the watch list.
- `no ip auth-proxy watch-list expiry-time` --Returns to the default setting.

A watch list consists of IP addresses that have opened TCP connections to port 80 and have not sent any data. No new connections are accepted from this type of IP address (to port 80) and the packet is dropped.

An entry remains in the watch list for the time that is specified by `expiry-time minutes`.

When you disable a watch list, no new entries are put into the watch list, but the sessions are put in SERVICE_DENIED state. The timer deletes sessions after 2 minutes.
Examples

This example shows how to enable an authentication proxy watch list:

Router(config-if)# ip auth-proxy watch-list enable
Router(config-if)#

This example shows how to disable an authentication proxy watch list:

Router(config-if)# no ip auth-proxy watch-list
Router(config-if)#

This example shows how to add an IP address to a watch list:

Router(config-if)# ip auth-proxy watch-list add-item 10.0.0.2
Router(config-if)#

This example shows how to set the duration of time that an entry is in a watch list:

Router(config-if)# ip auth-proxy watch-list expiry-time 29
Router(config-if)#

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip auth-proxy watch-list</td>
<td>Deletes a single watch-list entry or all watch-list entries.</td>
</tr>
<tr>
<td>ip auth-proxy max-login-attempts</td>
<td>Limits the number of login attempts at a firewall interface.</td>
</tr>
<tr>
<td>show ip auth-proxy watch-list</td>
<td>Displays the information about the authentication proxy watch list.</td>
</tr>
</tbody>
</table>
To enable the tracking of device probes, use the `ip device tracking probe` command in configuration mode. To disable device probes, use the `no` form of this command.

```
ip device tracking probe {count count|delay delay|interval interval}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count count</td>
<td>Specifies the number of IP tracking probes from 1 to 5.</td>
</tr>
<tr>
<td>delay delay</td>
<td>Specifies the delay time of IP tracking probes from 1 to 120 seconds.</td>
</tr>
<tr>
<td>interval interval</td>
<td>Specifies the time between IP tracking probes from 30 to 300 minutes.</td>
</tr>
</tbody>
</table>

### Command Default

Device probe tracking is disabled.

### Command Modes

Config mode (config #)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SX17</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to set the probe count to 5:

```
Router(config)# ip device tracking probe count 5
```

The following example shows how to set the delay time to 60:

```
Router(config)# ip device tracking probe delay 60
```

The following example shows how to set the interval time to 35:

```
Router(config)# ip device tracking probe interval 35
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip device tracking</td>
<td>Displays information about entries in the IP device tracking table.</td>
</tr>
</tbody>
</table>
ip dhcp client broadcast-flag (interface)

To configure a DHCP client to set or clear the broadcast flag, use the `ip dhcp client broadcast-flag` command in interface configuration mode. To disable the configuration, use the `no` form of this command.

```
ip dhcp client broadcast-flag {clear|set}
no ip dhcp client broadcast-flag
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear</td>
<td>Clears the broadcast flag.</td>
</tr>
<tr>
<td>set</td>
<td>Sets the broadcast flag.</td>
</tr>
</tbody>
</table>

**Command Default**
The broadcast flag is set.

**Command Modes**
Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(3)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For a DHCP server to work on a Dynamic Multipoint VPN (DMVPN) network, the DHCP client available on the spoke must unicast the DHCP messages from the server to the client. By default, the DHCP client on the spoke broadcasts the DHCP messages. The broadcast flag is set during broadcast. Hence, the DHCP client on the spoke must have an option to clear the DHCP broadcast flag. You can use the `ip dhcp client broadcast-flag` command to configure the DHCP client to set or clear the broadcast flag.

**Examples**

The following example shows how to configure a DHCP client to clear the broadcast flag:

```
Router(config)# tunnel 1
Router(config-if)# ip dhcp client broadcast-flag clear
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address dhcp</td>
<td>Acquires an IP address on an interface from the DHCP.</td>
</tr>
<tr>
<td>ip dhcp support tunnel unicast</td>
<td>Configures a spoke-to-hub tunnel to unicast the DHCP replies over the DMVPN network.</td>
</tr>
</tbody>
</table>
ip dhcp support tunnel unicast

To configure a spoke-to-hub tunnel to unicast DHCP replies over a Dynamic Multipoint VPN (DMVPN) network, use the `ip dhcp support tunnel unicast` command in global configuration mode. To disable the configuration, use the `no` form of this command.

```
ip dhcp support tunnel unicast
no ip dhcp support tunnel unicast
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

A spoke-to-hub tunnel broadcasts the replies over the DMVPN network.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(3)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, the DHCP replies are broadcast from the DMVPN hub to the spoke. The DHCP relay agent must unicast the DHCP messages for a DHCP server to be functional in the DMVPN environment. Hence for the DHCP to be functional in DMVPN environment, you must configure the DHCP relay agent to unicast the DHCP messages.

Use the `ip dhcp support tunnel unicast` command to configure the DHCP relay agent to unicast the DHCP protocol messages from the server (hub) to the client (spoke). The relay agent uses the nonbroadcast multiaccess (NBMA) address to create temporary routes in Next Hop Resolution Protocol (NHRP) to help unicast the DHCP OFFER and DHCP ACK messages to the spoke.

**Examples**

The following example shows how to configure a spoke-to-hub tunnel to unicast the replies over a DMVPN network:

```
Router(config)# ip dhcp support tunnel unicast
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address dhcp</td>
<td>Configures an IP address on an interface acquired through DHCP.</td>
</tr>
<tr>
<td>ip dhcp client broadcast-flag</td>
<td>Configures the DHCP client to set or clear the broadcast flag.</td>
</tr>
</tbody>
</table>
To specify that IP extensions are included in a certificate request either for enrollment or generation of a certificate authority (CA) certificate for the Cisco IOS CA, use the **ip-extension** command in ca-trustpoint configuration mode. To remove a previously specified IP extension, use the **no** form of this command.

```
ip-extension multicast inherit [ipv4|ipv6]|prefix ipaddress|range min-ipaddress max-ipaddress
no ip-extension multicast inherit [ipv4|ipv6]|prefix ipaddress|range min-ipaddress max-ipaddress
```

**Syntax Description**

| **multicast** | (Optional) Specifies that only multicast traffic, a subsequent address family identifier (SAFI), will be included in certificate requests.  
**Note** If neither multicast nor unicast traffic is specified, both will be included in a certificate request. |
| **unicast** | (Optional) Specifies that only unicast traffic, a SAFI, will be included in certificate requests.  
**Note** If neither multicast nor unicast traffic is specified, both will be included in a certificate request. |
| **inherit** | Specifies that IP addresses will be inherited from an issuer certificate.  
The issuer’s certificate is first checked to find a certificate containing the address range or prefix. If no match is found, the certificate from the next issuer in the chain is checked, and so forth, up the certificate chain, recursively, until a match is located. |
| **ipv4** | (Optional) Specifies that only IPv4 addresses are inherited.  
**Note** If neither an **ipv4** nor an **ipv6** address is specified, both address families are inherited. |
| **ipv6** | (Optional) Specifies that only IPv6 addresses are inherited.  
**Note** If neither an **ipv4** nor an **ipv6** address is specified, both address families are inherited. |
| **prefix ipaddress** | Specifies the IP address prefix or a single IP address for either an IPv4 or IPv6 address.  
The IP address formats are:  
- A.B.C.D IPv4 address  
- A.B.C.D/nn IPv4 prefix  
- X:X::X IPv6 address  
- X:X::X/<0-128> IPv6 prefix |
| **range** | Specifies that there is a range of IP addresses. |
The beginning IP address in the IP address range, in either IPv4 or IPv6 address format.
The IP address formats are:
  • A.B.C.D Beginning IPv4 address in the range
  • X:X:X::X Beginning IPv6 address in the range

The ending IP address in the IP address range, in either IPv4 or IPv6 address format.
The IP address formats are:
  • A.B.C.D Ending IPv4 address in the range
  • X:X:X::X Ending IPv6 address in the range

Command Default
No IP extensions will be included in a certificate request.

Command Modes
Ca-trustpoint configuration (ca-trustpoint)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(22)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(24)T</td>
<td>Support for IPv6 Secure Neighbor Discovery (SeND) was added.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Note
Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

The **ip-extension** command may be used to specify IP extensions for a public key infrastructure (PKI) server or client and may be issued one or more times, including multiple issuances with the **inherit**, **prefix**, and **range** keywords. For the inherit option, if the address family is not specified, both IPv4 and IPv6 addresses will be inherited. When the IPv4 or IPv6 address family is not specified for prefix or range, the address family will be determined from the address format.

Note
It is recommended that you validate each **ip-extension** command line against your existing IP-extension configuration according to RFC 3779, verifying that IP address ranges do not overlap. The issue’s certificate may not be available to validate the issuer’s certificate for subsets of addresses.

Examples

The following example shows how to specify that multiple IP extensions are included in the server certificate request:

```
Router(ca-trustpoint)# ip-extension multicast prefix 10.64.0.0/11
```
! Only multicast traffic with the IPv4 prefix 10.64.0.0/11 will be included in certificate requests.

Router(ca-trustpoint)# ip-extension prefix 2001:100:1::/48

! Multicast and unicast traffic with the IPv6 prefix 2001:100:1::/48 will be included in certificate requests.

Router(ca-trustpoint)# ip-extension inherit

! Multicast and unicast traffic with IPv4 and IPv6 addresses will be inherited from the issuer’s certificate.

Router(ca-trustpoint)# ip-extension inherit ipv6

! Multicast and unicast traffic with IPv6 addresses only will be inherited from the issuer’s certificate.

Router(ca-trustpoint)# ip-extension unicast range 209.165.200.225 143.255.55.255

! Unicast traffic within the specified IPv4 address range will be included in the certificate request.


! Multicast and unicast traffic within the specified IPv6 address range will be included in the certificate request.

The following is sample output from the `show crypto pki certificates verbose` command. The output displays X.509 certificate IP address extension information where the IPv4 multicast prefix has been set to 10.64.0.0/11, and the IPv4 unicast range has been set to 209.165.201.1 209.165.201.30.

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=srtr1
  Subject:
    cn=srtr1
  Validity Date:
    start date: 21:50:11 PST Sep 29 2008
    end date: 21:50:11 PST Sep 29 2011
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
  Signature Algorithm: MD5 with RSA Encryption
  Fingerprint MD5: 30C1C9B6 BC17815F DF6095CD EDE2A5F3
  Fingerprint SHA1: A67C451E 49E94E87 8EB0F71D 5BE642CF C68901EF
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: B593E52F F711094F 1CCAA4AE 683049AE 4ACE8E8C
    X509v3 Basic Constraints:
      CA: TRUE
    X509v3 Authority Key ID: B593E52F F711094F 1CCAA4AE 683049AE 4ACE8E8C
    Authority Info Access:
      X509v3 IP Extension:
        IPv4 (Unicast):
        IPv4 (Multicast):
          10.64.0.0/11
    Associated Trustpoints: srtr1
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show crypto pki certificates</code></td>
<td>Displays information about the CA certificate.</td>
</tr>
<tr>
<td><code>show crypto pki trustpoints</code></td>
<td>Displays information about trustpoints that are configured on the router.</td>
</tr>
</tbody>
</table>
ip http ezvpn

To enable the Cisco Easy VPN remote web server interface, use the `ip http ezvpn` command in global configuration mode. To disable the Cisco Easy VPN remote web server interface, use the `no` form of this command.

### Syntax Description
This command has no arguments or keywords.

### Command Default
The Cisco Easy VPN Remote web server interface is disabled by default.

### Command Modes
Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)YJ</td>
<td>This command was introduced for the Cisco uBR905 and Cisco uBR925 cable access routers.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
This command enables the Cisco Easy VPN Remote web server, an onboard web server that allows users to connect an IPSec Easy VPN tunnel and to provide the required authentication information. The Cisco Easy VPN Remote web server allows the user to perform these functions without having to use the Cisco command-line interface (CLI).

Before using this command, you must first enable the Cisco web server that is onboard the cable access router by entering the `ip http server` command. Then use the `ip http ezvpn` command to enable the Cisco Easy VPN remote web server. You can then access the web server by entering the IP address for the Ethernet interface of the router in your web browser.

### Note
The Cisco Easy VPN Remote web interface does not work with the cable monitor web interface in Cisco IOS Release 12.2(8)YJ. To access the cable monitor web interface, you must first disable the Cisco Easy VPN remote web interface with the `no ip http ezvpn` command, and then enable the cable monitor with the `ip http cable-monitor` command.

### Examples
The following example shows how to enable the Cisco Easy VPN remote web server interface:

```
Router# configure terminal
```
Router(config)# ip http server
Router(config)# ip http ezvpn
Router(config)# exit
Router# copy running-config startup-config

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip http cable-monitor</td>
<td>Enables and disables the Cable Monitor Web Server feature.</td>
</tr>
<tr>
<td>ip http port</td>
<td>Configures the TCP port number for the HTTP web server of the router.</td>
</tr>
<tr>
<td>ip http server</td>
<td>Enables and disables the HTTP web server of the router.</td>
</tr>
</tbody>
</table>
ip inspect through ip security strip

- ip inspect, on page 469
- ip inspect alert-off, on page 471
- ip inspect audit-trail, on page 472
- ip inspect dns-timeout, on page 474
- ip inspect hashtable, on page 476
- ip inspect L2-transparent dhcp-passthrough, on page 477
- ip inspect log drop-pkt, on page 479
- ip inspect max-incomplete high, on page 482
- ip inspect max-incomplete low, on page 484
- ip inspect name, on page 486
- ip inspect one-minute high, on page 498
- ip inspect one-minute low, on page 500
- ip inspect tcp block-non-session, on page 502
- ip inspect tcp finwait-time, on page 504
- ip inspect tcp idle-time, on page 506
- ip inspect tcp max-incomplete host, on page 508
- ip inspect tcp reassembly, on page 510
- ip inspect tcp synwait-time, on page 512
- ip inspect tcp window-scale-enforcement loose, on page 513
- ip inspect udp idle-time, on page 515
- ip inspect waas enable, on page 517
- integrity, on page 518
- ip interface, on page 520
- ip ips, on page 522
- ip ips auto-update, on page 524
- ip ips config location, on page 526
- ip ips deny-action ips-interface, on page 528
- ip ips enable-clidelta, on page 530
- ip ips event-action-rules, on page 531
- ip ips fail closed, on page 532
- ip ips inherit-obsolete-tunings, on page 533
- ip ips memory regex chaining, on page 535
- ip ips memory threshold, on page 537
• ip inspect through ip security strip
**ip inspect**

To apply a set of inspection rules to an interface, use the `ip inspect` command in interface configuration mode. There are two different modes for this command, configuration mode and interface configuration mode. To remove the set of rules from the interface, use the `no` form of this command.

**Global Configuration Mode**

```
ip inspect inspection-name \{in|out\} [[redundancy|stateful hsrp-group-name|update seconds|seconds]]
no ip inspect inspection-name \{in|out\} [[redundancy|stateful hsrp-group-name|update seconds|seconds]]
```

**Interface Configuration Mode**

```
ip inspect inspection-name \{in|out\} [[redundancy|stateful hsrp-group-name]]
no ip inspect inspection-name \{in|out\} [[redundancy|stateful hsrp-group-name]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Interface Configuration Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>inspection-name</code></td>
<td>Identifies which set of inspection rules to apply.</td>
</tr>
<tr>
<td><code>in</code></td>
<td>Applies the inspection rules to inbound interface.</td>
</tr>
<tr>
<td><code>out</code></td>
<td>Applies the inspection rules to outbound interface.</td>
</tr>
<tr>
<td><code>redundancy</code></td>
<td>Enables redundancy.</td>
</tr>
<tr>
<td><code>stateful</code></td>
<td>Enables stateful redundancy.</td>
</tr>
<tr>
<td><code>hsrp-group-name</code></td>
<td>The hsrp-group name that is used to configure box-to-box HA</td>
</tr>
</tbody>
</table>

**Global Configuration Mode**

<table>
<thead>
<tr>
<th>Redundancy settings for firewall sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>redundancy</code></td>
</tr>
<tr>
<td><code>update</code></td>
</tr>
<tr>
<td><code>seconds &lt;10-60&gt;</code></td>
</tr>
</tbody>
</table>

**Command Default**

If no set of inspection rules is applied to an interface, no traffic will be inspected by CBAC. If `redundancy stateful <hsrp-grp-name>` is not used, there will be no stateful firewall high-availability.

**Command Modes**

Interface configuration mode(conf-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(6)T</td>
<td>Added support for <code>redundancy</code>, <code>update</code>, <code>seconds</code>, and <code>stateful</code> keywords.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>
Modification
This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines
Use this command to apply a set of inspection rules to an interface.

Typically, if the interface connects to the external network, you apply the inspection rules to outbound traffic; alternately, if the interface connects to the internal network, you apply the inspection rules to inbound traffic.

In the Interface Configuration mode, use `ip inspect <name> in/out redundancy stateful <hsrp-group>` command. Use the redundancy stateful `<hsrp-grp>` option to turn on stateful high availability for all session that come up on this inspect rule. The incoming IP traffic is the return traffic of an existing session. It not necessary to have redundancy stateful HSRP group name if you do not require IOS Firewall High availability.

In the Global Configuration mode, use `ip inspect redundancy update seconds <10-60>`. Use the redundancy update seconds option to configure the time interval between the synchronization of the active and standby firewall HA sessions.

Examples
The following example applies a set of inspection rules named MY-INSPECT_RULE to serial0 interface’s outbound traffic. This causes the inbound IP traffic to be permitted only if the traffic is part of an existing session, and to be denied if the traffic is not part of an existing session.

```
interface serial0
ip inspect MY-INSPECT_RULE out redundancy stateful B2B-HA-HSRP-GRP
```

Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip inspect</td>
<td>Defines a set of inspection rules.</td>
</tr>
<tr>
<td>name</td>
<td></td>
</tr>
</tbody>
</table>
ip inspect alert-off

To disable Context-based Access Control (CBAC) alert messages, which are displayed on the console, use the `ip inspect alert-off` command in global configuration mode. To enable CBAC alert messages, use the `no` form of this command.

```
ip inspect alert-off [vrf vrf-name]
no ip inspect alert-off [vrf vrf-name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument/Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Disables CBAC alert messages only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

Alert messages are displayed.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>vrf vrf-name</code> keyword/argument pair was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Examples**

The following example disables CBAC alert messages:

```
ip inspect alert-off
```
ip inspect audit-trail

To turn on Context-based Access Control (CBAC) audit trail messages, which will be displayed on the console after each CBAC session closes, use the `ip inspect audit-trail` command in global configuration mode. To turn off CBAC audit trail messages, use the `no` form of this command.

```
ip inspect audit-trail [vrf vrf-name]
no ip inspect audit-trail [vrf vrf-name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Turns on CBAC audit trail messages only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

Audit trail messages are not displayed.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 P</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>vrf vrf-name</code> keyword/argument pair was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to turn on CBAC audit trail messages.

**Examples**

The following example turns on CBAC audit trail messages:

```
ip inspect audit-trail
```

Afterward, audit trail messages such as the following are displayed. These messages are examples of audit trail messages. To determine which protocol was inspected, see the port number of the responder. The port number follows the IP address of the responder.

```
%FW-6-SESS_AUDIT_TRAIL: tcp session initiator (192.168.1.13:33192) sent 22 bytes -- responder (192.168.129.11:25) sent 208 bytes
%FW-6-SESS_AUDIT_TRAIL: ftp session initiator 192.168.1.13:33194) sent 336 bytes -- responder (192.168.129.11:21) sent 325 bytes
```

The following example disables CBAC audit trail messages for VRF interface vrf1:

```
no ip inspect audit-trail vrf vrf1
```

Following are examples of audit trail messages:

```
```
sent 54 bytes -- responder (192.168.114.1:7) sent 54 bytes
00:10:47: %FW-6-SESS_AUDIT_TRAIL: VRF-vrf1:Stop ftp-data session: initiator (192.168.114.1:20)
sent 80000 bytes -- responder (192.168.14.1:38766) sent 0 bytes
sent 80 bytes -- responder (192.168.114.1:21) sent 265 bytes
sent 31 bytes -- responder (192.168.114.1:514) sent 12 bytes
00:10:57: %FW-6-SESS_AUDIT_TRAIL: VRF-vrf1:Stop rcmd-data session: initiator
(192.168.114.1:594) sent 0 bytes -- responder (192.168.14.1:530) sent 0 bytes
**ip inspect dns-timeout**

To specify the Domain Name System (DNS) idle timeout (the length of time during which a DNS name lookup session will still be managed while there is no activity), use the **ip inspect dns-timeout** command in global configuration mode. To reset the timeout to the default of 5 seconds, use the **no** form of this command.

```
ip inspect dns-timeout seconds [vrf vrf-name]
no ip inspect dns-timeout seconds [vrf vrf-name]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>seconds</strong></td>
<td>Specifies the length of time in seconds, for which a DNS name lookup session will still be managed while there is no activity. The default is 5 seconds.</td>
</tr>
<tr>
<td><strong>vrf vrf-name</strong></td>
<td>(Optional) Specifies the DNS idle timeout only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

5 seconds

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 P</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <strong>vrf vrf-name</strong> keyword/argument pair was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the software detects a valid User Datagram Protocol (UDP) packet for a new DNS name lookup session, if Context-based Access Control (CBAC) inspection is configured for UDP, the software establishes state information for the new DNS session.

If the software detects no packets for the DNS session for a time period defined by the DNS idle timeout, the software will not continue to manage state information for the session.

The DNS idle timeout applies to all DNS name lookup sessions inspected by CBAC.

The DNS idle timeout value overrides the global UDP timeout. The DNS idle timeout value also enters aggressive mode and overrides any timeouts specified for specific interfaces when you define a set of inspection rules with the **ip inspect name** command.

**Examples**

The following example sets the DNS idle timeout to 30 seconds:

```
ip inspect dns-timeout 30
```

The following example sets the DNS idle timeout back to the default (5 seconds):
no ip inspect dns-timeout
ip inspect hashtable

To change the size of the session hash table, use the `ip inspect hashtable` command in global configuration mode. To restore the size of the session hash table to the default, use the `no` form of this command.

```
ip inspect hashtable number
no ip inspect hashtable number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>number</th>
<th>Size of the hash table in terms of buckets. Possible values for the hash table are 1024, 2048, 4096, and 8192; the default value is 1024.</th>
</tr>
</thead>
</table>

**Command Default**

1024 buckets

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ip inspect hashtable` command to increase the size of the hash table when the number of concurrent sessions increases or to reduce the search time for the session. Collisions in a hash table result in poor hash function distribution because many entries are hashed into the same bucket for certain patterns of addresses. Even if a hash function distribution evenly dispenses the input across all of the buckets, a small hash table size will not scale well if there are a large number of sessions. As the number of sessions increase, the collisions increase, which increases the length of the linked lists, thereby, deteriorating the throughput performance.

**Note**

You should increase the hash table size when the total number of sessions running through the context-based access control (CBAC) router is approximately twice the current hash size; decrease the hash table size when the total number of sessions is reduced to approximately half the current hash size. Essentially, try to maintain a 1:1 ratio between the number of sessions and the size of the hash table.

**Examples**

The following example shows how to change the size of the session hash table to 2048 buckets:

```
ip inspect hashtable 2048
```
ip inspect L2-transparent dhcp-passthrough

To allow a transparent firewall to forward Dynamic Host Control Protocol (DHCP) pass-through traffic, use the `ip inspect L2-transparent dhcp-passthrough` command in global configuration mode. To return to the default functionality, use the `no` form of this command.

```
   ip inspect L2-transparent dhcp-passthrough
   no ip inspect L2-transparent dhcp-passthrough
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

This command is not enabled; thus, DHCP packets are forwarded or denied according to the configured access control list (ACL).

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A transparent firewall allows a Cisco IOS Firewall (a Layer 3 device) to operate as a Layer 2 firewall in bridging mode. Thus, the firewall can exist “transparently” to a network, no longer requiring users to reconfigure their statically defined network devices.

The `ip inspect L2-transparent dhcp-passthrough` command overrides the ACL for DHCP packets; that is, DHCP packets are forwarded even if the ACL is configured to deny all IP packets. Thus, this command can be used to enable a transparent firewall to forward DHCP packets across the bridge without inspection so clients on one side of the bridge can get an IP address from a DHCP server on the opposite side of the bridge.

**Examples**

**Allowing DHCP Pass-Through Traffic**

In this example, the static IP address of the client is removed, and the address is acquired via DHCP using the `ip address dhcp` command on the interface that is connected to the transparent firewall.

```
Router# show debug
ARP:
   ARP packet debugging is on
L2 Inspection:
   INSPECT L2 firewall debugging is on
   INSPECT L2 firewall DHCP debugging is on
Router#
Router(config)# ip inspect L2-transparent dhcp-passthrough
! The DHCP discover broadcast packet arrives from the client. Since this packet is a broadcast (255.255.255.255), it arrives in the flood path
*Mar 1 00:35:01.299:L2FW:insp_l2_flood:input is Ethernet0 output is Ethernet1
*Mar 1 00:35:01.299:L2FW:udp ports src 0.0.0.0 dst 255.255.255.255 protocol udp
*Mar 1 00:35:01.299:L2FW:udp ports src 68 dst 67
*Mar 1 00:35:01.299:L2FW:src 0.0.0.0.0 dst 255.255.255.255
```
! The DHCP pass through flag is checked and the packet is allowed
*Mar 1 00:35:01.299:L2FW:DHCP packet seen. Pass-through flag allows the packet
! The packet is a broadcast packet and therefore not sent to CBAC
*Mar 1 00:35:01.299:L2FW*:Packet is broadcast or multicast.PASS
*Mar 1 00:35:01.303:L2FW:insp_l2_flood:input is Ethernet1 output is Ethernet0
*Mar 1 00:35:01.303:L2FW*:Src 172.16.0.23 dst 255.255.255.255 protocol udp
*Mar 1 00:35:01.307:L2FW:udp ports src 67 dst 68
*Mar 1 00:35:01.307:L2FW:src 172.16.0.23 dst 255.255.255.255
*Mar 1 00:35:01.307:L2FW:DHCP packet seen. Pass-through flag allows the packet
*Mar 1 00:35:01.307:L2FW*:Packet is broadcast or multicast.PASS
*Mar 1 00:35:01.311:L2FW:insp_l2_flood:input is Ethernet0 output is Ethernet1
*Mar 1 00:35:01.311:L2FW*:Src 0.0.0.0 dst 255.255.255.255 protocol udp
*Mar 1 00:35:01.311:L2FW:udp ports src 68 dst 67
*Mar 1 00:35:01.311:L2FW:src 0.0.0.0 dst 255.255.255.255
*Mar 1 00:35:01.311:L2FW:DHCP packet seen. Pass-through flag allows the packet
*Mar 1 00:35:01.311:L2FW*:Packet is broadcast or multicast.PASS
*Mar 1 00:35:01.323:L2FW:insp_l2_flood:input is Ethernet1 output is Ethernet0
*Mar 1 00:35:01.323:L2FW*:Src 172.16.0.23 dst 255.255.255.255 protocol udp
*Mar 1 00:35:01.323:L2FW:udp ports src 67 dst 68
*Mar 1 00:35:01.323:L2FW:src 172.16.0.23 dst 255.255.255.255
*Mar 1 00:35:01.323:L2FW:DHCP packet seen. Pass-through flag denies the packet
*Mar 1 00:35:01.323:L2FW*:Packet is broadcast or multicast.PASS
! The client has an IP address (172.16.0.5) and has issued a G-ARP to let everyone know
it's address
*Mar 1 00:35:01.327:IP ARP:rcvd rep src 172.16.0.5 0008.a3b6.b603, dst 172.16.0.5 BVI1
Router#

Denying DHCP Pass-Through Traffic

In this example, DHCP pass-through traffic is not allowed (via the no ip inspect L2-transparent
dhcp-passthrough command). The client is denied when it attempts to acquire a DHCP address from
the server.

! Deny DHCP pass-through traffic
Router(config)# no ip inspect L2-transparent dhcp-passthrough

! The DHCP discover broadcast packet arrives from the client
*Mar 1 00:36:40.003:L2FW:insp_l2_flood:input is Ethernet0 output is Ethernet1
*Mar 1 00:36:40.003:L2FW*:Src 0.0.0.0 dst 255.255.255.255 protocol udp
*Mar 1 00:36:40.003:L2FW:udp ports src 68 dst 67
*Mar 1 00:36:40.003:L2FW:src 0.0.0.0 dst 255.255.255.255
*Mar 1 00:36:40.007:L2FW:DHCP packet seen. Pass-through flag denies the packet
! The packet is dropped because the flag does not allow DHCP passthrough traffic. Thus, !
the client cannot acquire an address, and it times out
*Mar 1 00:36:40.007:L2FW:FLOOD Dropping the packet after ACL check.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>debug ip inspect L2-transparent</td>
<td>Enables debugging messages for transparent firewall events.</td>
</tr>
<tr>
<td></td>
<td>show ip inspect</td>
<td>Displays Cisco IOS Firewall configuration and session information.</td>
</tr>
</tbody>
</table>

Cisco IOS Security Command Reference: Commands D to L
**ip inspect log drop-pkt**

To log all packets dropped by the firewall, use the **ip inspect log drop-pkt** command in global configuration mode. To return to the default state, use the **no** form of this command.

**ip inspect log drop-pkt**
**no ip inspect log drop-pkt**

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Packets dropped by the firewall are not logged.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>This command was integrated into Release 12.3(8)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To see the packets that are dropped by the firewall, the **ip inspect log drop-pkt** command must be enabled.

**Examples**

The following example shows how to enable the logging of packets dropped by the firewall:

```
Router> enable
Router# configure terminal
Router(config)
) # ip inspect log drop-pkt
```

The following example shows a possible message that can be displayed when packets are dropped:

```
*Sep 9 19:56:28.699: %FW-6-DROP_PKT: Dropping tcp pkt 17.2.2.1:0 => 19.2.2.1:0 with ip ident 229 due to Invalid Header length
*Sep 9 20:30:47.839: %FW-6-DROP_TCP_PKT: Dropping tcp pkt 17.2.2.1:42829 => 19.2.2.1:80 due to SYN pkt with illegal flags -- ip ident 23915 tcpflags 40962 seq.no 3928613134 ack 0
*Sep 10 00:30:24.931: %FW-6-DROP_TCP_PKT: Dropping tcp pkt 17.2.2.1:45771 => 19.2.2.1:80 due to SYN with data or with PSH/URG flags -- ip ident 55001 tcpflags 40962 seq.no 2232798685 ack 0
*Aug 29 21:57:16.895: %FW-6-DROP_PKT: Dropping tcp pkt 17.2.2.1:51613 => 19.2.2.1:80 due to Out-Of-Order Segment
```

The table below describes messages that occur when packets are dropped.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid Header length</td>
<td>The datagram is so small that it could not contain the layer 4 TCP, Universal Computer Protocol (UCP), or Internet Control Message Protocol (ICMP) header.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Police rate limiting</td>
<td>Rate limiting is enabled, and the packet in question has exceeded the rate limit.</td>
</tr>
<tr>
<td>Session limiting</td>
<td>Session limiting is on, and the session count exceeds the configured session threshold.</td>
</tr>
<tr>
<td>Bidirectional traffic disabled</td>
<td>Session is unidirectional and the firewall is seeing packets in the other direction and dropping the session.</td>
</tr>
<tr>
<td>SYN with data or with PSH/URG flags</td>
<td>TCP SYN packet is seen with data.</td>
</tr>
<tr>
<td>Segment matching no TCP connection</td>
<td>Non-initial TCP segment is received without a valid session.</td>
</tr>
<tr>
<td>Invalid Segment</td>
<td>There is an invalid TCP segment.</td>
</tr>
<tr>
<td>Invalid Seq#</td>
<td>The packet contains an invalid TCP sequence number.</td>
</tr>
<tr>
<td>Invalid Ack (or no Ack)</td>
<td>The packet contains an invalid TCP acknowledgement number.</td>
</tr>
<tr>
<td>Invalid Flags</td>
<td>Flags in a TCP segment are invalid.</td>
</tr>
<tr>
<td>Invalid Checksum</td>
<td>There is an invalid TCP checksum.</td>
</tr>
<tr>
<td>SYN inside current window</td>
<td>A synchronization packet is seen within the window of an already established TCP connection.</td>
</tr>
<tr>
<td>RST inside current window</td>
<td>A reset (RST) packet is observed within the window of an already established TCP connection.</td>
</tr>
<tr>
<td>Out-Of-Order Segment</td>
<td>The packets in a segment are out of order.</td>
</tr>
<tr>
<td>Retransmitted Segment with Invalid Flags</td>
<td>A retransmitted packet was already acknowledged by the receiver.</td>
</tr>
<tr>
<td>Stray Segment</td>
<td>A TCP segment is received that should not have been received through the TCP state machine such as a TCP SYN packet being received in the listen state.</td>
</tr>
<tr>
<td>Internal Error</td>
<td>The TCP state machine that is maintained by the firewall encounters an internal error.</td>
</tr>
<tr>
<td>Invalid Window scale option</td>
<td>The responder on one side of a firewall proposes an illegal window scale option. The window scale option is illegal in this case because the initiating side did not propose the option first.</td>
</tr>
<tr>
<td>Invalid TCP options</td>
<td>The options in the TCP header are not TCP protocol compliant.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip inspect tcp block-non-session</td>
<td>Blocks packets that do not belong to the existing firewall TCP sessions in the inbound and outbound directions.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ip inspect tcp finwait-time</td>
<td>Defines how long a TCP session will still be managed after the firewall detects a FIN-exchange.</td>
</tr>
<tr>
<td>ip inspect tcp idle-time</td>
<td>Specifies the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity).</td>
</tr>
<tr>
<td>ip inspect tcp max-incomplete host</td>
<td>Specifies threshold and blocking time values for TCP host-specific DoS detection and prevention.</td>
</tr>
<tr>
<td>ip inspect tcp reassembly</td>
<td>Sets parameters that define how Cisco IOS Firewall application inspection and Cisco IOS IPS will handle out-of-order TCP packets.</td>
</tr>
<tr>
<td>ip inspect tcp synwait-time</td>
<td>Defines how long the software will wait for a TCP session to reach the established state before dropping the session.</td>
</tr>
<tr>
<td>ip inspect udp idle-time</td>
<td>Specifies the UDP idle timeout (the length of time for which a UDP session will still be managed while there is no activity).</td>
</tr>
</tbody>
</table>
ip inspect max-incomplete high

To define the number of existing half-open sessions that will cause the software to start deleting half-open sessions, use the `ip inspect max-incomplete high` command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the `no` form of this command.

```
ip inspect max-incomplete high number [vrf vrf-name]
no ip inspect max-incomplete high
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Specifies the number of existing half-open sessions that will cause the software to start deleting half-open sessions. The default is 500 half-open sessions.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Defines the number of existing half-open sessions only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>500 half-open sessions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global configuration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 P</td>
<td>This command was introduced.</td>
<td></td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>vrf vrf-name</code> keyword/argument pair was added.</td>
<td></td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
<td></td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, “half-open” means that the session has not reached the established state. For User Datagram Protocol (UDP), “half-open” means that the firewall has detected traffic from one direction only.</td>
</tr>
</tbody>
</table>

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the `max-incomplete high` number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the `max-incomplete low` number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

<table>
<thead>
<tr>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions when the number drops below 800:</td>
</tr>
</tbody>
</table>
The following example shows an ALERT_ON message generated for the `ip inspect max-incomplete high` command:

```
ip inspect max-incomplete high 20 vrf vrf1
show log / include ALERT_ON
00:59:00:%FW-4-ALERT_ON: VRF-vrf1:getting aggressive, count (21/20) current 1-min rate: 21
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip inspect max-incomplete low</code></td>
<td>Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.</td>
</tr>
<tr>
<td><code>ip inspect one-minute high</code></td>
<td>Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.</td>
</tr>
<tr>
<td><code>ip inspect one-minute low</code></td>
<td>Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.</td>
</tr>
<tr>
<td><code>ip inspect tcp max-incomplete host</code></td>
<td>Specifies the threshold and blocking time values for TCP host-specific DoS detection and prevention.</td>
</tr>
</tbody>
</table>
ip inspect max-incomplete low

To define the number of existing half-open sessions that will cause the software to stop deleting half-open sessions, use the `ip inspect max-incomplete low` command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the `no` form of this command.

```
ip inspect max-incomplete low number [vrf vrf-name]
no ip inspect max-incomplete low
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Specifies the number of existing half-open sessions that will cause the software to stop deleting half-open sessions. The default is 400 half-open sessions.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Defines the number of existing half-open sessions only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

400 half-open sessions

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 P</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>vrf vrf-name</code> keyword/argument pair was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, “half-open” means that the session has not reached the established state. For User Datagram Protocol (UDP), “half-open” means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

**Examples**

The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions when the number drops below 800:
ip inspect max-incomplete high 900
ip inspect max-incomplete low 800

The following example shows an ALERT_OFF message generated for the `ip inspect max-incomplete low` command:

```
ip inspect max-incomplete low 10 vrf vrf1
show log / include ALERT_OFF
00:59:31: %FW-4-ALERT_OFF: VRF=vrf1:calming down, count (9/10) current 1-min rate: 100
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip inspect max-incomplete high</td>
<td>Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.</td>
</tr>
<tr>
<td>ip inspect one-minute high</td>
<td>Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.</td>
</tr>
<tr>
<td>ip inspect one-minute low</td>
<td>Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.</td>
</tr>
<tr>
<td>ip inspect tcp max-incomplete host</td>
<td>Specifies the threshold and blocking time values for TCP host-specific DoS detection and prevention.</td>
</tr>
</tbody>
</table>
To define a set of inspection rules, use the `ip inspect name` command in global configuration mode. To remove the inspection rule for a protocol or to remove the entire set of inspection rules, use the `no` form of this command.

```
ip inspect name inspection-name [parameter max-sessions number] protocol [alert {on|off}] [audit-trail {on|off}] [timeout seconds]
no ip inspect name inspection-name [parameter max-sessions number] protocol [alert {on|off}] [audit-trail {on|off}] [timeout seconds]
```

### HTTP Inspection Syntax
```
ip inspect name inspection-name http [java-list access-list] [urlfilter] [alert {on|off}] [audit-trail {on|off}] [timeout seconds]
no ip inspect name inspection-name protocol
```

### Simple Mail Transfer Protocol (SMTP) and Extended SMTP Inspection (ESMTP) Syntax
```
ip inspect name inspection-name {smtp|esmtp} [alert {on|off}] [audit-trail {on|off}] [max-data number] [timeout seconds]
```

remote-procedure call (RPC) Inspection Syntax
```
ip inspect name inspection-name [parameter max-sessions number] rpc program-number number [wait-time minutes] [alert {on|off}] [audit-trail {on|off}] [timeout seconds]
no ip inspect name inspection-name protocol
```

Post Office Protocol 3(POP3)/ Internet Message Access Protocol(IMAP) Inspection Syntax
```
ip inspect name inspection-name imap [alert {on|off}] [audit-trail {on|off}] [reset] [secure-login] [timeout number]
ip inspect name inspection-name pop3 [alert {on|off}] [audit-trail {on|off}] [reset] [secure-login] [timeout number]
```

Fragment Inspection Syntax
```
ip inspect name inspection-name [parameter max-sessions number] fragment [max number timeout seconds]
no ip inspect name inspection-name [parameter max-sessions number] fragment [max number timeout seconds]
```

Application Firewall Provisioning Syntax
```
ip inspect name inspection-name [parameter max-sessions number] appfw policy-name
no ip inspect name inspection-name [parameter max-sessions number] appfw policy-name
```

User-Defined Application Syntax
```
ip inspect inspection-name user-10 [alert {on|off}] [audit-trail {on|off}] [timeout seconds]
no ip inspect inspection-name user-10 [alert {on|off}] [audit-trail {on|off}] [timeout seconds]
```

Session Limiting Syntax
```
no ip inspect name inspection-name [parameter max-sessions number]
```
### Syntax Description

<table>
<thead>
<tr>
<th><strong>Syntax</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>inspection-name</code></td>
<td>Name the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same <code>inspection-name</code> as the existing set of rules.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The <code>inspection-name</code> cannot exceed 16 characters; otherwise, the name will be truncated to the 16-character limit.</td>
</tr>
<tr>
<td><code>parameter max-sessions number</code></td>
<td>(Optional) Limits the number of established firewall sessions that a firewall rule creates. By default, there is no limit to the number of firewall sessions.</td>
</tr>
<tr>
<td><code>protocol</code></td>
<td>A protocol keyword listed in the tables below.</td>
</tr>
<tr>
<td>`alert {on</td>
<td>off}`</td>
</tr>
<tr>
<td>`audit-trail {on</td>
<td>off}`</td>
</tr>
<tr>
<td><code>timeout seconds</code></td>
<td>(Optional) To override the global TCP or UDP, or Internet Control Message Protocol (ICMP) idle timeouts for the specified protocol, specify the number of seconds for a different idle timeout.</td>
</tr>
<tr>
<td></td>
<td>This timeout overrides the global TCP, UDP, or ICMP timeouts but will not override the global Domain Name System (DNS) timeout.</td>
</tr>
<tr>
<td><code>http</code></td>
<td>Specifies the HTTP protocol for Java applet blocking.</td>
</tr>
<tr>
<td><code>java-list access-list</code></td>
<td>(Optional) Specifies the numbered standard access list to use to determine &quot;friendly&quot; sites. This keyword is available only for the HTTP protocol, for Java applet blocking. Java blocking works only with numbered standard access lists.</td>
</tr>
<tr>
<td><code>urlfilter</code></td>
<td>(Optional) Associates URL filtering with HTTP inspection.</td>
</tr>
<tr>
<td>`smtp</td>
<td>esmtp`</td>
</tr>
<tr>
<td><code>max-data number</code></td>
<td>(Optional) Specifies the maximum amount of data, in bytes, that can be transferred in a single Simple Mail Transport Protocol (SMTP) session. After the maximum value is exceeded, the firewall logs an alert message and closes the session. The default value is 20MB.</td>
</tr>
<tr>
<td><code>rpc program-number number</code></td>
<td>Specifies the program number to permit. This keyword is available only for the remote-procedure call (RPC) protocol.</td>
</tr>
<tr>
<td><code>wait-time minutes</code></td>
<td>(Optional) Specifies the number of minutes to keep a small gap in the firewall to allow subsequent connections from the same source address and to the same destination address and port. The default wait-time is zero minutes. This keyword is available only for the RPC protocol.</td>
</tr>
<tr>
<td><code>imap</code></td>
<td>Specifies that the Internet Message Access Protocol (IMAP) is being used.</td>
</tr>
<tr>
<td><code>reset</code></td>
<td>(Optional) Resets the TCP connection if the client enters a nonprotocol command before authentication is complete.</td>
</tr>
</tbody>
</table>
Causes a user at a nonsecure location to use encryption for authentication.

Specifies that the Post Office Protocol, Version 3 (POP3) is being used.

Specifies fragment inspection for the named rule.

(Optional) Specifies the maximum number of unassembled packets for which state information (structures) is allocated by Cisco IOS software. Unassembled packets are packets that arrive at the router interface before the initial packet for a session. The acceptable range is 50 through 10000. The default is 256 state entries.

- Memory is allocated for the state structures, and setting this value to a larger number may cause memory resources to be exhausted.

(Optional) Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet. The default timeout value is 1 second.

- If this number is set to a value greater than 1 second, it is automatically adjusted by the Cisco IOS software when the number of free state structures goes below certain thresholds: when the number of free states is fewer than 32, the timeout is divided by 2. When the number of free states is fewer than 16, the timeout is set to 1 second.

Specifies application firewall provisioning.

Application firewall policy name.

This name must match the name specified via the `appfw policy-name` command.

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Command Modes</th>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td>No inspection rules are defined.</td>
<td>Global configuration (config)</td>
<td>Release</td>
</tr>
<tr>
<td>11.2P</td>
<td>This command was introduced.</td>
<td></td>
</tr>
<tr>
<td>12.0(5)T</td>
<td>This command was modified. Support was added for configurable alert and audit trail, IP fragmentation checking, and NetShow protocol.</td>
<td></td>
</tr>
<tr>
<td>12.2(11)YU</td>
<td>This command was modified. Support was added for ICMP and Session Initiation Protocol (SIP) protocols. The <code>urlfilter</code> keyword was added to the HTTP inspection syntax.</td>
<td></td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was modified. Support was added for ICMP, SIP, and the <code>urlfilter</code> keyword was added.</td>
<td></td>
</tr>
<tr>
<td>12.3(1)</td>
<td>This command was modified. Skinny protocol support was added.</td>
<td></td>
</tr>
</tbody>
</table>
Modification Release

This command was modified. Extended Simple Mail Transfer Protocol (ESMTP) protocol support was added.

This command was modified. The appfw keyword and the policy-name argument were added to support application firewall provisioning. The parameter max-sessions, reset, router-traffic, and secure-login, and keywords were added.

Support for a larger list of protocols including user-defined applications was added.

This command was integrated into Cisco IOS Release 12.(33)SRA.

This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

This command was modified. Support for the CU-SeeMe protocol and the cuseeme keyword was removed.

Usage Guidelines

To define a set of inspection rules, enter the `ip inspect name` command for each protocol that you want the Cisco IOS firewall to inspect, using the same inspection-name. Give each set of inspection rules a unique inspection-name, which should not exceed the 16-character length limit. Define either one or two sets of rules per interface— you can define one set to examine both inbound and outbound traffic, or you can define two sets: one for outbound traffic and one for inbound traffic. The `no ip inspect-name protocol` removes the inspection rule for the specified protocol.

`no ip inspect name` command removes the entire set of inspection rules.

To define a single set of inspection rules, configure inspection for all the desired application-layer protocols, and for ICMP, TCP, and UDP, or as desired. This combination of TCP, UDP, and application-layer protocols join together to form a single set of inspection rules with a unique name. (There are no application-layer protocols associated with ICMP.)

To remove the inspection rule for a protocol, use the `no` form of this command with the specified inspection name and protocol; To remove the entire set of inspection rules, use the `no` form of this command only; that is, do not list any inspection names or protocols.

In general, when inspection is configured for a protocol, return traffic entering the internal network will be permitted only if the packets are part of a valid, existing session for which state information is being maintained.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Keyword</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>icmp</td>
</tr>
<tr>
<td>TCP</td>
<td>tcp</td>
</tr>
<tr>
<td>UDP</td>
<td>udp</td>
</tr>
</tbody>
</table>

Table 9: Protocol Keywords--Transport-Layer and Network-Layer Protocols
The TCP, UDP, and H.323 protocols support the `router-traffic` keyword, which enables inspection of traffic destined to or originated from a router. The command format is as follows: `ip inspect name inspection-name \{tcp | udp | H323\} [alert \{on | off\}] [audit-trail \{on | off\}] [router-traffic][timeout seconds]

TCP and UDP Inspection

You can configure TCP and UDP inspection to permit TCP and UDP packets to enter the internal network through the firewall, even if the application-layer protocol is not configured to be inspected. However, TCP and UDP inspection do not recognize application-specific commands, and therefore might not permit all return packets for an application, particularly if the return packets have a different port number from the previous exiting packet.

Any application-layer protocol that is inspected will take precedence over the TCP or UDP packet inspection. For example, if inspection is configured for FTP, all control channel information will be recorded in the state table, and all FTP traffic will be permitted back through the firewall if the control channel information is valid for the state of the FTP session. The fact that TCP inspection is configured is irrelevant.

With TCP and UDP inspection, packets entering the network must exactly match an existing session. The entering packets must have the same source or destination addresses and source or destination port numbers as the exiting packet (but reversed). Otherwise, the entering packets will be blocked at the interface.

Granular protocol inspection allows you to specify TCP or UDP ports by using the port-to-application mapping (PAM) table. This eliminates having to inspect all applications running under TCP or UDP and the need for multiple ACLs to filter the traffic.

Using the PAM table, you can pick an existing application or define a new one for inspection, thereby simplifying Access Control List (ACL) configuration.

ICMP Inspection

ICMP inspection sessions are done on the basis of the source address of the inside host that originates the ICMP packet. Dynamic ACLs are created for return ICMP packets of the allowed types (echo-reply, destination unreachable, time-exceeded, and timestamp reply) for each session. No port numbers associated with an ICMP session, and the permitted IP address of the return packet is a wild-card in the ACL. The wildcard address is because the IP address of the return packet cannot be known in advance for time-exceeded and destination-unreachable replies. These replies can come from intermediate devices rather than the intended destination.

Application-Layer Protocol Inspection

In general, if you configure inspection for an application-layer protocol, packets for that protocol should be permitted to exit the firewall (by configuring the correct ACL), and packets for that protocol will be allowed back in through the firewall only if they belong to a valid existing session. Each protocol packet is inspected to maintain information about the session state.

Java, H.323, RPC, SIP, and SMTP inspection have additional information, described in the next five sections. The table below lists the supported application-layer protocols.

Table 10: Protocol Keywords--Application-Layer Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Keyword</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Firewall</td>
<td>appfw</td>
</tr>
<tr>
<td>CU-SeeMe</td>
<td>cuseeme</td>
</tr>
</tbody>
</table>
### Java Inspection

Java inspection enables Java applet filtering at the firewall. Java applet filtering distinguishes between trusted and untrusted applets by relying on a list of external sites that you designate as "friendly." If an applet is from a friendly site, the firewall allows the applet through. If the applet is not from a friendly site, the applet will be blocked. Alternately, you could permit applets from all sites except sites specifically designated as "hostile."

---

#### Note

Before you configure Java inspection, you must configure a numbered standard access list that defines "friendly" and "hostile" external sites. You configure this numbered standard access list to permit traffic from friendly sites, and to deny traffic from hostile sites. If you do not configure a numbered standard access list, but use a "placeholder" access list in the `ip inspect name inspection-name http` command, all Java applets will be blocked.
Java blocking forces a strict order on TCP packets. To properly verify that Java applets are not in the response, a firewall will drop any TCP packet that is out of order. Because the network—not the firewall—determines how packets are routed, the firewall cannot control the order of the packets; the firewall can only drop and retransmit all TCP packets that are not in order.

Note

Context-Based Access Control (CBAC) does not detect or block encapsulated Java applets. Therefore, Java applets that are wrapped or encapsulated, such as applets in .zip or .jar format, are not blocked at the firewall. CBAC also does not detect or block applets loaded via FTP, gopher, or HTTP on a nonstandard port.

Caution

H.323 Inspection

If you want CBAC inspection to work with NetMeeting 2.0 traffic (an H.323 application-layer protocol), you must also configure inspection for TCP, as described in the chapter "Configuring Context-Based Access Control" in the *Cisco IOS Security Configuration Guide*. This requirement exists because NetMeeting 2.0 uses an additional TCP channel not defined in the H.323 specification.

RPC Inspection

RPC inspection allows the specification of various program numbers. You can define multiple program numbers by creating multiple entries for RPC inspection, each with a different program number. If a program number is specified, all traffic for that program number will be permitted. If a program number is not specified, all traffic for that program number will be blocked. For example, if you created an RPC entry with the NFS program number, all NFS traffic will be allowed through the firewall.

SIP Inspection

You can configure SIP inspection to permit media sessions associated with SIP-signaled calls to traverse the firewall. Because SIP is frequently used to signal both incoming and outgoing calls, it is often necessary to configure SIP inspection in both directions on a firewall (both from the protected internal network and from the external network). Because inspection of traffic from the external network is not done with most protocols, it may be necessary to create an additional inspection rule to cause only SIP inspection to be performed on traffic coming from the external network.

SMTP Inspection

SMTP inspection causes SMTP commands to be inspected for illegal commands. Packets with illegal commands are modified to a "xxxx" pattern and forwarded to the server. This process causes the server to send a negative reply, forcing the client to issue a valid command. An illegal SMTP command is any command except the following:

- DATA
- HELO
- HELP
- MAIL
- NOOP
- QUIT
- RCPT
Like SMTP, ESMTP inspection also causes the commands to be inspected for illegal commands. Packets with illegal commands are modified to a "xxxx" pattern and forwarded to the server. This process causes the server to send a negative reply, forcing the client to issue a valid command. An illegal ESMTP command is any command except the following:

- AUTH
- DATA
- EHLO
- ETRN
- HELO
- HELP
- MAIL
- NOOP
- QUIT
- RCPT
- RSET
- SAML
- SEND
- SOML
- VRFY

In addition to inspecting commands, the ESMTP firewall also inspects the following extensions via deeper command inspection:

- Message Size Declaration (SIZE)
- Remote Queue Processing Declaration (ETRN)
- Binary MIME (BINARYMIME)
- Command Pipelining
- Authentication
- Delivery Status Notification (DSN)
• Enhanced Status Code (ENHANCEDSTATUSCODE)
• 8bit-MIMEtransport (8BITMIME)

SMTP and ESMTP cannot exist simultaneously. An attempt to configure both protocols will result in an error message.

**Use of the urllfilter Keyword**

If you specify the urllfilter keyword, the Cisco IOS Firewall will interact with a URL filtering software to control web traffic for a given host or user on the basis of a specified security policy.

**Note**

Enabling HTTP inspection with or without any option triggers the Java applet scanner, which is CPU intensive. The only way to stop the Java applet scanner is to specify the java-list access-list option. Configuring URL filtering without enabling the java-list access-list option will severely impact performance.

**Use of the timeout Keyword**

If you specify a timeout for any of the transport-layer or application-layer protocols, the timeout will override the global idle timeout for the interface to which the set of inspection rules is applied.

If the protocol is TCP or a TCP application-layer protocol, the timeout will override the global TCP idle timeout. If the protocol is UDP or a UDP application-layer protocol, the timeout will override the global UDP idle timeout.

If you do not specify a timeout for a protocol, the timeout value applied to a new session of that protocol will be taken from the corresponding TCP or UDP global timeout value valid at the time of session creation.

The default ICMP timeout is deliberately short (10 seconds) due to the security hole that is opened by allowing ICMP packets with a wild-card source address back into the inside network. The timeout will occur 10 seconds after the last outgoing packet from the originating host. For example, if you send a set of 10 ping packets spaced one second apart, the timeout will expire in 20 seconds or 10 seconds after the last outgoing packet. However, the timeout is not extended for return packets. If a return packet is not seen within the timeout window, the gap will be closed and the return packet will not be allowed in. Although the default timeout can be made longer if desired, it is recommended that this value be kept relatively short.

**IP Fragmentation Inspection**

CBAC inspection rules can help protect hosts against certain denial-of-service attacks involving fragmented IP packets. Even though the firewall keeps an attacker from making actual connections to a given host, the attacker may still be able to disrupt services provided by that host. This is done by sending many noninitial IP fragments or by sending complete fragmented packets through a router with an ACL that filters the first fragment of a fragmented packet. These fragments can tie up resources on the target host as it tries to reassemble the incomplete packets.

Using fragmentation inspection, the firewall maintains an *interfragment state* (structure) for IP traffic. Noninitial fragments are discarded unless the corresponding initial fragment was permitted to pass through the firewall. Noninitial fragments received before the corresponding initial fragments are discarded.
Fragmentation inspection can have undesirable effects in certain cases, because it can result in the firewall discarding any packet whose fragments arrive out of order. There are many circumstances that can cause out-of-order delivery of legitimate fragments. Apply fragmentation inspection in situations where legitimate fragments, which are likely to arrive out of order, might have a severe performance impact.

Because routers running Cisco IOS software are used in a very large variety of networks, and because the CBAC feature is often used to isolate parts of internal networks from one another, the fragmentation inspection feature is not enabled by default. Fragmentation detection must be explicitly enabled for an inspection rule using the `ip inspect name` command. Unfragmented traffic is never discarded because it lacks a fragment state. Even when the system is under heavy attack with fragmented packets, legitimate fragmented traffic, if any, will still get some fraction of the firewall’s fragment state resources, and legitimate, unfragmented traffic can flow through the firewall unimpeded.

**Application Firewall Provisioning**

Application firewall provisioning allows you to configure your Cisco IOS Firewall to detect and prohibit a specific protocol type of traffic.

Most firewalls provide packet filtering capabilities that simply permit or deny traffic without inspecting the data stream; the Cisco IOS application firewall can detect whether a packet is in compliance with a given HTTP protocol. If the packet is determined to be unauthorized, it will be dropped, the connection will be reset, and a syslog message will be generated, as appropriate.

**User-Defined Applications**

You can define your own applications and enter them into the PAM table using the `ip port-map` command. Then you set up your inspection rules by inserting your user-defined application as a value for the `protocol` argument in the `ip inspect name` command.

**Session Limiting**

Users can limit the number of established firewall sessions that a firewall rule creates by setting the "max-sessions" threshold. A session counter is maintained for each firewall interface. When a session count exceeds the specified threshold, an alert FW-4-SESSION_THRESHOLD_EXCEEDED message is logged to the syslog server and no new sessions can be created.

**Examples**

The following example causes the software to inspect TCP sessions and UDP sessions, and to specifically allow CU-SeeMe, FTP, and RPC traffic back through the firewall for existing sessions only. For UDP traffic, audit-trail is on. For FTP traffic, the idle timeout is set to override the global TCP idle timeout. For RPC traffic, program numbers 100003, 100005, and 100021 are permitted.

```
ip inspect name myrules tcp
ip inspect name myrules udp audit-trail on
ip inspect name myrules cuseeme
ip inspect name myrules ftp timeout 120
ip inspect name myrules rpc program-number 100003
ip inspect name myrules rpc program-number 100005
ip inspect name myrules rpc program-number 100021
```

The following example adds fragment checking to software inspection of TCP and UDP sessions for the rule named "myrules." In this example, the firewall software will allocate 100 state structures, and the timeout value for dropping unassembled packets is set to 4 seconds. If 100 initial fragments for 100 different packets are sent through the router, all of the state structures will be used up. The
initial fragment for packet 101 will be dropped. Additionally, if the number of free state structures (structures available for use by unassembled packets) drops below the threshold values, 32 or 16, the timeout value is automatically reduced to 2 or 1, respectively. Changing the timeout value frees up packet state structures more quickly.

    ip inspect name myrules tcp
    ip inspect name myrules udp audit-trail on
    ip inspect name myrules cuseeme
    ip inspect name myrules ftp timeout 120
    ip inspect name myrules rpc program-number 100003
    ip inspect name myrules rpc program-number 100005
    ip inspect name myrules rpc program-number 100021
    ip inspect name myrules fragment max 100 timeout 4

The following firewall and SIP example shows how to allow outside-initiated calls and internal calls. For outside-initiated calls, an ACL needs to be accessed to allow for the traffic from the initial signaling packet from outside. Subsequent signaling and media channels will be allowed by the inspection module.

    ip inspect name voip sip
    interface FastEthernet0/0
      ip inspect voip in
    !
    interface FastEthernet0/1
      ip inspect voip in
      ip access-group 100 in
    !
      access-list 100 permit udp host <gw ip> any eq 5060
      access-list 100 permit udp host <proxy ip> any eq 5060
      access-list deny ip any any

The following example shows two configured inspections named fw_only and fw_urlf; URL filtering will work only on the traffic that is inspected by fw_urlf. Note that the java-list access-list option has been enabled, which disables java scanning.

    ip inspect name fw_only http java-list 51 timeout 30
    interface e0
      ip inspect fw_only in
    !
    ip inspect name fw_urlf http java-list 51 urlfilter timeout 30
    interface e1
      ip inspect fw_urlf in

The following example shows how to define the HTTP application firewall policy mypolicy. This policy includes all supported HTTP policy rules. This example also includes sample output from the show appfw configuration and show ip inspect config commands, which allow you to verify the configured setting for the application policy.

    ! Define the HTTP policy.
    appfw policy-name mypolicy
    application http
      strict-http action allow alarm
      content-length maximum 1 action allow alarm
      content-type-verification match-req-rsp action allow alarm
      max-header-length request 1 response 1 action allow alarm
      max-uri-length 1 action allow alarm
      port-misuse default action allow alarm
request-method rfc default action allow alarm
request-method extension default action allow alarm
transfer-encoding type default action allow alarm

! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http

! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
ip inspect firewall in

! Issue the **show appfw configuration**
cmd and the **show ip inspect config**
cmd after the inspection rule "mypolicy" is applied to all incoming HTTP traffic on the
FastEthernet0/0 interface.

Router# **show appfw configuration**

Application Firewall Rule configuration
Application Policy name mypolicy
Application http
  strict-http action allow alarm
  content-length minimum 0 maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request length 1 response length 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding default action allow alarm

Router# **show ip inspect config**

Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name firewall
http alert is on audit-trail is off timeout 3600

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip inspect</td>
<td>Applies a set of inspection rules to an interface.</td>
</tr>
<tr>
<td>ip inspect alert-off</td>
<td>Disables CBAC alert messages.</td>
</tr>
<tr>
<td>ip inspect audit trail</td>
<td>Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.</td>
</tr>
</tbody>
</table>
**ip inspect one-minute high**

To define the rate of new unestablished sessions that will cause the software to start deleting half-open sessions, use the `ip inspect one-minute high` command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the `no` form of this command.

```
ip inspect one-minute high number [vrf vrf-name]
no ip inspect one-minute high
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Specifies the rate of new unestablished TCP sessions that will cause the software to start deleting half-open sessions. The default is 500 half-open sessions.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Defines the information only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

500 half-open sessions

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 P</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>vrf vrf-name</code> keyword/argument pair was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.3(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, “half-open” means that the session has not reached the established state. For User Datagram Protocol (UDP), “half-open” means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the `one-minute high` number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the `one-minute low` number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. (The rate is calculated as an exponentially decayed rate.)

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.
Examples

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ip inspect one-minute high 1000
ip inspect one-minute low 950
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip inspect one-minute low</td>
<td>Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.</td>
</tr>
<tr>
<td>ip inspect max-incomplete high</td>
<td>Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.</td>
</tr>
<tr>
<td>ip inspect max-incomplete low</td>
<td>Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.</td>
</tr>
<tr>
<td>ip inspect tcp max-incomplete host</td>
<td>Specifies the threshold and blocking time values for TCP host-specific DoS detection and prevention.</td>
</tr>
</tbody>
</table>
**ip inspect one-minute low**

To define the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions, use the `ip inspect one-minute low` command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the `no` form of this command.

```
ip inspect one-minute low number [vrf vrf-name]
no ip inspect one-minute low
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>number</strong></td>
</tr>
<tr>
<td>Specifies the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions. The default is 400 half-open sessions.</td>
</tr>
<tr>
<td><strong>vrf vrf-name</strong></td>
</tr>
<tr>
<td>(Optional) Defines the information only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

400 half-open sessions

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2P</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>vrf vrf-name</code> keyword/argument pair was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, “half-open” means that the session has not reached the established state. For User Datagram Protocol (UDP), “half-open” means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the `one-minute high` number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the `one-minute low` number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. (The rate is calculated as an exponentially decayed rate.)

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.
## Examples

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ip inspect one-minute high 1000
ip inspect one-minute low 950
```

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip inspect max-incomplete high</code></td>
<td>Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.</td>
</tr>
<tr>
<td><code>ip inspect max-incomplete low</code></td>
<td>Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.</td>
</tr>
<tr>
<td><code>ip inspect one-minute high</code></td>
<td>Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.</td>
</tr>
<tr>
<td><code>ip inspect tcp max-incomplete host</code></td>
<td>Specifies the threshold and blocking time values for TCP host-specific DoS detection and prevention.</td>
</tr>
</tbody>
</table>
ip inspect tcp block-non-session

To block packets that do not belong to the existing firewall TCP sessions in the inbound and outbound directions, use the `ip inspect tcp block-non-session` command in global configuration mode. To return to the default state, use the `no` form of this command.

```
ip inspect tcp block-non-session [vrf vrf-name]
no inspect tcp block-non-session [vrf vrf-name]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf</code></td>
<td>(Optional) Declares a specific VPN routing/forwarding instance (VRF).</td>
</tr>
<tr>
<td><code>vrf-name</code></td>
<td>(Optional) Name of the VRF.</td>
</tr>
</tbody>
</table>

### Command Default

TCP packets that do not belong to an existing TCP session on the firewall are allowed through the firewall.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(6)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>This command was integrated into Release 12.3(6)T.</td>
</tr>
<tr>
<td>12.3(7)XI</td>
<td>This command was integrated into the Release 12.3(7)XI.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>vrf</code> keyword and <code>vrf-name</code> argument were added.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command will deny TCP packets that do not belong to an existing TCP session the firewall knows about. To be applicable, the following conditions must be met:

- The TCP packets should traverse interfaces where a firewall rule is applicable.
- The TCP packets should be non-connection initiating (that is, packets without the SYN bit set in them). For connection initiating packets, the existing rules of session creation would apply.

### Examples

The following example shows how to configure the firewall to block any externally initiated TCP sessions:

```
Router> enable
Router# config terminal
Router(config)
# ip inspect tcp block-non-session
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip inspect log drop-pkt</code></td>
<td>Logs all packets dropped by the firewall.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ip inspect tcp finwait-time</td>
<td>Defines how long a TCP session will still be managed after the firewall detects a FIN-exchange.</td>
</tr>
<tr>
<td>ip inspect tcp idle-time</td>
<td>Specifies the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity).</td>
</tr>
<tr>
<td>ip inspect tcp max-incomplete host</td>
<td>Specifies threshold and blocking time values for TCP host-specific (DoS) detection and prevention.</td>
</tr>
<tr>
<td>ip inspect tcp reassembly</td>
<td>Sets parameters that define how Cisco IOS Firewall application inspection and Cisco IOS IPS will handle out-of-order TCP packets.</td>
</tr>
<tr>
<td>ip inspect tcp synwait-time</td>
<td>Defines how long the software will wait for a TCP session to reach the established state before dropping the session.</td>
</tr>
<tr>
<td>ip inspect udp idle-time</td>
<td>Specifies the UDP idle timeout (the length of time for which a UDP session will still be managed while there is no activity).</td>
</tr>
</tbody>
</table>
ip inspect tcp finwait-time

To define how long a TCP session will be managed after the firewall detects a finish (FIN)-exchange, use the **ip inspect tcp finwait-time** command in global configuration mode. To reset the timeout to the default of 5 seconds, use the **no** form of this command.

**Syntax**

```
[36x677]ip inspect tcp finwait-time seconds [vrf vrf-name]
no ip inspect tcp finwait-time
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>seconds</strong></td>
<td>Specifies how long a TCP session will be managed after the firewall detects a FIN-exchange. The default is 5 seconds. Valid values are from 1 to 2147483. If the FIN-exchange completes within the configured finwait time, the connection is closed normally.</td>
</tr>
<tr>
<td><strong>vrf vrf-name</strong></td>
<td>(Optional) Defines the information only for the specified VPN routing and forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

The default management time is 5 seconds.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 P</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>This command was modified. The <strong>vrf vrf-name</strong> keyword and argument pair was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.33(SRA).</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the software detects a valid TCP packet that is the first in a session, and if Context-Based Access Control (CBAC) inspection is configured for the protocol of the packet, the software establishes state information for the new session.

Use this command to define how long a TCP session state information will be maintained after the firewall detects a FIN-exchange for the session. The FIN-exchange occurs when the TCP session is ready to close. In a TCP connection, the client and the server terminate their end of the connection by sending a FIN message. The time that the client and the server wait for their FIN message to be acknowledged by each other before closing the sequence during a TCP connection is called the finwait time. The timeout that you set for the finwait time is referred to as the finwait timeout.

The global value specified for the finwait timeout applies to all TCP sessions inspected by CBAC.

**Examples**

The following example shows how to change the finwait timeout to 10 seconds:

```
ip inspect tcp finwait-time 10
```

The following example shows how to change the finwait timeout back to the default (5 seconds):

```
o ip inspect tcp finwait-time
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip inspect</code></td>
<td>Displays CBAC configuration and session information.</td>
</tr>
</tbody>
</table>
ip inspect tcp idle-time

To specify the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity), use the `ip inspect tcp idle-time` command in global configuration mode. To reset the timeout to the default of 3600 seconds (1 hour), use the `no` form of this command.

```
ip inspect tcp idle-time seconds [vrf vrf-name]
no ip inspect tcp idle-time
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>Specifies the length of time, in seconds, for which a TCP session will still be managed while there is no activity. The default is 3600 seconds (1 hour).</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Specifies the TCP idle timer only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

3600 seconds (1 hour)

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 P</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>vrf vrf-name</code> keyword/argument pair was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.33SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the software detects a valid TCP packet that is the first in a session, and if Context-based Access Control (CBAC) inspection is configured for the packet’s protocol, the software establishes state information for the new session.

If the software detects no packets for the session for a time period defined by the TCP idle timeout, the software will not continue to manage state information for the session.

The global value specified for this timeout applies to all TCP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the `ip inspect name` (global configuration) command.

**Note**

This command does not affect any of the currently defined inspection rules that have explicitly defined timeouts. Sessions created based on these rules still inherit the explicitly defined timeout value. If you change the TCP idle timeout with this command, the new timeout will apply to any new inspection rules you define or to any existing inspection rules that do not have an explicitly defined timeout. That is, new sessions based on these rules (having no explicitly defined timeout) will inherit the global timeout value.
Examples

The following example sets the global TCP idle timeout to 1800 seconds (30 minutes):

```
ip inspect tcp idle-time 1800
```

The following example sets the global TCP idle timeout back to the default of 3600 seconds (one hour):

```
no ip inspect tcp idle-time
```
ip inspect tcp max-incomplete host

To specify threshold and blocking time values for TCP host-specific denial-of-service (DoS) detection and prevention, use the `ip inspect tcp max-incomplete host` command in global configuration mode. To reset the threshold and blocking time to the default values, use the `no` form of this command.

`ip inspect tcp max-incomplete host number block-time minutes [vrf vrf-name]`
`no ip inspect tcp max-incomplete host`

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Specifies how many half-open TCP sessions with the same host destination address can exist at a time, before the software starts deleting half-open sessions to the host. Use a number from 1 to 250. The default is 50 half-open sessions.</td>
</tr>
<tr>
<td>block-time</td>
<td>Specifies blocking of connection initiation to a host.</td>
</tr>
<tr>
<td>minutes</td>
<td>Specifies how long the software will continue to delete new connection requests to the host. The default is 0 minutes.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies the information only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

50 half-open sessions and 0 minutes

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 P</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>vrf vrf-name</code> keyword/argument pair was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An unusually high number of half-open sessions with the same destination host address could indicate that a denial-of-service attack is being launched against the host. For TCP, “half-open” means that the session has not reached the established state.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (the `max-incomplete host` number), the software will delete half-open sessions according to one of the following methods:

- If the `block-time minutes` timeout is 0 (the default):

  The software will delete the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.

- If the `block-time minutes` timeout is greater than 0:
The software will delete all existing half-open sessions for the host, and then block all new connection requests to the host. The software will continue to block all new connection requests until the block-time expires. The software also sends syslog messages whenever the max-incomplete host number is exceeded and when blocking of connection initiations to a host starts or ends. The global values specified for the threshold and blocking time apply to all TCP connections inspected by Context-based Access Control (CBAC).

**Examples**

The following example changes the max-incomplete host number to 40 half-open sessions, and changes the block-time timeout to 2 minutes:

```plaintext
ip inspect tcp max-incomplete host 40 block-time 2
```

The following example resets the defaults (50 half-open sessions and 0 minutes):

```plaintext
no ip inspect tcp max-incomplete host
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip inspect max-incomplete high</td>
<td>Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.</td>
</tr>
<tr>
<td>ip inspect max-incomplete low</td>
<td>Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.</td>
</tr>
<tr>
<td>ip inspect one-minute high</td>
<td>Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.</td>
</tr>
<tr>
<td>ip inspect one-minute low</td>
<td>Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.</td>
</tr>
</tbody>
</table>
ip inspect tcp reassembly

To set parameters that define how Cisco IOS Firewall application inspection and Cisco IOS Intrusion Prevention System (IPS) will handle out-of-order TCP packets, use the `ip inspect tcp reassembly` command in global configuration mode. To disable at least one defined parameter, use the `no` form of this command.

```
ip inspect tcp reassembly {alarm |on|off|memory limit size-in-kb|queue length number-of-packets|timeout seconds} [vrf vrf-name]
oip inspect tcp reassembly {alarm|queue length|timeout|memory limit} [vrf vrf-name]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarm</td>
<td>on</td>
</tr>
<tr>
<td>memory</td>
<td>Specifies the memory use allowed by the TCP reassembly module.</td>
</tr>
<tr>
<td>limit size-in-kb</td>
<td>Specifies the limit of out of order queue size.</td>
</tr>
<tr>
<td>queue</td>
<td>Specifies the out of order queue parameters.</td>
</tr>
<tr>
<td>length number-of-packets</td>
<td>Maximum number of out-of-order packets that can be held per queue (buffer). (There are two queues per session.) Available value range: 0 to 1024. Default value: 16. <strong>Note</strong> If the queue length is set to 0, all out-of-order packets are dropped; that is, TCP out-of-order packet buffering and reassembly is disabled.</td>
</tr>
<tr>
<td>timeout seconds</td>
<td>Number of seconds the TCP reassembly module will hold out-of-order segments that are waiting for the first segment missing in the sequence. After the timeout timer has expired, a retry timer is started. The value for the retry timer is four times the configured timeout value.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>Specifies the VPN routing and forwarding (VRF) parameter and name.</td>
</tr>
</tbody>
</table>

**Command Default**
- Queue length: 16
- Memory Limit: 1024 kilobytes
- Alarm: on

**Command Modes**
- Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(11)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

The queue length Value

The value specified for the queue length is applicable for two queues per session: one queue is for the initiator traffic and the other queue is for the responder traffic. For example, the default queue size is 16. Thus, up to 16 packets can be held per queue, so 16 packets per queue results in a maximum of 32 packets per session.

When the maximum queue length value is reached, the packet being switched is dropped unless it is the packet that will be processed by a firewall or IPS. If the packet is dropped, a syslog message, which explains why the packet was dropped, will be generated. (To generate syslog messages, you must have the alarm option set to “on.”)

The timeout Value

When a timer expires for the first time, the packets in the queue are not deleted. However, after the retry timer expires, the session is deleted, a syslog message is generated, and all unprocessed, out-of-order packets still in the queue are deleted.

The memory limit Value

When the limit for TCP reassembly memory is reached, packets from the reassembly queue of the current session are released so incoming packets can be accepted. Packets from the end of the queue are released to ensure that they are farthest away from the hole that is to be filled. However, if the queue is empty and the maximum memory has been reached, the incoming packet is dropped.

The alarm Value

If an alarm value is not configured, the value is set to “on,” unless the `ip inspect alarm` command is enabled and set to off; thus, syslog messages related to TCP connections will not be generated. However, if the alarm value for this command is set to “on” and the `ip inspect alarm` command is set to “off,” the value of the `ip inspect alarm` command is ignored and syslog messages are generated.

The alarm value is independent of and in addition to the syslog messages that can be enabled for a Cisco IOS Firewall or Cisco IOS IPS.

**Examples**

The following examples show how to instruct Cisco IOS IPS how to handle out-of-order packets for TCP connections:

```
Router(config)#
ip inspect tcp reassembly queue length 18
Router(config)#
ip inspect tcp reassembly memory limit 200
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip inspect tcp block-non-session</code></td>
<td>Blocks packets that do not belong to the existing firewall TCP sessions in the inbound and outbound directions.</td>
</tr>
</tbody>
</table>
**ip inspect tcp synwait-time**

To define how long the software will wait for a TCP session to reach the established state before dropping the session, use the `ip inspect tcp synwait-time` command in global configuration mode. To reset the timeout to the default of 30 seconds, use the `no` form of this command.

```
ip inspect tcp synwait-time seconds [vrf vrf-name]
o ip inspect tcp synwait-time
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Specifies how long, in seconds, the software will wait for a TCP session to reach the established state before dropping the session. The default is 30 seconds.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Defines the information only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

30 seconds

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 P</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>vrf vrf-name</code> keyword/argument pair was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to define how long Cisco IOS software will wait for a TCP session to reach the established state before dropping the session. The session is considered to have reached the established state after the first synchronize sequence number (SYN) bit of the session is detected.

The global value specified for this timeout applies to all TCP sessions inspected by Context-based Access Control (CBAC).

**Examples**

The following example changes the synwait timeout to 20 seconds:

```
ip inspect tcp synwait-time 20
```

The following example changes the synwait timeout back to the default (30 seconds):

```
o ip inspect tcp synwait-time
```
### ip inspect tcp window-scale-enforcement loose

To configure Cisco IOS software to disable the window scale option check for a TCP packet that has an invalid window scale option under the Context-Based Access Control (CBAC) firewall, use the `ip inspect tcp window-scale-enforcement loose` command in global configuration mode. To return to the command default, use the `no` form of this command.

```plaintext
ip inspect tcp window-scale-enforcement loose
no ip inspect tcp window-scale-enforcement loose
```

#### Command Default

The strict window scale option check is enabled in the firewall by default.

#### Command Modes

Global configuration (config)

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

The window scale extension expands the definition of the TCP window to 32 bits and then uses a scale factor to carry this 32-bit value in the 16-bit Window field of the TCP header. Cisco IOS software enforces strict checking of the TCP window scale option. See section 2 of RFC1323, “TCP Window Scale Option,” for more information on this function.

There are occasions when a server may be using a non-RFC compliant TCP/IP protocol stack. In this case, the initiator does not offer the window scale option, but the responder has the option enabled with a window scale factor that is not zero.

Cisco IOS administrators who experience issues with a noncompliant server may not have control over the client to which they need to connect. Disabling the Cisco IOS firewall to connect to the noncompliant server is not desirable and may fail if each endpoint cannot agree on the window scaling factor to use for its respective receive window.

The `ip inspect tcp window-scale-enforcement loose` command is used in global configuration mode to allow noncompliant window scale negotiation and works without the firewall being disabled to access the noncompliant servers. This command works under the CBAC firewall, which intelligently filters TCP and UDP packets based on application-layer protocol session information. CBAC inspects traffic that travels through the firewall to discover and manage state information for TCP and UDP sessions. CBAC is configured using an inspect rule only on interfaces. This state information is used to create temporary openings in the firewall's access lists to allow return traffic and additional data connections for permissible sessions. Traffic entering or leaving the configured interface is inspected based on the direction that the inspect rule was applied.

#### Examples

The following example configures the IOS to disable the window scale option check in the CBAC firewall for a TCP packet that has an invalid window scale option:

```plaintext
Router(config)# ip inspect tcp window-scale-enforcement loose
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip inspect tcp synwait-time</code></td>
<td>Configures the length of time the software waits for a TCP session to reach the established state before dropping the session.</td>
</tr>
</tbody>
</table>
**ip inspect udp idle-time**

To specify the User Datagram Protocol (UDP) idle timeout (the length of time for which a UDP “session” will still be managed while there is no activity), use the `ip inspect udp idle-time` command in global configuration mode. To reset the timeout to the default of 30 seconds, use the `no` form of this command.

```
ip inspect udp idle-time seconds [vrf vrf-name]
o sip inspect udp idle-time
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>Specifies the length of time a UDP “session” will still be managed while there is no activity. The default is 30 seconds.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Specifies the UDP idle timeout only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

30 seconds

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 P</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>vrf vrf-name</code> keyword/argument pair was added.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the software detects a valid UDP packet, if Context-based Access Control (CBAC) inspection is configured for the packet’s protocol, the software establishes state information for a new UDP “session.” Because UDP is a connectionless service, there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining if the packet is similar to other UDP packets (for example, it has similar source or destination addresses) and if the packet was detected soon after another similar UDP packet.

If the software detects no UDP packets for the UDP session for the a period of time defined by the UDP idle timeout, the software will not continue to manage state information for the session.

The global value specified for this timeout applies to all UDP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the `ip inspect name` command.
This command does not affect any of the currently defined inspection rules that have explicitly defined timeouts. Sessions created based on these rules still inherit the explicitly defined timeout value. If you change the UDP idle timeout with this command, the new timeout will apply to any new inspection rules you define or to any existing inspection rules that do not have an explicitly defined timeout. That is, new sessions based on these rules (having no explicitly defined timeout) will inherit the global timeout value.

**Examples**

The following example sets the global UDP idle timeout to 120 seconds (2 minutes):

```
ip inspect udp idle-time 120
```

The following example sets the global UDP idle timeout back to the default of 30 seconds:

```
oip inspect udp idle-time
```
ip inspect waas enable

To enable the zone-based firewall to inspect Cisco Wide Area Application Service (WAAS) traffic, use the `ip inspect waas enable` command in global configuration mode. To disable the firewall inspection of WAAS traffic, use the `no` form of this command.

```
ip inspect waas enable
no ip inspect waas enable
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

WAAS traffic inspection is not enabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 12.4(11)T2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Because the WAAS automatic discovery process uses TCP options before sending UDP traffic, the firewall must be configured to pass TCP options. Use the `ip inspect waas enable` command to configure the firewall to allow TCP options.

**Examples**

The following example shows how to enable the firewall inspection of WAAS traffic:

```
Device# configure terminal
Device(config)# ip inspect waas enable
```
integrity

To specify one or more integrity algorithms for an Internet Key Exchange Version 2 (IKEv2) proposal, use the `integrity` command in IKEv2 proposal configuration mode. To remove the configuration of the hash algorithm, use the `no` form of this command.

```
integrity integrity_type
no integrity
```

**Syntax Description**

| `integrity_type` | Specifies the hash algorithm. |

**Command Default**

The default integrity algorithm is used.

**Command Modes**

IKEv2 proposal configuration (config-ikev2-proposal)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(2)T</td>
<td>This command was modified. The <code>sha256</code> and <code>sha384</code> keywords were added.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use this command to specify the integrity algorithm to be used in an IKEv2 proposal. The default integrity algorithms in the default proposal are SHA-1 and MD5. The integrity algorithms can be one of the following:

<table>
<thead>
<tr>
<th>Integrity Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sha1</code></td>
<td>Specifies Secure Hash Algorithm (SHA-1 - HMAC variant) as the hash algorithm (No longer recommended).</td>
</tr>
<tr>
<td><code>sha256</code></td>
<td>Specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm.</td>
</tr>
<tr>
<td><code>sha384</code></td>
<td>Specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.</td>
</tr>
<tr>
<td><code>sha512</code></td>
<td>Specifies SHA-2 family 512-bit (HMAC variant) as the hash algorithm.</td>
</tr>
</tbody>
</table>
Integrity Type | Description |
---|---|
md5 | Specifies Message-Digest algorithm 5 (MD5 - HMAC variant) as the hash algorithm.

You cannot selectively remove an integrity algorithm when multiple integrity algorithms are configured.

Note
Suites-B adds support for the SHA-2 family (HMAC variant) hash algorithm used to authenticate packet data and verify the integrity verification mechanisms for the IKEv2 proposal configuration. HMAC is a variant that provides an additional level of hashing.

Examples
The following example configures an IKEv2 proposal with the MD5 integrity algorithm:

```
Device(config)# crypto ikev2 proposal proposal1
Device(config-ikev2-proposal)# integrity md5
```

Related Commands
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2 proposal</td>
<td>Defines an IKEv2 proposal.</td>
</tr>
<tr>
<td>encryption (ikev2 proposal)</td>
<td>Specifies the encryption algorithm in an IKEv2 proposal.</td>
</tr>
<tr>
<td>group (ikev2 proposal)</td>
<td>Specifies the Diffie-Hellman group identifier in an IKEv2 proposal.</td>
</tr>
<tr>
<td>show crypto ikev2 proposal</td>
<td>Displays the parameters for each IKEv2 proposal.</td>
</tr>
</tbody>
</table>
### ip interface

To configure a virtual gateway IP interface on a Secure Socket Layer Virtual Private Network (SSL VPN) gateway, use the `ip interface` command in webvpn gateway configuration mode. To disable the configuration, use the `no` form of this command.

```plaintext
ip interface type number [port {443|port-number}]
no ip interface
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>number</td>
<td>Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>port</td>
<td>(Optional) Configures a specific port on the gateway.</td>
</tr>
<tr>
<td>443</td>
<td>(Optional) Configures the default secure port.</td>
</tr>
<tr>
<td>port-number</td>
<td>(Optional) Port number to be configured on the SSL VPN gateway. Range: 1025 to 65535. Default: 443.</td>
</tr>
</tbody>
</table>

#### Command Default

The command is disabled. The virtual gateway IP address is not configured.

#### Command Modes

Webvpn gateway configuration (config-webvpn-gateway)

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

The `ip interface` command is used to configure a interface on a SSL VPN gateway. You can use this command to configure the WebVPN gateway to retrieve the IP address from an interface, and if you do not want to configure the IP address manually. This command is useful when the public interface is Dynamic Host Configuration Protocol (DHCP) and you do not know the IP address or when the IP address gets changed.

If the `ip interface` command is not configured then the WebVPN will use the IP address configured using the `ip address` command.

#### Examples

The following example shows how to configure a virtual gateway IP interface on port 1036 of an SSL VPN gateway:

```plaintext
Router# configure terminal
Router(config)# webvpn gateway gateway1
Router(config-webvpn-gateway)# ip interface FastEthernet 0/1 port 1036
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Configures a proxy IP address on an SSL VPN gateway.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>webvpn gateway</td>
<td>Defines an SSL VPN gateway and enters WebVPN gateway configuration mode.</td>
</tr>
</tbody>
</table>
ip ips

To apply an Intrusion Prevention System (IPS) rule to an interface, use the `ip ips` command in interface configuration mode. To remove an IPS rule from an interface direction, use the `no` form of this command.

```
ip ips  ips-name  {in|out}
no ip ips  ips-name  {in|out}
```

**Syntax Description**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ips-name</code></td>
<td>Name of IPS signature definition file (SDF).</td>
</tr>
<tr>
<td><code>in</code></td>
<td>Applies IPS to inbound traffic.</td>
</tr>
<tr>
<td><code>out</code></td>
<td>Applies IPS to outbound traffic.</td>
</tr>
</tbody>
</table>

**Command Default**

By default, IPS signatures are not applied to an interface or direction.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>The command name was changed from the <code>ip audit</code> command to the <code>ip ips</code> command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ip ips` command loads the SDF onto the router and builds the signature engines when IPS is applied to the first interface.

**Note**

The router prompt disappears while the signatures are loading and the signature engines are building. It will reappear after these tasks are complete. Depending on your platform and how many signatures are being loaded, building the signature engine can take several minutes. It is recommended that you enable logging messages so you can monitor the engine building status.

The `ip ips` command replaces the `ip audit` command. If the `ip audit` command is part of an existing configuration, IPS will interpret it as the `ip ips` command.

**Examples**

The following example shows the basic configuration necessary to load the `attack-drop.sdf` file onto a router running Cisco IOS IPS. Note that the configuration is almost the same as when you load the default signatures onto a router, except for the `ip ips sdf location` command, which specifies the `attack-drop.sdf` file.

```
! ip ips sdf location disk2:attack-drop.sdf
ip ips name MYIPS
! interface GigabitEthernet0/1
  ip address 10.1.1.16 255.255.255.0
```
The following example shows how to configure the router to load and merge the attack-drop.sdf file with the default signatures. After you have merged the two files, it is recommended to copy the newly merged signatures to a separate file. The router can then be reloaded (via the reload command) or reinitialized to so as to recognize the newly merged file (as shown the following example)

```
!  
ip ips name MYIPS  
!  
interface GigabitEthernet0/1  
ip address 10.1.1.16 255.255.255.0  
ip ips MYIPS in  
duplex full  
speed 100  
media-type rj45  
no negotiation auto  
!  
! Merge the flash-based SDF (attack-drop.sdf) with the built-in signatures.  
! Configure the router to use the new file, my-signatures.sdf
```
**ip ips auto-update**

To enable automatic signature updates for Cisco IOS Intrusion Prevention System (IPS), use the `ip ips auto-update` command in global configuration mode. To revert back to the default value, use the `no` form of this command.

```plaintext
ip ips auto-update
no ip ips auto-update
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The default value is defined in the signature definition XML.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Automatic signature updates allow users to override the existing IPS configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Use the `ip ips auto-update` command to enable Cisco IOS IPS to automatically update the signature file on the system. When enabling automatic signature updates, it is recommended that you ensure the following configuration guidelines have been met:

- The router’s clock is set up with the proper relative time.
- The frequency for Cisco IOS IPS to obtain updated signature information has been defined (through the `occur-at` command).
- Automatic signature updates can be enabled from Cisco.com by using the `cisco` command. This command cannot be used in conjunction with the `url` command.
- The URL in which to retrieve the Cisco IOS IPS signature configuration files has been specified (through the `url` command).
- Optionally, the username and password in which to access the files from the server has been specified (through the `username` command). The `username` command would be optional in this case if the username and password command were previously configured through the `ips signature update cisco` command in Privileged EXEC mode. The user name and password must be configured for updating signatures directly from Cisco.com.

**The Default Value**

A user or a management station can override the default value through the `category` command or the `signature` command; a value set with either of these commands will be saved as the delta value. The no form of the `ip ips auto-update` command will remove the delta value and revert back to the default value in the definition XML.

**Setting Time for Auto Updates**
Cisco IOS time can be updated through the hardware clock or the software configurable clock (which ever option is available on your system). Although Network Time Protocol (NTP) is typically used for automated time synchronization, Cisco IOS IPS updates use the local clock resources as a reference for update intervals. Thus, NTP should be configured to update the local time server of the router, as appropriate.

Examples

The following example shows how to configure automatic signature updates and issue the `show ip ips auto-update` command to verify the configuration. In this example, the signature package file is pulled from the TFTP server at the third hour of the 5 day of the month, at the 56th minute of this hour. (Note that adjustments are made for months without 31 days and daylight savings time.)

```
Router# clock set 10:38:00 20 apr 2006
Router# ip ips auto-update
Router(config-ips-auto-update)# occur-at monthly 5 56 3
Router# show ip ips auto-update
```

```
IPS Auto Update Configuration
URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
Username : not configured
Password : not configured
Auto Update Intervals
  minutes (0-59) : 56
  hours (0-23) : 3
  days of month (1-31) : 5
  days of week: (0-6) :
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>occur-at</strong></td>
<td>Defines the frequency in which Cisco IOS IPS obtains updated signature information.</td>
</tr>
<tr>
<td><strong>cisco</strong></td>
<td>Enables automatic signature updates from Cisco.com.</td>
</tr>
<tr>
<td><strong>url (ips-autoupdate)</strong></td>
<td>Defines a location in which to retrieve the Cisco IOS IPS signature configuration files.</td>
</tr>
<tr>
<td><strong>username (ips-autoupdate)</strong></td>
<td>Defines a username and password in which to access signature files from the server.</td>
</tr>
</tbody>
</table>
ip ips config location

To specify the location in which the router will save signature information, use the `ip ips config location` command in global configuration mode. To remove the specified location, use the `no` form of this command.

```
ip ips config location url
no ip ips config location
```

**Syntax Description**

| `url` | Location where the signature file is saved. Available URL options:
|       | • Local flash, such as flash:sig.xml
|       | • FTP server, such as ftp://myuser:mypass@ftp_server.sig.xml
|       | • rcp, such as rcp://myuser@rcp_server/sig.xml
|       | • TFTP server, such as tftp://tftp_server/sig.xml

**Note** If the specified location is a URL, such as an FTP server, the user must have writer privileges.

**Command Default**

No configuration files are saved.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before configuring the `ip ips config location` command, you must create a directory for the config location via the `mkdir` command.

The `ip ips config location` command configures a Cisco IOS Intrusion Prevention System (IPS) signature location, which tells Cisco IOS IPS where to save signature information.

The configuration location is used to restore the IPS configuration in cases such as router reboots or IPS becoming disabled or reenabled. Files, such as signature definitions, signature-type definitions, and signature category information, are written in XML format, compressed, and saved to the specified IPS signature location.

**Note**

If a location is not specified, or if a location is removed via the `no` form, no files will be saved.
The **ip ips config location** command replaces the **ip ips sdf location** command.

**Examples**

The following example shows how to instruct the router to save all signature information to the directory “flash:/ips5”:

```bash
Router# mkdir flash:/ips5
Create directory filename [ips5]?
Created dir flash:/ips5
Router#
Router#
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips name MYIPS
Router(config)# ip ips config location flash:/ips5
Router(config)# ip ips signature-category
Router(config-ips-category)# category all
Router(config-ips-category-action)# retired true
Router(config-ips-category-action)# exit
Router(config-ips-category)# category ios_ips advanced
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# exit
Router(config-ips-category)# exit
Do you want to accept these changes? [confirm]
Router(config)# d
*Nov 14 2006 17:16:42 MST: Applying Category configuration to signatures ..
Router(config)#
```
ip ips deny-action ips-interface

To create an access control list (ACL) filter for the deny actions (“denyFlowInline” and “denyConnectionInline”) on the intrusion prevention system (IPS) interface rather than ingress interface, use the `ip ips deny-action ips-interface` command in global configuration mode. To return to the default, use the `no` form of this command.

```
ip ips deny-action ips-interface
no ip ips deny-action ips-interface
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

ACLs filter for the deny actions are applied to the ingress interface.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ip ips deny-action ips-interface` command to change the default behavior of the ACL filters that are created for the deny actions.

---

**Note**

You should configure this command only if at least one signature is configured to use the supported deny actions (denyFlowInline and denyConnectionInline, if the input interface is configured for load balancing, and if IPS is configured on the output interface.

**Default ACL Filter Approach**

By default, ACL filters for the deny actions are created on the ingress interfaces of the offending packet. Thus, if Cisco IOS IPS is configured in outbound direction on the egress interface and the “deny” ACLs are created on the ingress interface, Cisco IOS IPS will drop the matching traffic before it goes through much processing. Unfortunately, this approach does not work in load balancing scenarios for which there is more than one ingress interface performing load-balancing.

**Alternative ACL Filter Approach**

The `ip ips deny-action ips-interface` command enables ACLs to be created on the same interface and in the same direction as Cisco IOS IPS is configured. This alternative approach supports load-balancing scenarios--assuming that the load-balancing interfaces have the same Cisco IOS IPS configuration. However, all outbound Cisco IOS IPS traffic will go through substantial packet path processing before it is eventually dropped by the ACLs.

**Examples**

The following example shows how to configure load-balancing between interface e0 and interface e1:

```
ip ips name test
```
ip inspect through ip security strip

ip inspect through ip security strip
**ip ips enable-clidelta**

To enable the signature tuning settings in the clidelta.xmz file on the router to take precedence over the signature settings in the intrusion prevention system (IPS) iosips-sig-delta.xmz file, use the `ip ips enable-clidelta` command in global configuration mode. To restore precedence to the iosips-sig-delta.xmz file settings, use the `no` form of this command.

```
ip ips enable-clidelta
no ip ips enable-clidelta
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

This command is disabled by default.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Most IPS devices and applications provide either a single default configuration or multiple default configurations. Using one of these default configurations is an ideal starting point for deploying IPS. When IOS IPS is deployed, parameters such as severity, active status, or event actions of certain signatures need to be tuned to meet the requirements of an enterprise network traffic profile.

Once the `ip ips enable-clidelta` command is enabled, a local cli-delta.xmz file is generated containing the local tuning signatures configured through the CLI. The settings in the clidelta.xmz file take precedence when a globally administered delta signature update, contained in the iosips-sig-delta.xmz file, is sent from a central repository and applied to the configuration of the local router.

**Examples**

The following example shows how to enable the clidelta functionality:

```
Router(config)# ip ips enable-clidelta
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip ips sig-clidelta</code></td>
<td>Displays information about the IPS iosips-sig-clidelta.xmz file on the router to verify signature tuning settings.</td>
</tr>
</tbody>
</table>
**ip ips event-action-rules**

To enter config-rule configuration mode, which allows users to change the target value rating, use the `ip ips event-action-rules` command in global configuration mode.

```
ip ips event-action-rules
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

None

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must issue the `ip ips event-action-rules` command to define the target value rating via the `target-value` command.

**Examples**

The following example shows how to change the target value to low for the host 192.168.0.1:

```
configure terminal
ip ips event-action-rules
target-value low target-address 192.168.0.1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>target-value</code></td>
<td>Defines the target value rating for a host.</td>
</tr>
</tbody>
</table>
**ip ips fail closed**

To instruct the router to drop all packets until the signature engine is built and ready to scan traffic, use the `ip ips fail closed` command in global configuration mode. To return to the default functionality, use the `no` form of this command.

```plaintext
ip ips fail closed
no ip ips fail closed
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

All packets are passed without being scanned while the signature engine is being built or if the signature engine fails to build.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Cisco IOS IPS Fails to Load the SDF**

By default, the router running Intrusion Prevention System (IPS) will load the built-in signatures if it fails to load the signature definition file (SDF). If this command is issued, the router will drop all packets--unless the user specifies an access control list (ACL) for packets to send to IPS.

**IPS Loads the SDF but Fails to Build a Signature Engine**

If the router running IPS loads the SDF but fails to build a signature engine, the router will mark the engine “not ready.” If an available engine is previously loaded, the IPS will keep the available engine and discard the engine that is not ready for use. If no previous engines have been loaded or “not ready,” the router will install the engine that is not ready and rely on the configuration of the `ip ips fail closed` command.

By default, packets destined for an engine marked “not ready” will be passed without being scanned. If this command is issued, the router will drop all packets that are destined for that signature engine.

**Examples**

The following example shows how to instruct the router to drop all packets if the SME is not yet available:

```plaintext
Router(config)# ip ips fail closed
```
ip ips inherit-obsolete-tunings

**Note**
Effective with Cisco IOS Release 15.2T, the `ip ips inherit-obsolete tunings` command is deprecated because the Cisco IOS IPS Signature Scanning with Lightweight Signatures feature is discontinued.

To enable Cisco IOS Intrusion Prevention System (IPS) signatures to inherit tunings from obsoleted signatures in a Cisco IOS IPS, use the `ip ips inherit-obsolete tunings` command in global configuration mode. To disable this function, use the `no` form of this command.

```plaintext
ip ips inherit-obsolete-tunings
no ip ips inherit-obsolete-tunings
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Tunings from obsoleted signatures in Cisco IOS IPS are not inherited.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2T</td>
<td>This command was deprecated.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `ip ips inherit-obsolete-tunings` command enables new signatures to obsolete older signatures and inherit the event-action and enabled parameters of the obsolete tuning values without the need to manually tune the new signatures. All other parameter changes, including the "Retire" parameter saved in the old signatures, will be ignored.

After you enter the command, the screen displays a warning message asking you to clarify the intended usage and then asks whether you accept the configuration. By default, old signatures tunings are not inherited by new signatures.

```plaintext
Note
The tunings of old signatures will be lost if they are not migrated to new signatures.
```

```plaintext
Note
To enable inheritance of tunings, configure the ip ips inherit-obsolete-tunings command before a signature file is loaded.
```

```plaintext
Note
Users of management devices should use those devices and not enable the ip ips inherit-obsolete-tunings command.
```
Examples

The following example shows how to configure a router running Cisco IOS IPS to allow new signatures to inherit the tuning values from the obsoleted signatures, without having to manually tune the new signatures:

Router(config)# ip ips inherit-obsolete-tunings

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ips</td>
<td>Applies a IPS rule to an interface.</td>
</tr>
<tr>
<td>ip ips memory regex chaining</td>
<td>Enables an Cisco IOS IPS to chain multiple regex tables together and load additional signatures.</td>
</tr>
<tr>
<td>ip ips memory threshold</td>
<td>Specifies an Cisco IOS IPS memory threshold.</td>
</tr>
<tr>
<td>show ip ips</td>
<td>Displays Cisco IOS IPS information such as configured sessions and signatures.</td>
</tr>
</tbody>
</table>
ip ips memory regex chaining

Note
Effective with Cisco IOS Release 15.2T, the ip ips memory regex chaining command is deprecated because the Cisco IOS IPS Signature Scanning with Lightweight Signatures feature is discontinued.

To enable a Cisco IOS Intrusion Prevention System (IPS) to chain multiple regex tables together and load additional signatures, use the ip ips memory regex chaining command in global configuration mode. To disable this function, use the no form of this command.

ip ips memory regex chaining
no ip ips memory regex chaining

Syntax Description
This command has no arguments or keywords.

Command Default
Multiple regex table chaining is disabled.

Command Modes
Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2T</td>
<td>This command was deprecated.</td>
</tr>
</tbody>
</table>

Usage Guidelines
Multiple regex table chaining is used to load additional signatures when a Cisco IOS IPS is supporting a large signature set. The default is three chained tables when the ip ips memory regex chaining command is enabled. This results in slower performance of Cisco IOS IPS scanning due to scanning packets across more than a single regex table.

When a user tries to load a specific set of signatures that does not fit using a single table, compilation errors will result. A compiler failure error message looks like this:

*Sep 9 17:27:46.907: %IPS-4-SIGNATURE_COMPILE_FAILURE: string-tcp 3730:0 - compiles discontinued for this engine

Examples
The following example shows how to enable the ip ips memory regex chaining command:

Router(config)# ip ips memory regex chaining

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ips</td>
<td>Applies an IPS rule to an interface.</td>
</tr>
<tr>
<td>ip ips inherit-obsolete-tunings</td>
<td>Applies tunings from obsoleted signatures to the new versions of the signatures.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>ip ips memory threshold</strong></td>
<td>Specifies a Cisco IOS IPS memory threshold.</td>
</tr>
<tr>
<td><strong>show ip ips</strong></td>
<td>Displays Cisco IOS IPS information such as configured sessions and signatures.</td>
</tr>
</tbody>
</table>
ip ips memory threshold

Effectively with Cisco IOS Release 15.2T, the `ip ips memory threshold` command is deprecated because the Cisco IOS IPS Signature Scanning with Lightweight Signatures feature is discontinued.

To specify a memory threshold when using a Cisco IOS Intrusion Prevention System (IPS), use the `ip ips memory threshold` command in global configuration mode. To disable this function, use the no form of this command.

```
ip ips memory threshold megabytes
no ip ips memory threshold
```

**Syntax Description**

| megabytes | The IPS memory threshold, in megabytes. The valid range is from 0-1024. |

**Command Default**

The default IPS memory threshold is 10 percent of free memory--this is available for router operations other than Cisco IOS IPS.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2T</td>
<td>This command was deprecated.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The IPS memory threshold defines the amount of free memory unavailable to the IPS.

When you are loading signatures, the default state is that Cisco IOS IPS cannot consume any more memory if the remaining (free) memory becomes less than 10 percent of the size of the total DRAM installed on the router (for example, less than 25.6 MB free memory left on routers with 256 MB DRAM). The 10 percent of free memory unavailable to IPS defines the IPS memory threshold. The IPS memory threshold can be changed using the `ip ips memory threshold` command to force IPS to use less memory, so that other features get access to more memory if they need it.

Setting a memory threshold for Cisco IOS IPS is recommended especially when an arbitrary number of signatures may be added on top of the recommended sets in Cisco IOS IPS Basic or Advanced/Default categories, or when a fully customized signature set is created and loaded.

**Examples**

The following example shows how to configure a router running Cisco IOS IPS to set the IPS memory threshold to a value of 50 MB:

```
Router(config)# ip ips memory threshold 50
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip ips</code></td>
<td>Applies an IPS rule to an interface.</td>
</tr>
<tr>
<td><code>ip ips inherit-obsolete-tunings</code></td>
<td>Applies tunings from obsoleted signatures to the newer versions of the signatures.</td>
</tr>
<tr>
<td><code>ip ips memory regex chaining</code></td>
<td>Enables a Cisco IOS IPS to chain multiple regex tables together and load additional signatures.</td>
</tr>
<tr>
<td><code>show ip ips</code></td>
<td>Displays Cisco IOS IPS information such as configured sessions and signatures.</td>
</tr>
</tbody>
</table>
ip ips name

To specify an intrusion prevention system (IPS) rule, use the `ip ips name` command in global configuration mode. To delete an IPS rule, use the `no` form of this command.

```
ip ips name ips-name [list acl]
no ip ips name ips-name [list acl]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ips-name</code></td>
<td>Name for IPS rule.</td>
</tr>
<tr>
<td><code>list acl</code></td>
<td>(Optional) Specifies an extended or standard access control list (ACL) to filter the traffic that will be scanned.</td>
</tr>
</tbody>
</table>

**Note**

All traffic that is permitted by the ACL is subject to inspection by the IPS. Traffic that is denied by the ACL is not inspected by the IPS.

**Command Default**

An IPS rule does not exist.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>The command name was changed from the <code>ip audit name</code> command to the <code>ip ips name</code> command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The IPS does not load the signatures until the rule is applied to an interface via the `ip ips` command.

**Note**

This command replaces the `ip audit name` global configuration command. If the `ip audit name` command has been issued in an existing configuration and an access control list (ACL) has been defined, IPS will apply the `ip ips name` command and the ACL parameter on all interfaces that applied the rule.

**Examples**

The following example shows how to configure a router running Cisco IOS IPS to load the default, built-in signatures. Note that a configuration option for specifying an SDF location is not necessary; built-in signatures reside statically in Cisco IOS.

```
!  ip ips po max-events 100
  ip ips name MYIPS
  !
  interface GigabitEthernet0/1
  ip address 10.1.1.16 255.255.255.0
  ip ips MYIPS in
duplex full
  speed 100
  media-type rj45
```
no negotiation auto
!

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ips</td>
<td>Applies an IPS rule to an interface.</td>
</tr>
<tr>
<td>show ip ips</td>
<td>Displays IPS information such as configured sessions and signatures.</td>
</tr>
</tbody>
</table>
**ip ips notify**

To specify the method of event notification, use the `ip ips notify` command in global configuration mode. To disable event notification, use the `no` form of this command.

```
ip ips notify [{log|sdee}]
no ip ips notify [{log|sdee}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>log</code></td>
<td>(Optional) Send messages in syslog format.</td>
</tr>
<tr>
<td><code>sdee</code></td>
<td>(Optional) Send messages in Security Device Event Exchange (SDEE) format.</td>
</tr>
</tbody>
</table>

**Note**

If an option is not specified, alert messages are sent in syslog format.

**Command Default**

Disabled (alert messages are not sent).

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>The command name was changed from the ip audit notify command to the ip ips notify command. Also, support for SDEE was introduced, and the sdee keyword was added.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The Post Office protocol was deprecated, and the nr-director keyword was removed.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

SDEE is always running, but it does not receive and process events from Intrusion Prevention System (IPS) unless SDEE notification is enabled. If it is not enabled and a client sends a request, SDEE will respond with a fault response message, indicating that notification is not enabled.

To use SDEE, the HTTP server must be enabled (via the `ip http server` command). If the HTTP server is not enabled, the router cannot respond to the SDEE clients because it cannot not see the requests.

**Note**

The `ip ips notify` command replaces the `ip audit notify` command. If the `ip audit notify` command is part of an existing configuration, the IPS will interpret it as the `ip ips notify` command.

**Examples**

In the following example, event notifications are specified to be sent in SDEE format:

```
ip ips notify sdee
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip http server</code></td>
<td>Enables the HTTP server on your system.</td>
</tr>
</tbody>
</table>
ip ips sdf location

Note
In Cisco IOS Release 12.4(11)T, the **ip ips sdf location** command was replaced with the **ip ips config location** command. For more information, see the **ip ips config location** command.

To specify the location in which the router will load the signature definition file (SDF), use the **ip ips sdf location** command in global configuration mode. To remove an SDF location from the configuration, use the **no** form of this command.

**ip ips sdf location** *url* [*[retries number wait-time seconds]*] [autosave]

**no ip ips sdf location** *url* [*[retries number wait-time seconds]*] [autosave]

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>url</strong></th>
<th>Location of the SDF. Available URL options:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- local flash, such as flash: sig.xml</td>
</tr>
<tr>
<td></td>
<td>- FTP server, such as ftp://myuser:<a href="mailto:mypass@ftp_server.sig.xml">mypass@ftp_server.sig.xml</a></td>
</tr>
<tr>
<td></td>
<td>- rcp, such as rcp://myuser@rcp_server/sig.xml</td>
</tr>
<tr>
<td></td>
<td>- TFTP server, such as tftp://tftp_server/sig.xml</td>
</tr>
</tbody>
</table>

| **retries number** | (Optional) Number of times the router will try to load the SDF after the first attempt fails. |
| **wait-time seconds** | (Optional) Duration, in seconds, between retry attempts. |
| **autosave** | (Optional) Specifies that the router will save a new SDF to the specified location. |

**Command Default**

If an SDF location is not specified, the router will load the default built-in signatures.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(4)T</td>
<td>The <strong>autosave</strong> keyword was added.</td>
</tr>
<tr>
<td>12.4(7.20)T</td>
<td>The <strong>retries number</strong> and the <strong>wait-time seconds</strong> options were added.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was replaced with the <strong>ip ips config location</strong> command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you specify the **ip ips sdf location** command, the signatures are not loaded until the router is rebooted or until the Intrusion Prevention System (IPS) is applied to an interface (via the **ip ips** command). If IPS is already applied to an interface, the signatures are not loaded. If IPS cannot load the SDF, an error message is issued and the router uses the built-in IPS signatures.
You can also specify the `copy ips-sdf` command to load an SDF from a specified location. Unlike the `ip ips sdf location` command, the signatures are loaded immediately after the `copy ips-sdf` command is entered.

When you specify the `autosave` keyword, the router saves a new SDF to the specified location when signatures are loaded using either the `copy` command or an external management platform such as Security Device Manager (SDM), IPS Management Center (IPSMC) or Cisco Incident Control Server (Cisco ICS). You can specify multiple autosave locations. The router will attempt to save to all autosave locations. The URL must have proper write access permissions.

**Examples**

The following example shows how to configure the router to load and merge the attack-drop.sdf file with the default signatures. After the files are merged, it is recommended that you copy the merged signatures to a separate file. You can then reload the router (by entering the `reload` command) or reinitialize the router so that it recognizes the newly merged file (as shown the following example).

```plaintext
! ip ips name MYIPS
!
interface GigabitEthernet0/1
    ip address 10.1.1.16 255.255.255.0
    ip ips MYIPS in
duplex full
    speed 100
    media-type rj45
    no negotiation auto
!
!
! Merge the flash-based SDF (attack-drop.sdf) with the built-in signatures.
copy disk2:attack-drop.sdf ips-sdf
!
! Save the newly merged signatures to a separate file.
copy ips-sdf disk2:my-signatures.sdf
!
! Configure the router to use the new file, my-signatures.sdf
configure terminal
ip ips sdf location disk2:my-signatures.sdf
!
! Reinitialize the IPS by removing the IPS rule set and reapplying the rule set.
interface gig 0/1
no ip ips MYIPS in
!
*Apr 8 14:05:38.243:%IPS-2-DISABLED:IPS removed from all interfaces - IPS disabled
!
ip ips MYIPS in
!
exit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy ips-sdf</td>
<td>Loads or saves the SDF in the router.</td>
</tr>
<tr>
<td>ip ips</td>
<td>Applies the IPS rule to an interface.</td>
</tr>
</tbody>
</table>
ip ips signature

Note
In Cisco IOS Release 12.4(11)T, the ip ips signature command was deprecated.

To attach a policy to a signature, use the ip ips signature command in global configuration mode. If the policy disabled a signature, use the no form of this command to reenable the signature. If the policy attached an access list to the signature, use the no form of this command to remove the access list.

ip ips signature signature-id {delete|disable|list acl-list}
no ip ips signature signature-id

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>signature-id</td>
<td>Signature within the signature detection file (SDF).</td>
</tr>
<tr>
<td>delete</td>
<td>Deleted a specified signature.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables a specified signature.</td>
</tr>
<tr>
<td>list acl-list</td>
<td>A named, standard, or ACL that is associated with the signature.</td>
</tr>
</tbody>
</table>

Command Default
No policy is attached to a signature.

Command Modes
Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(8)T</td>
<td>The command name was changed from the ip audit signature command to the ip ips signature command to support SDFs.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command and support for SDFs were removed.</td>
</tr>
</tbody>
</table>

Usage Guidelines
This command allow you to set three policies: delete a signature, disable the audit of a signature, or qualify the audit of a signature with an access list.

If you are attaching an ACL to a signature, then you also need to create an Intrusion Prevention System (IPS) rule with the ip ips name command and apply it to an interface with the ip ips command.

Note
The ip ips signature command replaces the ip audit signature command. If the ip audit signature command is found in an existing configuration, Cisco IOS IPS will interpret it as the ip ips signature command.

Examples
In the following example, a signature is disabled, another signature has ACL 99 attached to it, and ACL 99 is defined:
ip ips signature 6150 disable
ip ips signature 1000 list 99
access-list 99 deny 10.1.10.0 0.0.0.255
access-list 99 permit any
ip ips signature-category

To enter IPS category (config-ips-category) configuration mode, which allows you to tune Cisco IOS Intrusion Prevention System (IPS) signature parameters on the basis of a signature category, use the **ip ips signature-category** command in global configuration mode.

**ip ips signature-category**

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
None

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the **ip ips signature-category** command if you want to tune signature parameters per category.

**Examples**
The following example shows how to tune event-action parameters for the signature category “adware/spyware.” All tuning information will be applied to all signatures that belong to the adware/spyware category.

```
Router(config)# ip ips signature-category
Router(config-ips-category)# category attack adware/spyware
Router(config-ips-category-action)# event-action produce-alert
Router(config-ips-category-action)# event-action deny-packet-inline
Router(config-ips-category-action)# event-action reset-tcp-connection
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# ^Z
Do you want to accept these changes? [confirm]y
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>category</td>
<td>Specifies a signature category that is to be used for multiple signature actions or conditions.</td>
</tr>
</tbody>
</table>
**ip ips signature-definition**

To enter signature-definition-signature configuration mode, which allows you to define a signature for command-line interface (CLI) user tunings, use the `ip ips signature-definition` command in global configuration mode. To revert back to the default value, use the `no` form of this command.

```
ip ips signature-definition
no ip ips signature-definition
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Signature parameters cannot be defined and default values are used.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ip ips signature-definition` command to enter signature-definition-signature configuration mode, which allows you to issue the `signature` command. The `signature` command is used to specify a signature whose CLI user tunings are to be customized. After you issue the `signature` command, you can begin to specify which signature parameters (user tunings) are to be changed.

**Examples**

The following example shows how to modify signature 5081/0 to “produce alert” and “reset tcp connection”:

```
Router(config)# ip ips signature-definition
Router(config-sigdef-sig)# signature 5081 0
Router(config-sigdef-action)# engine
Router(config-sigdef-action-engine)# event-action produce-alert reset-tcp-connection
Router(config-sigdef-action-engine)# ^Z
Do you want to accept these changes:[confirm]y
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>signature</td>
<td>Specifies a signature for which the CLI user tunings will be changed.</td>
</tr>
</tbody>
</table>
ip ips signature disable

To instruct the router to scan for a given signature but not take any action if the signature is detected, use the `ip ips signature` command in global configuration mode. To reenable a signature, use the `no` form of this command.

```
ip ips signature signature-id [sub-signature-id] disable [list acl-list]
no ip ips signature signature-id [sub-signature-id] disable [list acl-list]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>signature-id</code></td>
<td>Signature that is disabled.</td>
</tr>
<tr>
<td><code>sub-signature-id</code></td>
<td>(Optional) A named, standard, or extended access control list (ACL) to filter the traffic that will be scanned.</td>
</tr>
<tr>
<td><code>list acl-list</code></td>
<td>If the packet is permitted by the ACL, the signature will be scanned and reported; if the packet is denied by the ACL, the signature is deemed disabled.</td>
</tr>
</tbody>
</table>

### Command Default

All signatures within the signature definition file (SDF) are reported, if detected.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

You may want to disable a signature (or set of signatures) if your deployment scenario deems the signatures unnecessary.

### Examples

The following example shows how to instructs the router not to report on signature 1000, if detected:

```
Router(config) ip ips signature 1000 disable
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ips</td>
<td>Applies the IPS rule to an interface.</td>
</tr>
<tr>
<td>ip ips name</td>
<td>Specifies an IPS rule.</td>
</tr>
</tbody>
</table>
ip kerberos source-interface

To specify an interface for the source address of the kerberos packets, use the **ip kerberos source-interface** command in global configuration mode. To disable the configuration, use the **no** form of this command.

**ip kerberos source-interface** *interface-type number*

**no ip kerberos source-interface**

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>interface-type</strong></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><strong>number</strong></td>
<td>Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.</td>
</tr>
</tbody>
</table>

**Command Default**

An interface for the source address of Kerberos packets is not set.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to specify an interface for the source address of the Kerberos packets:

```
Router# configure terminal
Router(config)# ip kerberos source-interface FastEthernet 0/0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear kerberos creds</td>
<td>Deletes the contents of the credentials cache.</td>
</tr>
<tr>
<td>debug kerberos</td>
<td>Displays information associated with the Kerberos Authentication Subsystem.</td>
</tr>
</tbody>
</table>
ip msdp border

To configure a router that borders a Protocol Independent Multicast (PIM) sparse mode region and dense mode region to use Multicast Source Discovery Protocol (MSDP), use the \texttt{ip msdp border} command in global configuration mode. To prevent this action, use the \texttt{no} form of this command.

\begin{verbatim}
ip msdp [vrf vrf-name] border sa-address interface-type interface-number
no ip msdp [vrf vrf-name] border sa-address interface-type interface-number
\end{verbatim}

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td>vrf-name</td>
<td>(Optional) Name assigned to the VRF.</td>
</tr>
<tr>
<td>sa-address</td>
<td>Specifies the active source IP address.</td>
</tr>
<tr>
<td>interface-type</td>
<td>Interface type and number from which the IP address is derived and used as</td>
</tr>
<tr>
<td>interface-number</td>
<td>the rendezvous point (RP) address in Source-Active (SA) messages. Thus,</td>
</tr>
<tr>
<td></td>
<td>MSDP peers can forward SA messages away from this border. The IP address</td>
</tr>
<tr>
<td></td>
<td>of the interface is used as the originator ID, which is the RP field in the</td>
</tr>
<tr>
<td></td>
<td>MSDP SA message. No space is needed between the values.</td>
</tr>
</tbody>
</table>

**Command Default**

The active sources in the dense mode region will not participate in MSDP.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(23)S</td>
<td>The \texttt{vrf} keyword and \texttt{vrf-name} argument were added.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>The \texttt{vrf} keyword and \texttt{vrf-name} argument were added.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(18)SXE</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command if you want the router to send SA messages for sources active in the PIM dense mode region to MSDP peers.

Specifying the interface-type and interface-number values allow the MSDP peers to forward source-active messages away from this border. The IP address of the interface is used as the originator ID, which is the rendezvous point field in the MSDP source-active message.
We recommend configuring the border router in the sparse mode domain to proxy-register sources in the dense mode domain, and have the sparse mode domain use standard MSDP procedures to advertise these sources.

Note
If you use this command, you must constrain the sources advertised by using the `ip msdp redistribute` command. Configure the `ip msdp redistribute` command to apply to only local sources. Be aware that this configuration can result in (S, G) state remaining long after a source in the dense mode domain has stopped sending.

Note
The `ip msdp originator-id` command also identifies an interface type and number to be used as the RP address. If both the `ip msdp border` and `ip msdp originator-id` commands are configured, the address derived from the `ip msdp originator-id` command determines the address of the RP.

Examples
In the following example, the local router is not an RP. It borders a PIM sparse mode region with a dense mode region. It uses the IP address of Ethernet interface 0 as the “RP” address in SA messages.

```
ip msdp border sa-address ethernet0
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip msdp originator-id</code></td>
<td>Allows an MSDP speaker that originates an SA message to use the IP address of its interface as the RP address in the SA message.</td>
</tr>
<tr>
<td><code>ip msdp redistribute</code></td>
<td>Configures which (S, G) entries from the multicast routing table are advertised in SA messages originated to MSDP peers.</td>
</tr>
</tbody>
</table>
To set the maximum transmission unit (MTU) size of IP packets that are sent on an interface, use the `ip mtu` command in interface configuration mode. To restore the default MTU size, use the `no` form of this command.

```
ip mtu bytes
no ip mtu
```

**Syntax Description**

| bytes | MTU size, in bytes |

The default MTU value depends on the interface type.

**Table 11: Default MTU Values by Interface Type**

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>4470</td>
</tr>
<tr>
<td>Ethernet</td>
<td>1500</td>
</tr>
<tr>
<td>FDDI</td>
<td>4470</td>
</tr>
<tr>
<td>High-Speed Serial Interface High Speed Access (HSSI HSA)</td>
<td>4470</td>
</tr>
<tr>
<td>Serial</td>
<td>1500</td>
</tr>
<tr>
<td>Token Ring</td>
<td>4464</td>
</tr>
<tr>
<td>VRF-Aware Service Infrastructure (VASI)</td>
<td>9216</td>
</tr>
</tbody>
</table>

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.4</td>
<td>This command was integrated into Cisco IOS XE Release 2.4.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If an IP packet exceeds the MTU size that is set for the interface, the Cisco software fragments the IP packet.

When an IPsec MTU is less than 256 bytes, the crypto engine MTU is set to 256 bytes and packets greater than 256 bytes are fragmented.

For VASI interfaces that involve Ethernet type interfaces (Ethernet, Fast Ethernet, or Gigabit Ethernet), the IP MTU size of a VASI interface must be set to the same value as the lower default setting of the Ethernet
type interface of 1500 bytes. If this adjustment is not made, OSPF reconvergence on the VASI interface requires a long time.

Note
Changing the MTU value (by using the `mtu` interface configuration command) can affect the IP MTU value. If the current IP MTU value is the same as the MTU value and you change the MTU value, then the IP MTU value is modified automatically to match the new MTU value. However, the reverse is not true; changing the IP MTU value has no effect on the MTU value.

If a dynamic virtual tunnel interface (VTI) configured with an IP MTU causes encapsulating security payload (ESP) fragmentation, clear and re-establish the encryption session.

When a loopback interface is used as the VTI tunnel source, you must manually configure the `ip mtu` command. This is because the IPsec encapsulation bytes are calculated based on the outgoing physical interface.

MTU Size in an IPsec Configuration

In an IPsec configuration, such as in a crypto environment, an MTU value that is less than 256 bytes is not accepted. If you configure an MTU value less than 256 bytes, the MTU value is automatically overwritten and given a value of 256 bytes.

MTU Size in Cisco ME 3600X Series Ethernet Access Switches

In Cisco ME 3600X Series Ethernet Access Switches, you can configure seven unique MTU sizes on router and switchport interfaces and eight unique sizes on VLAN interfaces. This does not include the default size of 1500.

Examples

The following example shows how to set the maximum IP packet size for the first serial interface to 300 bytes:

```
Device(config)# interface serial 0
Device(config-if)# ip mtu 300
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mtu</td>
<td>Adjusts the MTU size.</td>
</tr>
</tbody>
</table>
### ip nhrp cache non-authoritative

To turn off authoritative flags on NHRP cache entries, use the `ip nhrp cache non-authoritative` command in interface configuration mode. To turn authoritative flags on again, use the `no` form of this command.

```
ip nhrp cache non-authoritative
no ip nhrp cache non-authoritative
```

#### Syntax Description

This command has no arguments or keywords.

#### Command Default

Authoritative flags are turned on.

#### Command Modes

Interface configuration

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

By default the next hop server (NHS) replies to authoritative Next Hop Resolution Protocol (NHRP) resolution requests if it has a cache entry that is marked as authoritative. The `ip nhrp cache non-authoritative` command turns off the “authoritative” flag on the cache entries. Thus, the request is forwarded to the next hop client (NHC), which responds to the resolution.

Configuring the `ip nhrp cache non-authoritative` command offloads the resolution replies from the hub to the spokes. It also helps the spokes complete NHRP mapping entries when a spoke-to-spoke tunnel is built, thus alleviating flap conditions in which the IP security (IPsec) tunnel is built but for which there are no corresponding NHRP mappings.

#### Examples

The following example shows that the authoritative flags have been turned off:

```
interface Tunnel0
 ip nhrp cache non-authoritative
```
**ip nhrp nhs**

To specify the address of one or more Next Hop Resolution Protocol (NHRP) servers, use the `ip nhrp nhs` command in interface configuration mode. To remove the address, use the `no` form of this command.

**Cisco IOS Release 12.2(33)SRA, 12.2SX, and Later Releases**

```
ip nhrp nhs nhs-address [net-address [netmask]]
no ip nhrp nhs nhs-address [net-address [netmask]]
```

**Cisco IOS Release 15.1(2)T and Later Releases**

```
ip nhrp nhs {nhs-address [nbma {nbma-addressFQDN-string}] [multicast] [priority value] [cluster value]cluster value max-connections value[dynamic nbma {nbma-addressFQDN-string} [multicast] [priority value] [cluster value]fallback seconds]}
no ip nhrp nhs {nhs-address [nbma {nbma-addressFQDN-string}] [multicast] [priority value] [cluster value]cluster value max-connections value[dynamic nbma {nbma-addressFQDN-string} [multicast] [priority value] [cluster value]fallback seconds]}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nhs-address</td>
<td>Address of the next-hop server being specified.</td>
</tr>
<tr>
<td>net-address</td>
<td>(Optional) IP address of a network served by the next-hop server.</td>
</tr>
<tr>
<td>netmask</td>
<td>(Optional) IP network mask to be associated with the IP address. The IP address is logically ANDed with the mask.</td>
</tr>
<tr>
<td>nbma</td>
<td>(Optional) Specifies the nonbroadcast multiple access (NBMA) address or FQDN.</td>
</tr>
<tr>
<td>nbma-address</td>
<td>NBMA address.</td>
</tr>
<tr>
<td>FQDN-string</td>
<td>Next hop server (NHS) fully qualified domain name (FQDN) string.</td>
</tr>
<tr>
<td>multicast</td>
<td>(Optional) Specifies to use NBMA mapping for broadcasts and multicasts.</td>
</tr>
<tr>
<td>priority value</td>
<td>(Optional) Assigns a priority to hubs to control the order in which spokes select hubs to establish tunnels. The range is from 0 to 255; 0 is the highest and 255 is the lowest priority.</td>
</tr>
<tr>
<td>cluster value</td>
<td>(Optional) Specifies NHS groups. The range is from 0 to 10; 0 is the highest and 10 is the lowest. The default value is 0.</td>
</tr>
<tr>
<td>max-connections value</td>
<td>Specifies the number of NHS elements from each NHS group that needs to be active. The range is from 0 to 255.</td>
</tr>
<tr>
<td>dynamic</td>
<td>Configures the spoke to learn the NHS protocol address dynamically.</td>
</tr>
<tr>
<td>fallback seconds</td>
<td>Specifies the duration, in seconds, for which the spoke must wait before falling back to an NHS of higher priority upon recovery.</td>
</tr>
</tbody>
</table>

**Command Default**

No next-hop servers are explicitly configured, so normal network layer routing decisions are used to forward NHRP traffic.

**Command Modes**

Interface configuration (config-if)
### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA. This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>15.1(2)T</td>
<td>This command was modified. The <code>net-address</code> and <code>mask</code> arguments were removed and the <code>nbma</code>, <code>nbma-address</code>, <code>FQDN-string</code>, <code>multicast</code>, <code>priority</code> value, <code>cluster</code> value, <code>max-connections</code> value, <code>dynamic</code>, and <code>fallback seconds</code> keywords and arguments were added.</td>
</tr>
<tr>
<td>15.2(1)T</td>
<td>This command was modified. The NBMA address was modified to support IPv6 address.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `ip nhrp nhs` command to specify the address of a next hop server and the networks it serves. Normally, NHRP consults the network layer forwarding table to determine how to forward NHRP packets. When next hop servers are configured, these next hop addresses override the forwarding path that would otherwise be used for NHRP traffic.

When the `ip nhrp nhs dynamic` command is configured on a DMVPN tunnel and the `shut` command is issued to the tunnel interface, the crypto socket does not receive shut message, thereby not bringing up a DMVPN session with the hub.

For any next hop server that is configured, you can specify multiple networks by repeating this command with the same `nhs-address` argument, but with different IP network addresses.

### Examples

The following example shows how to register a hub to a spoke using NBMA and FQDN:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs 192.0.2.1 nbma examplehub.example1.com
```

The following example shows how to configure the desired `max-connections` value:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs cluster 5 max-connections 100
```

The following example shows how to configure the NHS fallback time:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs fallback 25
```

The following example shows how to configure NHS priority and group values:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs 192.0.2.1 priority 1 cluster 2
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip nhrp map</code></td>
<td>Synchronously configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.</td>
</tr>
<tr>
<td><code>show ip nhrp</code></td>
<td>Displays NHRP mapping information.</td>
</tr>
</tbody>
</table>
ip port-map

To establish port-to-application mapping (PAM), use the `ip port-map` command in global configuration mode. To delete user-defined PAM entries, use the `no` form of this command.

```
ip port-map appl-name port [{tcp|udp}] [{port-num|from begin-port-num to end-port-num}] [list {standard-acl-number extended-acl-number ipv6-acl}] [description description-string]
no ip port-map appl-name port [{tcp|udp}] [{port-num|from begin-port-num to end-port-num}] [list {standard-acl-number extended-acl-number ipv6-acl}] [description description-string]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>appl-name</code></td>
<td>The application used to apply the port mapping. An application name can contain an underscore or a hyphen. An application can also be system or user-defined. However, a user-defined application must have the prefix <code>user-</code> in it; for example, <code>user-payroll</code>, <code>user-sales</code>, or <code>user-10</code>. Otherwise, the following error message appears: “Unable to add port-map entry. Names for user-defined applications must start with ‘user-’.”</td>
</tr>
<tr>
<td><code>port</code></td>
<td>Indicates that a port number maps to the application. You can specify up to five port numbers for each port.</td>
</tr>
<tr>
<td>`tcp</td>
<td>udp`</td>
</tr>
<tr>
<td><code>port-num</code></td>
<td>(Optional) The port number. The range is from 1 to 65535.</td>
</tr>
<tr>
<td><code>from begin-port-num to end-port-num</code></td>
<td>(Optional) Specifies a range of port numbers. You must use the <code>from</code> and <code>to</code> keywords together.</td>
</tr>
<tr>
<td><code>list</code></td>
<td>(Optional) Indicates that the port mapping information applies to a specific host or subnet by associating the port or subnet to an access control list (ACL) number used with PAM.</td>
</tr>
<tr>
<td><code>standard-acl-number</code></td>
<td>(Optional) The standard ACL number. The range is from 1 to 99.</td>
</tr>
<tr>
<td><code>extended-acl-number</code></td>
<td>(Optional) The extended ACL number. The range is from 1300 to 1999.</td>
</tr>
<tr>
<td><code>ipv6-acl</code></td>
<td>(Optional) Name of the IPv6 ACL.</td>
</tr>
<tr>
<td><code>description description-string</code></td>
<td>(Optional) Specifies a description of up to 40 characters in length.</td>
</tr>
</tbody>
</table>

**Command Default**
PAM does not get established by default.

**Command Modes**
Global configuration (config)
### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(1)</td>
<td>This command was modified. Support for the Skinny Client Control Protocol (SCCP) was added.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>This command was modified. Support was added for the following:</td>
</tr>
<tr>
<td></td>
<td>• User-defined application names</td>
</tr>
<tr>
<td></td>
<td>• User-specified descriptions</td>
</tr>
<tr>
<td></td>
<td>• Port ranges</td>
</tr>
<tr>
<td></td>
<td>• <code>tcp</code> and <code>udp</code> keywords</td>
</tr>
<tr>
<td></td>
<td>• <code>from begin-port-num to end-port-num</code> keyword-argument pairs</td>
</tr>
<tr>
<td></td>
<td>• <code>description description-string</code> keyword-argument pair</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.6S Release</td>
<td>This command was modified. The <code>ipv6-acl</code> argument was added.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `ip port-map` command associates TCP or UDP port numbers with applications or services, establishing a table of default port mapping information at the firewall. The port mapping information is used to support network environments that run services using ports that are different from the registered or well-known ports associated with a service or application.

When you configure the `no` form of the command, include all the parameters needed to remove the entry matching that specific set of parameters. For example, when you configure the `no ip port-map appl-name` command, all entries for that application are removed.

The port mapping information in the PAM table can be one of the following three types:

- System-defined
- User-defined
- Host-specific

#### System-Defined Port Mapping

Initially, PAM creates a set of system-defined entries in the mapping table by using well-known or registered port mapping information set up during system startup. The Context-Based Access Control (CBAC) firewall requires the system-defined port mapping information to function.
You can delete or modify system-defined port mapping information. Use the `no` form of the command to delete a port mapping and the regular form of the command to remap the system-defined port mapping information to another application.

You can also add new port numbers to system-defined applications. However, for some system-defined applications like HTTP and Simple Mail Transfer Protocol (SMTP), in which the firewall inspects deeper into packets, the protocol (UDP or TCP) cannot be changed from that defined in the system. In these instances, error messages are displayed.

The table below lists some default system-defined services and applications in the PAM table. (Use the `show ip port-map` command to display the complete list.)

**Table 12: System-Defined Port Mapping**

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Well-Known or Registered Port Number</th>
<th>Protocol Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cuseeme</td>
<td>7648</td>
<td>CU-SeeMe Protocol</td>
</tr>
<tr>
<td>exec</td>
<td>512</td>
<td>Remote Process Execution</td>
</tr>
<tr>
<td>ftp</td>
<td>21</td>
<td>File Transfer Protocol (control port)</td>
</tr>
<tr>
<td>h323</td>
<td>1720</td>
<td>H.323 Protocol (for example, MS NetMeeting, Intel Video Phone)</td>
</tr>
<tr>
<td>http</td>
<td>80</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>login</td>
<td>513</td>
<td>Remote login</td>
</tr>
<tr>
<td>msrpc</td>
<td>135</td>
<td>Microsoft Remote Procedure Call</td>
</tr>
<tr>
<td>netshow</td>
<td>1755</td>
<td>Microsoft NetShow</td>
</tr>
<tr>
<td>real-audio-video</td>
<td>7070</td>
<td>RealAudio and RealVideo</td>
</tr>
<tr>
<td>sccp</td>
<td>2000</td>
<td>Skinny Client Control Protocol</td>
</tr>
<tr>
<td>smtp</td>
<td>25</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>sql-net</td>
<td>1521</td>
<td>SQL-NET</td>
</tr>
<tr>
<td>streamworks</td>
<td>1558</td>
<td>StreamWorks Protocol</td>
</tr>
<tr>
<td>sunrpc</td>
<td>111</td>
<td>SUN Remote Procedure Call</td>
</tr>
<tr>
<td>tftp</td>
<td>69</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>vdlive</td>
<td>7000</td>
<td>VDOLive Protocol</td>
</tr>
</tbody>
</table>

You can override system-defined entries for a specific host or a subnet using the `ip port-map appl-name port list` command.

---

*Note* You can override system-defined entries for a specific host or a subnet using the `ip port-map appl-name port list` command.
User-Defined Port Mapping

Network applications that use nonstandard ports require user-defined entries in the mapping table. Use the `ip port-map` command to create default user-defined entries in the PAM table. These entries automatically appear as an option for the `ip inspect name` command to facilitate the creation of inspection rules.

You can specify up to five separate port numbers for each port map in a single entry. You can also specify a port range in a single entry. However, you cannot specify both single port numbers and port ranges in the same entry.

Note

If you try to map an application to a system-defined port, a message appears warning you of a mapping conflict. Delete the system-defined entry before mapping it to another application. Deleted system-defined mappings appear in the running configuration in their `no ip port-map` form.

Use the `no` form of the `ip port-map` command to delete user-defined entries from the PAM table. To remove a single mapping, use the `no` form of the command with all its parameters.

To overwrite an existing user-defined port mapping, use the `ip port-map` command to associate another service or application with the specific port.

Multiple commands for the same application name are cumulative.

If you assign the same port number to a new application, the new entry replaces the existing entry. The entry no longer appears in the running configuration and you receive a message about the remapping.

You cannot specify a port number that is in a range assigned to another application. You cannot specify overlapping port ranges.

Host-Specific Port Mapping

User-defined entries in the mapping table can include host-specific mapping information, which establishes port mapping information for specific hosts or subnets. In some environments, it might be necessary to override the default port mapping information for a specific host or a subnet, including system-defined default port mapping information. Use the `ip port-map appl-name port list` command to specify an ACL for a host or a subnet that uses PAM.

Note

If the host-specific port mapping information is the same as the existing system-defined or user-defined default entries, host-specific port changes have no effect.

Examples

The following examples show how to add and remove user-defined PAM configuration entries at the firewall.

The following example shows how to establish the nonstandard port 8000 as the user-defined default port for HTTP services:

```
Device(config)# ip port-map http port 8000
```

The following example shows how to configure PAM entries that establish a range of nonstandard ports for HTTP services:

```
Device(config)# ip port-map http port 8001
Device(config)# ip port-map http port 8002
```
Device(config)# ip port-map http port 8003
Device(config)# ip port-map http port 8004

The following example shows how to configure port 8000 for FTP services. ACL 10 identifies the server address (192.168.32.43), and port 8000 is mapped with FTP services:

Device(config)# access-list 10 permit 192.168.32.43
Device(config)# ip port-map ftp port 8000 list 10

The following example shows how to configure port 21, which is usually reserved for FTP services, to the RealAudio application for hosts in the ACL list 10. In this configuration, hosts in list 10 do not recognize FTP activity on port 21.

Device(config)# ip port-map realaudio port 21 list 10

The following example shows that the `ip port-map` command has failed and an error message is generated:

Device(config)# ip port-map netshow port 21

Command fail: the port 21 has already been defined for ftp by the system.
No change can be made to the system defined port mappings.

The following example shows how the `no` form of this command deletes user-defined entries from the PAM table. The `no` command has no effect on the system-defined port mappings. This command deletes the host-specific port mapping of FTP.

Device(config)# no ip port-map ftp port 1022 list 10

All `no` forms of the `ip port-map` command appear before other entries in the running configuration.

The following example shows how to configure a specific host to use port 8000 for FTP services. ACL 10 identifies the server address (192.168.32.43), and port 8000 is mapped with FTP services.

Device(config)# access-list 10 permit 192.168.32.43
Device(config)# ip port-map ftp port 8000 list 10

The following example shows how to configure a specific subnet to run HTTP services on port 8080. ACL 50 identifies the subnet, and the PAM entry maps port 8080 with HTTP services.

Device(config)# access-list 50 permit 192.168.92.0
Device(config)# ip port-map http port 8080 list 50

The following example shows how to configure a specific host to run HTTP services on port 25, which is the system-defined port number for SMTP services. This requires a host-specific PAM entry that overrides the system-defined default port mapping for HTTP, which is port 80. ACL 15 identifies the host address (192.168.33.43), and port 25 is mapped with HTTP services.

Device(config)# access-list 15 permit 192.168.33.43
Device(config)# ip port-map http port 25 list 15

The following example shows how to configure the same port number for different services running on different hosts. Port 8000 is required for HTTP services by host 192.168.3.4, and also required for FTP services by host 192.168.5.6. ACL 10 and ACL 20 identify the specific hosts, and PAM maps the ports with the services for each ACL.

Device(config)# access-list 10 permit 192.168.3.4
Device(config)# access-list 20 permit 192.168.5.6
Device(config)# ip port-map http port 8000 list 10
Device(config)# ip port-map http port 8000 list 20
The following example shows how to configure five separate port numbers:

```
Device(config)# ip port-map user-my-app port tcp 8085 8087 8092 8093 8094
```

The following example shows how to configure multiple commands for the same application name and both ports map to the myapp application:

```
Device(config)# ip port-map user-myapp port tcp 3400
Device(config)# ip port-map user-myapp port tcp 3500
```

The following example shows how to configure the same port number for a new application. The new entry replaces the existing entry, meaning that port 5670 gets mapped to user-my-new-app and its mapping to myapp is removed. As a result, the first command no longer appears in the running configuration and you receive a message about the remapping.

```
Device(config)# ip port-map user-myapp port tcp 5670
Device(config)# ip port-map user-my-new-app port tcp 5670
```

In the following example, the second command assigns port 8085 to user-my-new-app because you cannot specify a port number that is in a range assigned to another application. As a result, the first command no longer appears in the running configuration, and you receive a message about the port being moved from one application to another.

```
Device(config)# ip port-map user-my-app port tcp 8085
Device(config)# ip port-map user-my-new-app port tcp from 8080 to 8090
```

Similarly, in the following example the second command assigns port range 8080 to 8085 to user-my-new-app and the first command no longer appears in the running configuration. You receive a message about the remapping.

```
Device(config)# ip port-map user-my-app port tcp from 8080 to 8085
Device(config)# ip port-map user-my-new-app port tcp from 8080 to 8090
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip port-map</td>
<td>Displays PAM information.</td>
</tr>
</tbody>
</table>
**ip radius source-interface**

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the `ip radius source-interface` command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the `no` form of this command.

```
ip radius source-interface subinterface-name [vrf vrf-name]
no ip radius source-interface
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>subinterface-name</code></td>
<td>Name of the interface that RADIUS uses for all of its outgoing packets.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Per virtual route forwarding (VRF) configuration.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(1)DX</td>
<td>The <code>vrf</code> keyword and <code>vrf-name</code> argument were implemented on the Cisco 7200 series and Cisco 7401 ASR.</td>
</tr>
<tr>
<td>12.2(2)DD</td>
<td>This command was integrated into Cisco IOS Release 12.2(2)DD.</td>
</tr>
<tr>
<td>12.2(4)B</td>
<td>This command was integrated into Cisco IOS Release 12.2(4)B.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to set the IP address of a subinterface to be used as the source address for all outgoing RADIUS packets. The IP address is used as long as the subinterface is in the `up` state. The RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses. RADIUS uses the IP address of the interface that it is associated to, regardless of whether the interface is in the `up` or `down` state.

The `ip radius source-interface` command is especially useful in cases where the router has many subinterfaces and you want to ensure that all RADIUS packets from a particular router have the same IP address.
The specified sub-interface should have a valid IP address and should be in the up state for a valid configuration. If the specified sub-interface does not have a valid IP address or is in the down state, RADIUS enforces the source-interface configuration. In case the interface has no IP address, RADIUS configures the best available local IP address. To avoid this, add a valid IP address to the sub-interface or bring the sub-interface to the up state.

Use the vrf vrf-name keyword and argument to configure this command per VRF, which allows multiple disjoined routing or forwarding tables, where the routes of one user have no correlation with the routes of another user.

**Examples**

The following example shows how to configure RADIUS to use the IP address of subinterface s2 for all outgoing RADIUS packets:

```
ip radius source-interface s2
```

The following example shows how to configure RADIUS to use the IP address of subinterface Ethernet0 for VRF definition:

```
ip radius source-interface Ethernet0 vrf vrf1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip tacacs source-interface</td>
<td>Uses the IP address of a specified interface for all outgoing TACACS packets.</td>
</tr>
<tr>
<td>ip telnet source-interface</td>
<td>Allows a user to select an address of an interface as the source address for Telnet connections.</td>
</tr>
<tr>
<td>ip tftp source-interface</td>
<td>Allows a user to select the interface whose address will be used as the source address for TFTP connections.</td>
</tr>
</tbody>
</table>
ip reflexive-list timeout

To specify the length of time that reflexive access list entries will continue to exist when no packets in the session are detected, use the `ip reflexive-list timeout` command in global configuration mode. To reset the timeout period to the default timeout, use the `no` form of this command.

```
ip reflexive-list timeout seconds
no ip reflexive-list timeout
```

**Syntax Description**

<table>
<thead>
<tr>
<th>seconds</th>
<th>Specifies the number of seconds to wait (when no session traffic is being detected) before temporary access list entries expire. Use a positive integer from 0 to 2,147,483. The default is 300 seconds.</th>
</tr>
</thead>
</table>

**Command Default**

300 seconds

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is used with reflexive filtering, a form of session filtering.

This command specifies when a reflexive access list entry will be removed after a period of no traffic for the session (the timeout period).

With reflexive filtering, when an IP upper-layer session begins from within your network, a temporary entry is created within the reflexive access list, and a timer is set. Whenever a packet belonging to this session is forwarded (inbound or outbound) the timer is reset. When this timer counts down to zero without being reset, the temporary reflexive access list entry is removed.

The timer is set to the *timeout period*. Individual timeout periods can be defined for specific reflexive access lists, but for reflexive access lists that do not have individually defined timeout periods, the global timeout period is used. The global timeout value is 300 seconds by default; however, you can change the global timeout to a different value at any time using this command.

This command does not take effect for reflexive access list entries that were already created when the command is entered; this command only changes the timeout period for entries created after the command is entered.

**Examples**

The following example sets the global timeout period for reflexive access list entries to 120 seconds:

```
ip reflexive-list timeout 120
```

The following example returns the global timeout period to the default of 300 seconds:
no ip reflexive-list timeout

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>evaluate</td>
<td>Nests a reflexive access list within an access list.</td>
</tr>
<tr>
<td></td>
<td>ip access-list</td>
<td>Defines an IP access list by name.</td>
</tr>
<tr>
<td></td>
<td>permit (reflexive)</td>
<td>Creates a reflexive access list and enables its temporary entries to be automatically generated.</td>
</tr>
</tbody>
</table>
ip route (vasi)

To establish a static route on the VRF-Aware Service Infrastructure (VASI) interface, use the `ip route vrf` command in global configuration mode. To remove the static route connection, use the `no` form of this command.

```
ip route [vrf vrf-name] destination-prefix destination-prefix-mask {vasileft|vasiright} number
no ip route [vrf vrf-name] destination-prefix destination-prefix-mask {vasileft|vasiright} number
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>Specifies the Virtual Routing and Forwarding (VRF) instance for the static route.</td>
</tr>
<tr>
<td>destination-prefix</td>
<td>IP route prefix for the destination, in dotted decimal format.</td>
</tr>
<tr>
<td>destination-prefix-mask</td>
<td>Prefix mask for the destination, in dotted decimal format.</td>
</tr>
<tr>
<td>vasileft</td>
<td>Configures the vasileft interface.</td>
</tr>
<tr>
<td>vasiright</td>
<td>Configures the vasiright interface.</td>
</tr>
<tr>
<td>number</td>
<td>Identifier of the VASI interface. The range is from 1 to 256.</td>
</tr>
</tbody>
</table>

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 2.6</td>
<td></td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure static route on a VASI interface:

```
router(config)# ip route vrf red 0.0.0.0 0.0.0.0 vasileft 100
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface (vasi)</td>
<td>Configures the VASI interface.</td>
</tr>
<tr>
<td>debug interface (vasi)</td>
<td>Displays debugging information of VASI interface descriptor block.</td>
</tr>
<tr>
<td>debug vasi</td>
<td>Displays debugging information of VASI.</td>
</tr>
<tr>
<td>show vasi pair</td>
<td>Displays the status of a VASI pair.</td>
</tr>
</tbody>
</table>
ip scp server enable

To enable the router to securely copy files from a remote workstation, use the `ip scp server enable` command in global configuration mode. To disable secure copy functionality (the default), use the `no` form of this command.

```
ip scp server enable
no ip scp server enable
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The secure copy function is disabled.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(21)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(21)S and support for the Cisco 7500 series and Cisco 12000 series routers was added.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXD.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to enable secure copying of files from systems using the Secure Shell (SSH) application. This secure copy function is accomplished by an addition to the `copy` command in the Cisco IOS software, which takes care of using the secure copy protocol (scp) to copy to and from a router while logged in to the router itself. Because copying files is generally a restricted operation in the Cisco IOS software, a user attempting to copy such files needs to be at the correct enable level.

The Cisco IOS software must also allow files to be copied to or from itself from a remote workstation running the SSH application (which is supported by both the Microsoft Windows and UNIX operating systems). To get this information, the Cisco IOS software must have authentication and authorization configured in the authentication, authorization, and accounting (AAA) feature. SSH already relies on AAA authentication to authenticate the user username and password. SFTP adds the requirement that AAA authorization be turned on so that the operating system can determine whether or not the user is at the correct privilege level.

**Examples**

The following example shows a typical configuration that allows the router to securely copy files from a remote workstation. Because scp relies on AAA authentication and authorization to function properly, AAA must be configured.

```
aaa new-model
aaa authentication login default tac-group tacacs+
aaa authorization exec default local
```
username user1 privilege 15 password 0 lab
ip scp server enable

The following example shows how to use scp to copy a system image from Flash memory to a server that supports SSH:

Router# copy flash:c4500-ik2s-mz.scp scp://user1@host1/
Address or name of remote host [host1]?
Destination username [user1]?
Destination filename [c4500-ik2s-mz.scp]?
Writing c4500-ik2s-mz.scp
Password: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Note

When using scp, you cannot enter the password into the copy command; enter the password when prompted.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa authentication</td>
<td>Sets AAA authentication at login.</td>
</tr>
<tr>
<td>login</td>
<td></td>
</tr>
<tr>
<td>aaa authorization</td>
<td>Sets parameters that restrict user access to a network.</td>
</tr>
<tr>
<td>copy</td>
<td>Copies any file from a source to a destination.</td>
</tr>
<tr>
<td>debug ip scp</td>
<td>Troubleshoots scp authentication problems.</td>
</tr>
<tr>
<td>ip ssh port</td>
<td>Enables secure network access to the tty lines.</td>
</tr>
<tr>
<td>username</td>
<td>Establishes a username-based authentication system.</td>
</tr>
</tbody>
</table>

Cisco IOS Security Command Reference: Commands D to L
**ip sdee**

To set the Security Device Event Exchange (SDEE) attribute values, use the ip sdee command in global configuration mode. To change the current selection or return to the default, use the no form of this command.

```
ip sdee {alerts alert-number|messages message-number|subscriptions subscription-number}
no ip sdee {alerts|messages|subscriptions}
```

**Syntax Description**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alerts</td>
<td>Specifies the maximum number of alerts the router must store. The range is from 10 to 2000. The default value is 200.</td>
</tr>
<tr>
<td>messages</td>
<td>Specifies the maximum number of messages the router must store. The range is from 10 to 500. The default value is 200.</td>
</tr>
<tr>
<td>subscriptions</td>
<td>Specifies the maximum number of subscriptions. The range is from 1 to 3. The default value is 1.</td>
</tr>
</tbody>
</table>

**Command Default**

The default subscription is 1. The default message is 200. The default alert is 200.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The alerts alert-number and messages message-number keywords and arguments were added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The SDEE messages report on the progress of Cisco IOS Intrusion Prevention System (IPS) initialization and operation. After you have enabled SDEE to receive and process events from IPS, you can issue the ip sdee subscriptions command to modify the number of allowed open SDEE subscriptions.

**Examples**

The following example shows how to change the number of allowed open subscriptions to 2:

```
Router# configure terminal
Router(config)# ip ips notify sdee
Router(config)# ip sdee subscriptions 2
```

The following example shows how to change the number of alerts that must be stored on the router to 10:

```
Router# configure terminal
Router(config)# ip ips notify sdee
```
Router(config)# ip sdee events 500
Router(config)# ip sdee alerts 10

The following example shows how to change the number of messages that must be stored on the router to 10:

Router# configure terminal
Router(config)# ip ips notify sdee
Router(config)# ip sdee events 500
Router(config)# ip sdee messages 10

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip ips notify</td>
<td>Specifies the method of event notification.</td>
</tr>
</tbody>
</table>
ip sdee events

To set the maximum number of Security Device Event Exchange (SDEE) events that can be stored in the event buffer, use the `ip sdee events` command in global configuration mode. To change the buffer size or return to the default buffer size, use the `no` form of this command.

```
ip sdee events events
no ip sdee events events
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>events</code></td>
<td>Maximum number of events; maximum number of allowable events: 1000.</td>
</tr>
</tbody>
</table>

**Command Default**

200 events

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When SDEE notification is enabled (via the `ip ips notify sdee` command), 200 hundred events can automatically be stored in the buffer. When SDEE notification is disabled, all stored events are lost. A new buffer is allocated when the notifications are reenabled.

When specifying the size of an events buffer, note the following functionality:

- It is circular. When the end of the buffer is reached, the buffer will start overwriting the earliest stored events. (If overwritten events have not yet been reported, you will receive a buffer overflow notice.)
- If a new, smaller buffer is requested, all events that are stored in the previous buffer will be lost.
- If a new, larger buffer is requested, all existing events will be saved.

**Examples**

The following example shows how to set the maximum buffer events size to 500:

```
configure terminal
ip ips notify sdee
ip sdee events 500
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip ips notify</code></td>
<td>Specifies the method of event notification.</td>
</tr>
</tbody>
</table>
**ip security add**

To add a basic security option to all outgoing packets, use the `ip security add` command in interface configuration mode. To disable the adding of a basic security option to all outgoing packets, use the `no` form of this command.

```
ip security add
no ip security add
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled, when the security level of the interface is “Unclassified Genser” (or unconfigured). Otherwise, the default is enabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If an outgoing packet does not have a security option present, this interface configuration command will add one as the first IP option. The security label added to the option field is the label that was computed for this packet when it first entered the router. Because this action is performed after all the security tests have been passed, this label will either be the same or will fall within the range of the interface.

**Examples**

The following example adds a basic security option to each packet leaving Ethernet interface 0:

```
interface ethernet 0
ip security add
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip security dedicated</td>
<td>Sets the level of classification and authority on the interface.</td>
</tr>
<tr>
<td>ip security extended-allowed</td>
<td>Accepts packets on an interface that has an Extended Security Option present.</td>
</tr>
<tr>
<td>ip security first</td>
<td>Prioritizes the presence of security options on a packet.</td>
</tr>
<tr>
<td>ip security ignore-authorities</td>
<td>Causes the Cisco IOS software to ignore the authorities field of all incoming packets.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ip security implicit-labelling</td>
<td>Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.</td>
</tr>
<tr>
<td>ip security multilevel</td>
<td>Sets the range of classifications and authorities on an interface.</td>
</tr>
<tr>
<td>ip security reserved-allowed</td>
<td>Treats as valid any packets that have Reserved1 through Reserved4 security levels.</td>
</tr>
<tr>
<td>ip security strip</td>
<td>Removes any basic security option on outgoing packets on an interface.</td>
</tr>
</tbody>
</table>
ip security aeso

To attach Auxiliary Extended Security Options (AESOs) to an interface, use the **ip security aeso** command in interface configuration mode. To disable AESO on an interface, use the **no** form of this command.

```
ip security aeso source compartment-bits
no ip security aeso source compartment-bits
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Extended Security Option (ESO) source. This can be an integer from 0 to 255.</td>
</tr>
<tr>
<td>compartment-bits</td>
<td>Number of compartment bits in hexadecimal.</td>
</tr>
</tbody>
</table>

**Command Default**: Disabled

**Command Modes**: Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**: Compartments bits are specified only if this AESO is to be inserted in a packet. On every incoming packet at this level on this interface, these AESOs should be present.

Beyond being recognized, no further processing of AESO information is performed. AESO contents are not checked and are assumed to be valid if the source is listed in the configurable AESO table.

Configuring any per-interface extended IP Security Option (IPSO) information automatically enables **ip security extended-allowed** (disabled by default).

**Examples**

The following example defines the Extended Security Option source as 5 and sets the compartments bits to 5:

```
interface ethernet 0
ip security aeso 5 5
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip security eso-info</td>
<td>Configures system-wide defaults for extended IPSO information.</td>
</tr>
<tr>
<td>ip security eso-max</td>
<td>Specifies the maximum sensitivity level for an interface.</td>
</tr>
<tr>
<td>ip security eso-min</td>
<td>Configures the minimum sensitivity level for an interface.</td>
</tr>
</tbody>
</table>
### Command Reference

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip security extended-allowed</td>
<td>Accepts packets on an interface that has an Extended Security Option present.</td>
</tr>
</tbody>
</table>
**ip security dedicated**

To set the level of classification and authority on the interface, use the `ip security dedicated` command in interface configuration mode. To reset the interface to the default classification and authorities, use the `no` form of this command.

```
ip security dedicated level authority [authority ...]
no ip security dedicated level authority [authority ...]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>level</code></td>
<td>Degree of sensitivity of information. The <code>level</code> keywords are listed in the first table below.</td>
</tr>
<tr>
<td><code>authority</code></td>
<td>Organization that defines the set of security levels that will be used in a network. The authority keywords are listed in the second table below.</td>
</tr>
</tbody>
</table>

### Command Default

Disabled

### Command Modes

Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

All traffic entering the system on this interface must have a security option that exactly matches this label. Any traffic leaving via this interface will have this label attached to it.

The following definitions apply to the descriptions of the IP Security Option (IPSO) in this section:

- **level** -- The degree of sensitivity of information. For example, data marked TOPSECRET is more sensitive than data marked SECRET. The level keywords and their corresponding bit patterns are shown in the table below.

<table>
<thead>
<tr>
<th>Table 13: IPSO Level Keywords and Bit Patterns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level Keyword</td>
</tr>
<tr>
<td>Reserved4</td>
</tr>
<tr>
<td>TopSecret</td>
</tr>
<tr>
<td>Secret</td>
</tr>
<tr>
<td>Confidential</td>
</tr>
<tr>
<td>Reserved3</td>
</tr>
</tbody>
</table>
authority -- An organization that defines the set of security levels that will be used in a network. For example, the Gensera authority consists of level names defined by the U.S. Defense Communications Agency (DCA). The authority keywords and their corresponding bit patterns are shown in the table below.

Table 14: IPSO Authority Keywords and Bit Patterns

<table>
<thead>
<tr>
<th>Authority Keyword</th>
<th>Bit Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Genser</td>
<td>1000 0000</td>
</tr>
<tr>
<td>Slop-Esi</td>
<td>0100 0000</td>
</tr>
<tr>
<td>DIA</td>
<td>0010 0000</td>
</tr>
<tr>
<td>NSA</td>
<td>0001 0000</td>
</tr>
<tr>
<td>DOE</td>
<td>0000 1000</td>
</tr>
</tbody>
</table>

label -- A combination of a security level and an authority or authorities.

Examples

The following example sets a confidential level with Gensera authority:

```
ip security dedicated confidential Genser
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip security add</td>
<td>Adds a basic security option to all outgoing packets.</td>
</tr>
<tr>
<td>ip security extended-allowed</td>
<td>Accepts packets on an interface that has an Extended Security Option present.</td>
</tr>
<tr>
<td>ip security first</td>
<td>Prioritizes the presence of security options on a packet.</td>
</tr>
<tr>
<td>ip security ignore-authorities</td>
<td>Causes the Cisco IOS software to ignore the authorities field of all incoming packets.</td>
</tr>
<tr>
<td>ip security implicit-labelling</td>
<td>Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.</td>
</tr>
<tr>
<td>ip security multilevel</td>
<td>Sets the range of classifications and authorities on an interface.</td>
</tr>
<tr>
<td>ip security reserved-allowed</td>
<td>Treats as valid any packets that have Reserved1 through Reserved4 security levels.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>ip security strip</td>
<td>Removes any basic security option on outgoing packets on an interface.</td>
</tr>
</tbody>
</table>
ip security eso-info

To configure system-wide defaults for extended IP Security Option (IPSO) information, use the `ip security eso-info` command in global configuration mode. To return to the default settings, use the `no` form of this command.

```
ip security eso-info source compartment-size default-bit
no ip security eso-info source compartment-size default-bit
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>source</code></td>
<td>Hexadecimal or decimal value representing the extended IPSO source. This is an integer from 0 to 255.</td>
</tr>
<tr>
<td><code>compartment-size</code></td>
<td>Maximum number of bytes of compartment information allowed for a particular extended IPSO source. This is an integer from 1 to 16.</td>
</tr>
<tr>
<td><code>default-bit</code></td>
<td>Default bit value for any unsent compartment bits.</td>
</tr>
</tbody>
</table>

**Command Default**
Disabled

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command configures Extended Security Option (ESO) information, including Auxiliary Extended Security Option (AESO). Transmitted compartment information is padded to the size specified by the `compartment-size` argument.

**Examples**
The following example sets system-wide defaults for source, compartment size, and the default bit value:

```
ip security eso-info 100 5 1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip security eso-max</td>
<td>Specifies the maximum sensitivity level for an interface.</td>
</tr>
<tr>
<td>ip security eso-min</td>
<td>Configures the minimum sensitivity level for an interface.</td>
</tr>
</tbody>
</table>
**ip security eso-max**

To specify the maximum sensitivity level for an interface, use the `ip security eso-max` command in interface configuration mode. To return to the default, use the `no` form of this command.

```
ip security eso-max source compartment-bits
no ip security eso-max source compartment-bits
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Extended Security Option (ESO) source. This is an integer from 1 to 255.</td>
</tr>
<tr>
<td>compartment-bits</td>
<td>Number of compartment bits in hexadecimal.</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The command is used to specify the maximum sensitivity level for a particular interface. Before the per-interface compartment information for a particular Network-Level Extended Security Option (NLESO) source can be configured, the `ip security eso-info` global configuration command must be used to specify the default information.

On every incoming packet on the interface, these Extended Security Options should be present at the minimum level and should match the configured compartment bits. Every outgoing packet must have these ESOs.

On every packet transmitted or received on this interface, any NLESO sources present in the IP header should be bounded by the minimum sensitivity level and bounded by the maximum sensitivity level configured for the interface.

When transmitting locally generated traffic out this interface, or adding security information (with the `ip security add` command), the maximum compartment bit information can be used to construct the NLESO sources placed in the IP header.

A maximum of 16 NLESO sources can be configured per interface. Due to IP header length restrictions, a maximum of 9 of these NLESO sources appear in the IP header of a packet.

**Examples**

In the following example, the specified ESO source is 240 and the compartment bits are specified as 500:

```
interface ethernet 0
ip security eso-max 240 500
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip security eso-info</code></td>
<td>Configures system-wide defaults for extended IPSO information.</td>
</tr>
<tr>
<td><code>ip security eso-min</code></td>
<td>Configures the minimum sensitivity level for an interface.</td>
</tr>
</tbody>
</table>
**ip security eso-min**

To configure the minimum sensitivity for an interface, use the `ip security eso-min` command in interface configuration mode. To return to the default, use the `no` form of this command.

```
ip security eso-min source compartment-bits
no ip security eso-min source compartment-bits
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>source</code></td>
<td>Extended Security Option (ESO) source. This is an integer from 1 to 255.</td>
</tr>
<tr>
<td><code>compartment-bits</code></td>
<td>Number of compartment bits in hexadecimal.</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The command is used to specify the minimum sensitivity level for a particular interface. Before the per-interface compartment information for a particular Network Level Extended Security Option (NLESO) source can be configured, the `ip security eso-info` global configuration command must be used to specify the default information.

On every incoming packet on this interface, these Extended Security Options should be present at the minimum level and should match the configured compartment bits. Every outgoing packet must have these ESOs.

On every packet transmitted or received on this interface, any NLESO sources present in the IP header should be bounded by the minimum sensitivity level and bounded by the maximum sensitivity level configured for the interface.

When transmitting locally generated traffic out this interface, or adding security information (with the `ip security add` command), the maximum compartment bit information can be used to construct the NLESO sources placed in the IP header.

A maximum of 16 NLESO sources can be configured per interface. Due to IP header length restrictions, a maximum of 9 of these NLESO sources appear in the IP header of a packet.

**Examples**

In the following example, the specified ESO source is 5, and the compartment bits are specified as 5:

```
interface ethernet 0
ip security eso-min 5 5
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip security eso-info</code></td>
<td>Configures system-wide defaults for extended IPSO information.</td>
</tr>
<tr>
<td><code>ip security eso-max</code></td>
<td>Specifies the maximum sensitivity level for an interface.</td>
</tr>
</tbody>
</table>
ip security extended-allowed

To accept packets on an interface that has an extended security option present, use the `ip security extended-allowed` command in interface configuration mode. To restore the default, use the `no` form of this command.

```
ip security extended-allowed
no ip security extended-allowed
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Packets containing extended security options are rejected.

**Examples**

The following example allows interface Ethernet 0 to accept packets that have an extended security option present:

```
interface ethernet 0
    ip security extended-allowed
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip security add</code></td>
<td>Adds a basic security option to all outgoing packets.</td>
</tr>
<tr>
<td><code>ip security dedicated</code></td>
<td>Sets the level of classification and authority on the interface.</td>
</tr>
<tr>
<td><code>ip security first</code></td>
<td>Prioritizes the presence of security options on a packet.</td>
</tr>
<tr>
<td><code>ip security ignore-authorities</code></td>
<td>Causes the Cisco IOS software to ignore the authorities field of all incoming packets.</td>
</tr>
<tr>
<td><code>ip security implicit-labelling</code></td>
<td>Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.</td>
</tr>
<tr>
<td><code>ip security multilevel</code></td>
<td>Sets the range of classifications and authorities on an interface.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ip security reserved-allowed</td>
<td>Treats as valid any packets that have Reserved1 through Reserved4 security levels.</td>
</tr>
<tr>
<td>ip security strip</td>
<td>Removes any basic security option on outgoing packets on an interface.</td>
</tr>
</tbody>
</table>

Cisco IOS Security Command Reference: Commands D to L
ip security first

To prioritize the presence of security options on a packet, use the **ip security first** command in interface configuration mode. To prevent packets that include security options from moving to the front of the options field, use the **no** form of this command.

```
ip security first
no ip security first
```

### Syntax Description
This command has no arguments or keywords.

### Command Default
Disabled

### Command Modes
Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
If a basic security option is present on an outgoing packet, but it is not the first IP option, then the packet is moved to the front of the options field when this interface configuration command is used.

### Examples
The following example ensures that, if a basic security option is present in the options field of a packet exiting interface Ethernet 0, the packet is moved to the front of the options field:

```
interface ethernet 0
  ip security first
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip security add</strong></td>
<td>Adds a basic security option to all outgoing packets.</td>
</tr>
<tr>
<td><strong>ip security dedicated</strong></td>
<td>Sets the level of classification and authority on the interface.</td>
</tr>
<tr>
<td><strong>ip security extended-allowed</strong></td>
<td>Accepts packets on an interface that has an Extended Security Option present.</td>
</tr>
<tr>
<td><strong>ip security ignoreAuthorities</strong></td>
<td>Causes the Cisco IOS software to ignore the authorities field of all incoming packets.</td>
</tr>
<tr>
<td><strong>ip security implicit-labelling</strong></td>
<td>Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>ip security multilevel</td>
<td>Sets the range of classifications and authorities on an interface.</td>
</tr>
<tr>
<td>ip security reserved-allowed</td>
<td>Treats as valid any packets that have Reserved1 through Reserved4 security levels.</td>
</tr>
<tr>
<td>ip security strip</td>
<td>Removes any basic security option on outgoing packets on an interface.</td>
</tr>
</tbody>
</table>
ip security ignore-authorities

To have the Cisco IOS software ignore the authorities field of all incoming packets, use the `ip security ignore-authorities` command in interface configuration mode. To disable this function, use the `no` form of this command.

```
ip security ignore-authorities
no ip security ignore-authorities
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the packet’s authority field is ignored, the value used in place of this field is the authority value declared for the specified interface. The `ip security ignore-authorities` can be configured only on interfaces that have dedicated security levels.

**Examples**

The following example causes interface Ethernet 0 to ignore the authorities field on all incoming packets:

```
interface ethernet 0
  ip security ignore-authorities
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip security add</code></td>
<td>Adds a basic security option to all outgoing packets.</td>
</tr>
<tr>
<td><code>ip security dedicated</code></td>
<td>Sets the level of classification and authority on the interface.</td>
</tr>
<tr>
<td><code>ip security extended-allowed</code></td>
<td>Accepts packets on an interface that has an Extended Security Option present.</td>
</tr>
<tr>
<td><code>ip security first</code></td>
<td>Prioritizes the presence of security options on a packet.</td>
</tr>
<tr>
<td><code>ip security implicit-labelling</code></td>
<td>Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>ip security multilevel</code></td>
<td>Sets the range of classifications and authorities on an interface.</td>
</tr>
<tr>
<td><code>ip security reserved-allowed</code></td>
<td>Treats as valid any packets that have Reserved1 through Reserved4 security levels.</td>
</tr>
<tr>
<td><code>ip security strip</code></td>
<td>Removes any basic security option on outgoing packets on an interface.</td>
</tr>
</tbody>
</table>
ip security ignore-cipso

To enable Cisco IOS software to ignore the Commercial IP Security Option (CIPSO) field of all incoming packets at the interface, use the **ip security ignore-cipso** command in interface configuration mode. To disable this function, use the **no** form of this command.

```plaintext
ip security ignore-cipso
no ip security ignore-cipso
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Cisco IOS software cannot ignore the CIPSO field.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **ip security ignore-cipso** command allows a router running Cisco IOS software to ignore the CIPSO field in the IP packet and forward the packet as if the field was not present.

**Examples**

The following example shows how to enable Cisco IOS software to ignore the CIPSO field for all incoming packets at the Ethernet interface:

```plaintext
interface ethernet 0
  ip security ignore-cipso
```

The following sample output from the **show ip interface** command can be used to verify that the **ip security ignore-cipso** option has been enabled. If this option is enabled, the output will display the text “Commercial security options are ignored.”

```
Router# show ip interface ethernet 0
Ethernet0 is up, line protocol is up
Internet address is 172.16.0.0/28
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is enabled
Secondary address 172.19.56.31/24
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Commercial security options are ignored
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are always sent
ICMP mask replies are never sent
```
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP multicast fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
Probe proxy name replies are disabled
Gateway Discovery is disabled
Policy routing is disabled
Network address translation is disabled

The following sample outputs from the `show ip traffic` command can be used to verify that the `ip security ignore-cipso` command has been enabled:

### Sample Output Before the ip security ignore-cipso Command Was Introduced

```
Router# show ip traffic
IP statistics:
Rcvd: 153 total, 129 local destination
  0 format errors, 0 checksum errors, 0 bad hop count
  0 unknown protocol, 0 not a gateway
  0 security failures, 34 bad options, 44 with options
Opts: 10 end, 0 nop, 0 basic security, 0 loose source route
  0 timestamp, 0 extended security, 0 record route
  0 stream ID, 0 strict source route, 0 alert, 0 other
Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
  0 fragmented, 0 couldn't fragment
Bcast: 108 received, 1 sent
Mcast: 0 received, 4 sent
Sent: 30 generated, 0 forwarded
  2 encapsulation failed, 0 no route
```

### Sample Output with the ip security ignore-cipso Command Enabled

```
Router# show ip traffic
IP statistics:
Rcvd: 153 total, 129 local destination
  0 format errors, 0 checksum errors, 0 bad hop count
  0 unknown protocol, 0 not a gateway
  0 security failures, 34 bad options, 44 with options
Opts: 10 end, 0 nop, 0 basic security, 0 loose source route
  0 timestamp, 0 extended security, 0 record route
  0 stream ID, 0 strict source route, 0 alert, 0 other
  0 cipso
Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
  0 fragmented, 0 couldn't fragment
Bcast: 108 received, 1 sent
Mcast: 0 received, 4 sent
Sent: 30 generated, 0 forwarded
  2 encapsulation failed, 0 no route
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip interfaces</code></td>
<td>Displays the usability status of interfaces configured for IP.</td>
</tr>
<tr>
<td><code>show ip traffic</code></td>
<td>Displays statistics about IP traffic.</td>
</tr>
</tbody>
</table>
**ip security implicit-labelling**

To force the Cisco IOS software to accept packets on the interface, even if they do not include a security option, use the `ip security implicit-labelling` command in interface configuration mode. To require security options, use the `no` form of this command.

**Application Firewall Provisioning Syntax**

```
ip security implicit-labelling [level authority [authority...]]
no ip security implicit-labelling [level authority [authority...]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>level</code></td>
<td>(Optional) Degree of sensitivity of information. If your interface has multilevel security set, you must specify this argument. (See the <code>level</code> keywords listed in the first table in the <code>ip security dedicated</code> command section.)</td>
</tr>
<tr>
<td><code>authority</code></td>
<td>(Optional) Organization that defines the set of security levels that will be used in a network. If your interface has multilevel security set, you must specify this argument. You can specify more than one. (See the <code>authority</code> keywords listed in the second table in the <code>ip security dedicated</code> command section.)</td>
</tr>
</tbody>
</table>

**Command Default**

Enabled, when the security level of the interface is “Unclassified Genser” (or unconfigured). Otherwise, the default is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If your interface has multilevel security set, you must use the expanded form of the command (with the optional arguments as noted in brackets) because the arguments are used to specify the precise level and authority to use when labeling the packet. If your interface has dedicated security set, the additional arguments are ignored.

**Examples**

In the following example, an interface is set for security and will accept unlabeled packets:

```
ip security dedicated confidential genser
ip security implicit-labelling
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip security add</code></td>
<td>Adds a basic security option to all outgoing packets.</td>
</tr>
<tr>
<td><code>ip security dedicated</code></td>
<td>Sets the level of classification and authority on the interface.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ip security extended-allowed</td>
<td>Accepts packets on an interface that has an Extended Security Option present.</td>
</tr>
<tr>
<td>ip security first</td>
<td>Prioritizes the presence of security options on a packet.</td>
</tr>
<tr>
<td>ip security ignore-authorities</td>
<td>Causes the Cisco IOS software to ignore the authorities field of all incoming packets.</td>
</tr>
<tr>
<td>ip security multilevel</td>
<td>Sets the range of classifications and authorities on an interface.</td>
</tr>
<tr>
<td>ip security reserved-allowed</td>
<td>Treats as valid any packets that have Reserved1 through Reserved4 security levels.</td>
</tr>
<tr>
<td>ip security strip</td>
<td>Removes any basic security option on outgoing packets on an interface.</td>
</tr>
</tbody>
</table>
ip security multilevel

To set the range of classifications and authorities on an interface, use the `ip security multilevel` command in interface configuration mode. To remove security classifications and authorities, use the `no` form of this command.

```
ip security multilevel level1 [authority1... to level2 [authority2...]
no ip security multilevel
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>level1</code></td>
<td>Degree of sensitivity of information. The classification level of incoming packets must be equal to or greater than this value for processing to occur. (See the <code>level</code> keywords found in the first table in the <code>ip security dedicated</code> command section.)</td>
</tr>
<tr>
<td><code>authority1</code></td>
<td>(Optional) Organization that defines the set of security levels that will be used in a network. The authority bits must be a superset of this value. (See the <code>authority</code> keywords listed in the second table in the <code>ip security dedicated</code> command section.)</td>
</tr>
<tr>
<td><code>to</code></td>
<td>Separates the range of classifications and authorities.</td>
</tr>
<tr>
<td><code>level2</code></td>
<td>Degree of sensitivity of information. The classification level of incoming packets must be equal to or less than this value for processing to occur. (See the <code>level</code> keywords found in the first table in the <code>ip security dedicated</code> command section.)</td>
</tr>
<tr>
<td><code>authority2</code></td>
<td>Organization that defines the set of security levels that will be used in a network. The authority bits must be a proper subset of this value. (See the <code>authority</code> keywords listed in the second table in the <code>ip security dedicated</code> command section.)</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

All traffic entering or leaving the system must have a security option that falls within this range. Being within range requires that the following two conditions be met:

- The classification level must be greater than or equal to `level1` and less than or equal to `level2`.
- The authority bits must be a superset of `authority1` and a proper subset of `authority2`. That is, `authority1` specifies those authority bits that are required on a packet, and `authority2` specifies the required bits plus any optional authorities that also can be included. If the `authority1` field is the empty set, then a packet is required to specify any one or more of the authority bits in `authority2`. 
The following example specifies levels Unclassified to Secret and NSA authority:

```
ip security multilevel unclassified to secret nsa
```
**ip security reserved-allowed**

To treat as valid any packets that have Reserved1 through Reserved4 security levels, use the `ip security reserved-allowed` command in interface configuration mode. To disallow packets that have security levels of Reserved3 and Reserved2, use the `no` form of this command.

```
ip security reserved-allowed
no ip security reserved-allowed
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you set multilevel security on an interface, and indicate, for example, that the highest range allowed is Confidential, and the lowest is Unclassified, the Cisco IOS software neither allows nor operates on packets that have security levels of Reserved3 and Reserved2 because they are undefined.

If you use the IP Security Option (IPSO) to block transmission out of unclassified interfaces, and you use one of the Reserved security levels, you **must** enable this feature to preserve network security.

**Examples**

The following example allows a security level of Reserved through Ethernet interface 0:

```
interface ethernet 0
  ip security reserved-allowed
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip security add</td>
<td>Adds a basic security option to all outgoing packets.</td>
</tr>
<tr>
<td>ip security dedicated</td>
<td>Sets the level of classification and authority on the interface.</td>
</tr>
<tr>
<td>ip security extended-allowed</td>
<td>Accepts packets on an interface that has an Extended Security Option present.</td>
</tr>
<tr>
<td>ip security first</td>
<td>Prioritizes the presence of security options on a packet.</td>
</tr>
<tr>
<td>ip security ignore-authorities</td>
<td>Causes the Cisco IOS software to ignore the authorities field of all incoming packets.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ip security implicit-labelling</td>
<td>Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.</td>
</tr>
<tr>
<td>ip security multilevel</td>
<td>Sets the range of classifications and authorities on an interface.</td>
</tr>
<tr>
<td>ip security strip</td>
<td>Removes any basic security option on outgoing packets on an interface.</td>
</tr>
</tbody>
</table>
ip security strip

To remove any basic security option on outgoing packets on an interface, use the `ip security strip` command in interface configuration mode. To restore security options, use the `no` form of this command.

```
   ip security strip
   no ip security strip
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The removal procedure is performed after all security tests in the router have been passed. This command is not allowed for multilevel interfaces.

**Examples**

The following example removes any basic security options on outgoing packets on Ethernet interface 0:

```
   interface ethernet 0
   ip security strip
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip security add</strong></td>
<td>Adds a basic security option to all outgoing packets.</td>
</tr>
<tr>
<td><strong>ip security dedicated</strong></td>
<td>Sets the level of classification and authority on the interface.</td>
</tr>
<tr>
<td><strong>ip security extended-allowed</strong></td>
<td>Accepts packets on an interface that has an Extended Security Option present.</td>
</tr>
<tr>
<td><strong>ip security first</strong></td>
<td>Prioritizes the presence of security options on a packet.</td>
</tr>
<tr>
<td><strong>ip security ignoreAuthorities</strong></td>
<td>Causes the Cisco IOS software to ignore the authorities field of all incoming packets.</td>
</tr>
<tr>
<td><strong>ip security implicit-labelling</strong></td>
<td>Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ip security multilevel</td>
<td>Sets the range of classifications and authorities on an interface.</td>
</tr>
<tr>
<td>ip security reserved-allowed</td>
<td>Treats as valid any packets that have Reserved1 through Reserved4 security levels.</td>
</tr>
</tbody>
</table>
ip inspect through ip security strip

ip security strip
ip source-track through ivrf

- ip source-track, on page 606
- ip source-track address-limit, on page 608
- ip source-track export-interval, on page 609
- ip source-track syslog-interval, on page 611
- ip ssh, on page 613
- ip ssh break-string, on page 614
- ip ssh client algorithm encryption, on page 616
- ip ssh client algorithm mac, on page 619
- ip ssh dh min size, on page 621
- ip ssh dscp, on page 622
- ip ssh maxstartups, on page 623
- ip ssh port, on page 624
- ip ssh precedence, on page 626
- ip ssh pubkey-chain, on page 627
- ip ssh rekey, on page 628
- ip ssh rsa keypair-name, on page 629
- ip ssh server algorithm authentication, on page 631
- ip ssh server algorithm encryption, on page 633
- ip ssh server algorithm hostkey, on page 636
- ip ssh server algorithm mac, on page 638
- ip ssh server algorithm publickey, on page 641
- ip ssh server authenticate user, on page 643
- ip ssh source-interface, on page 645
- ip ssh stricthostkeycheck, on page 646
- ip ssh version, on page 647
- ip tacacs source-interface, on page 649
- ip tcp intercept connection-timeout, on page 651
- ip tcp intercept drop-mode, on page 652
- ip tcp intercept finrst-timeout, on page 654
- ip tcp intercept list, on page 655
- ip tcp intercept max-incomplete, on page 656
- ip tcp intercept max-incomplete high, on page 658
- ip tcp intercept max-incomplete low, on page 660
• ip tcp intercept mode, on page 662
• ip tcp intercept one-minute, on page 663
• ip tcp intercept one-minute high, on page 665
• ip tcp intercept one-minute low, on page 667
• ip tcp intercept watch-timeout, on page 669
• ip traffic-export apply, on page 670
• ip traffic-export profile, on page 672
• ip trigger-authentication (global), on page 675
• ip trigger-authentication (interface), on page 677
• ip urlfilter alert, on page 678
• ip urlfilter allowmode, on page 680
• ip urlfilter audit-trail, on page 681
• ip urlfilter cache, on page 683
• ip urlfilter exclusive-domain, on page 685
• ip urlfilter max-request, on page 687
• ip urlfilter max-resp-pak, on page 688
• ip urlfilter server vendor, on page 689
• ip urlfilter source-interface, on page 691
• ip urlfilter truncate, on page 692
• ip urlfilter urlf-server-log, on page 694
• ip verify drop-rate compute interval, on page 695
• ip verify drop-rate compute window, on page 697
• ip verify drop-rate notify hold-down, on page 699
• ip verify unicast notification threshold, on page 700
• ip verify unicast reverse-path, on page 701
• ip verify unicast source reachable-via, on page 705
• ip virtual-reassembly, on page 711
• ip virtual-reassembly-out, on page 714
• ip vrf, on page 716
• ip vrf forwarding, on page 718
• ip vrf forwarding (server-group), on page 719
• ip wccp web-cache accelerated, on page 721
• ips signature update cisco, on page 723
• ipsec profile, on page 724
• ipv4 (ldap), on page 725
• ipv6 crypto map, on page 726
• ipv6 cga modifier rsakeypair, on page 727
• ipv6 cga rsakeypair, on page 729
• ipv6 inspect, on page 730
• ipv6 inspect alert-off, on page 731
• ipv6 inspect audit trail, on page 732
• ipv6 inspect max-incomplete high, on page 733
• ipv6 inspect max-incomplete low, on page 735
• ipv6 inspect name, on page 737
• ipv6 inspect one-minute high, on page 740
• ipv6 inspect one-minute low, on page 742
• ipv6 inspect routing-header, on page 744
• ipv6 inspect tcp idle-time, on page 745
• ipv6 inspect tcp max-incomplete host, on page 747
• ipv6 inspect tcp synwait-time, on page 749
• ipv6 inspect udp idle-time, on page 750
• ipv6 nd inspection, on page 752
• ipv6 nd inspection policy, on page 754
• ipv6 nd prefix framed-ipv6-prefix, on page 756
• ipv6 nd raguard attach-policy, on page 757
• ipv6 nd raguard policy, on page 759
• ipv6 nd secured certificate-db, on page 761
• ipv6 nd secured full-secure, on page 762
• ipv6 nd secured full-secure (interface), on page 763
• ipv6 nd secured key-length, on page 764
• ipv6 nd secured sec-level, on page 765
• ipv6 nd secured timestamp, on page 766
• ipv6 nd secured timestamp-db, on page 767
• ipv6 nd secured trustanchor, on page 768
• ipv6 nd secured trustpoint, on page 769
• ipv6 nd suppress-ra, on page 770
• ipv6 neighbor binding, on page 772
• ipv6 neighbor binding down-lifetime, on page 774
• ipv6 neighbor binding logging, on page 775
• ipv6 neighbor binding max-entries, on page 776
• ipv6 neighbor binding stale-lifetime, on page 778
• ipv6 neighbor binding vlan, on page 779
• ipv6 neighbor tracking, on page 781
• ipv6 port-map, on page 783
• ipv6 radius source-interface, on page 786
• ipv6 routing-enforcement-header loose, on page 787
• ipv6 snooping logging packet drop, on page 788
• ipv6 tacacs source-interface, on page 789
• ipv6 virtual-reassembly, on page 790
• ipv6 virtual-reassembly drop-fragments, on page 792
• ipv6 vrf forwarding, on page 793
• isakmp authorization list, on page 795
• issuer-name, on page 796
• ivrf, on page 799
ip source-track

To enable IP source tracking for a specified host, use the `ip source-track` command in global configuration mode. To disable IP source tracking, use the `no` form of this command.

```
ip source-track ip-address
no ip source-track ip-address
```

**Syntax Description**

| ip-address | Destination IP address of the host that is to be tracked. |

**Command Default**

IP address tracking is not enabled.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(21)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was implemented on the Cisco 7500 series routers.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was implemented on Cisco 12000 series ISE line cards.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(7)T.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

IP source tracking allows you to gather information about the traffic that is flowing to a host that is suspected of being under attack. It also allows you to easily trace a denial-of-service (DoS) attack to its entry point into the network.

After you have identified the destination that is being attacked, enable tracking for the destination address on the whole router by entering the `ip source-track` command.

**Examples**

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for 2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```
Router# configure interface
Router(config)# ip source-track 10.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip source-track address-limit</strong></td>
<td>Configures the maximum number of destination hosts that can be simultaneously tracked at any given moment.</td>
</tr>
<tr>
<td><strong>ip source-track export-interval</strong></td>
<td>Sets the time interval (in seconds) in which IP source tracking statistics are exported from the line card to the RP.</td>
</tr>
<tr>
<td><strong>ip source-track syslog-interval</strong></td>
<td>Sets the time interval (in minutes) in which syslog messages are generated if IP source tracking is enabled on a device.</td>
</tr>
<tr>
<td><strong>show ip source-track</strong></td>
<td>Displays traffic flow statistics for tracked IP host addresses.</td>
</tr>
<tr>
<td><strong>show ip source-track export flows</strong></td>
<td>Displays the last 10 packet flows that were exported from the line card to the route processor.</td>
</tr>
</tbody>
</table>
**ip source-track address-limit**

To configure the maximum number of destination hosts that can be simultaneously tracked at any given moment, use the `ip source-track address-limit` command in global configuration mode. To cancel this administrative limit and return to the default, use the `no` form of this command.

```
ip source-track address-limit number
no ip source-track address-limit number
```

**Syntax Description**

- `number`: Maximum number of hosts that can be tracked.

**Command Default**

An unlimited number of hosts can be tracked.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(21)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was implemented on the Cisco 7500 series routers.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was implemented on Cisco 12000 series ISE line cards.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(7)T.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

After you have configured at least one destination IP address for source tracking (via the `ip source-track` command), you can limit the number of destination IP addresses that can be tracked via the `ip source-track address-limit` command.

**Examples**

The following example shows how to configure IP source tracking for data that flows to host 100.10.1.1 and limit IP source tracking to 10 IP addresses:

```
Router(config)# ip source-track 100.10.0.1
Router(config)# ip source-track address-limit 10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip source-track</td>
<td>Enables IP source tracking for a specified host.</td>
</tr>
<tr>
<td>show ip source-track</td>
<td>Displays traffic flow statistics for tracked IP host addresses.</td>
</tr>
</tbody>
</table>
ip source-track export-interval

To set the time interval (in seconds) in which IP source tracking statistics are exported from the line card to the route processor (RP), use the `ip source-track export-interval` command in global configuration mode. To return to default functionality, use the `no` form of this command.

```
ip source-track export-interval number
no ip source-track export-interval number
```

**Syntax Description**

| number | Number of seconds that pass before IP source tracking statistics are exported. |

**Command Default**

Traffic flow information is exported from the line card to the RP every 30 seconds.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(21)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was implemented on the Cisco 7500 series routers.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was implemented on Cisco 12000 series ISE line cards.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(7)T.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ip source-track export-interval` command to specify the frequency in which IP source tracking information is sent to the RP for viewing.

**Note**

This command can be issued only on distributed platforms such as the gigabit route processor (GRP) and the route switch processor (RSP).

**Examples**

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for 2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```
Router# configure interface
Router(config)# ip source-track 10.10.0.1
```
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip source-track</td>
<td>Enables IP source tracking for a specified host.</td>
</tr>
<tr>
<td></td>
<td>show ip source-track export flows</td>
<td>Displays the last 10 packet flows that were exported from the line card to the route processor.</td>
</tr>
</tbody>
</table>
**ip source-track syslog-interval**

To set the time interval (in minutes) in which syslog messages are generated if IP source tracking is enabled on a device, use the `ip source-track syslog-interval` command in global configuration mode. To cancel this setting and disable syslog generation, use the `no` form of this command.

```
ip source-track syslog-interval number
no ip source-track syslog-interval number
```

**Syntax Description**

| `number` | IP address of the destination that is to be tracked. |

**Command Default**

Syslog messages are not generated.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(21)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was implemented on the Cisco 7500 series routers.</td>
</tr>
<tr>
<td>12.0(26)S</td>
<td>This command was implemented on Cisco 12000 series ISE line cards.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(7)T.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ip source-track syslog-interval` command to track the source interfaces of traffic that are destined to a particular address.

**Examples**

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for 2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```
Router# configure interface
Router(config)# ip source-track 10.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip source-track</td>
<td>Enables IP source tracking for a specified host.</td>
</tr>
<tr>
<td>show ip source-track</td>
<td>Displays traffic flow statistics for tracked IP host addresses.</td>
</tr>
</tbody>
</table>
### ip ssh

To configure Secure Shell (SSH) control parameters on your router, use the **ip ssh** command in global configuration mode. To restore the default value, use the **no** form of this command.

**ip ssh [:timeout seconds][authentication-retries integer]***

**no ip ssh [:timeout seconds][authentication-retries integer]***

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>timeout</strong></td>
<td>(Optional) The time interval that the router waits for the SSH client to respond. This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vty defined (0-4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes.</td>
</tr>
<tr>
<td><strong>seconds</strong></td>
<td>(Optional) The number of seconds until timeout disconnects, with a maximum of 120 seconds. The default is 120 seconds.</td>
</tr>
<tr>
<td><strong>authentication-retries</strong></td>
<td>(Optional) The number of attempts after which the interface is reset.</td>
</tr>
<tr>
<td><strong>integer</strong></td>
<td>(Optional) The number of retries, with a maximum of 5 authentication retries. The default is 3.</td>
</tr>
</tbody>
</table>

#### Command Default

SSH control parameters are set to default router values.

#### Command Modes

Global configuration (config)

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(1)T</td>
<td>This command was integrated into Cisco IOS Release 12.1(1) T.</td>
</tr>
<tr>
<td>12.2(17a)SX</td>
<td>This command was integrated into Cisco IOS Release 12.2(17a)SX.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.4</td>
<td>This command was implemented on the Cisco ASR 1000 series routers.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

Before you configure SSH on your router, you must enable the SSH server using the **crypto key generate rsa** command.

#### Examples

The following examples configure SSH control parameters on your router:

```plaintext
ip ssh timeout 120
ip ssh authentication-retries 3
```
ip ssh break-string

To configure a string that, when received from a Secure Shell (SSH) client, will cause the Cisco IOS SSH server to transmit a break signal out an asynchronous line, use the `ip ssh break-string` command in global configuration mode. To remove the string, use the `no` form of this command.

```
ip ssh break-string string
no ip ssh break-string string
```

**Syntax Description**

| `string` | Any sequence of characters not including embedded whitespace. Include control characters by prefixing them with `^V` (control/V) or denote them using the `\000` notation (that is, a backslash followed by the the ASCII value of the character in three octal digits.) |

**Command Default**

Break signal is not enabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(2)T</td>
<td>This command was integrated into Cisco IOS Release 12.3(2)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Note**

This break string is used only for SSH sessions that are outbound on physical lines using the SSH Terminal-Line Access feature. This break string is not used by the Cisco IOS SSH client, nor is it used by the Cisco IOS SSH server when the server uses a virtual terminal (VTY) line. This break string does not provide any interoperability with the method that is described in the Internet Engineering Task Force (IETF) Internet-Draft “Session Channel Break Extension” (draft-ietf-secsh-break-02.txt).

**Note**

In some versions of Cisco IOS, if the SSH break string is set to a single character, the Cisco IOS server will not immediately process that character as a break signal on receipt of that character but will delay until it has received a subsequent character. A break string of two or more characters will be immediately processed as a break signal after the last character in the string has been received from the SSH client.

**Examples**

The following example shows that the control-B character (ASCII 2) has been set as the SSH break string:

```
Router (config)# ip ssh break-string \002
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip ssh port</strong></td>
<td>Enables SSH access to TTY lines.</td>
</tr>
</tbody>
</table>
ip ssh client algorithm encryption

To define the order of encryption algorithms in a Cisco IOS secure shell (SSH) client, use the `ip ssh {server | client} algorithm encryption` command in global configuration mode. To disable an algorithm from the configured list, use the `no` form of this command. To return to the default behavior in which all encryption algorithms are enabled in the predefined order, use the `default` form of this command.

```
ip ssh client algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | 3des-cbc | aes192-cbc | aes256-cbc}

no ip ssh client algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | 3des-cbc | aes192-cbc | aes256-cbc}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aes128-ctr</td>
<td>Configures Advanced Encryption Standard Counter Mode (AES-CTR) encryption for 128-bit key length.</td>
</tr>
<tr>
<td>aes192-ctr</td>
<td>Configures AES-CTR encryption for 192-bit key length.</td>
</tr>
<tr>
<td>aes256-ctr</td>
<td>Configures AES-CTR encryption for 256-bit key length.</td>
</tr>
<tr>
<td>aes128-cbc</td>
<td>Configures AES Cipher Block Chaining (AES-CBC) 128-bit key length.</td>
</tr>
<tr>
<td>3des-cbc</td>
<td>Configures Triple Data Encryption Standard (3DES) CBC algorithm.</td>
</tr>
<tr>
<td>aes192-cbc</td>
<td>Configures AES-CBC encryption for 192-bit key length.</td>
</tr>
<tr>
<td>aes256-cbc</td>
<td>Configures AES-CBC encryption for 256-bit key length.</td>
</tr>
</tbody>
</table>

**Command Default**

SSH encryption algorithms are set to the following default order:


**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS 15.5(2)S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**Modification**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE 3.15S</td>
<td>This command was integrated into Cisco IOS XE Release 3.15S.</td>
</tr>
<tr>
<td>Cisco IOS 15.5(2)T</td>
<td>This command was integrated into Cisco IOS Release 15.5(2)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To start an encrypted session between an SSH client and server, the preferred mode of encryption needs to be decided. For increased security, the preferred crypto algorithm for an SSH session is AES-CTR.

SSH Version 2 (SSHv2) supports AES-CTR encryption for 128-bit, 192-bit, and 256-bit key length. From the supported AES-CTR algorithms, the preferred algorithm is chosen based on the processing capability. The greater the length of the key, the stronger the encryption.

The Cisco IOS SSH servers and clients support three types of crypto algorithms to encrypt data and select an encryption mode in the following order of preferred encryption:

1. AES-CTR
2. AES-CBC
3. 3DES

If the SSH session uses a remote device that does not support AES-CTR encryption mode, the encryption mode for the session falls back to AES-CBC mode.

The default order of the encryption algorithms are:


To disable more than one algorithm, use the `no` form of the command multiple times with different algorithm names. If you try to disable the last encryption algorithm in the configuration, the following message is displayed, and the command is rejected:

```
% SSH command rejected: All encryption algorithms cannot be disabled
```

**Example**

The following example shows how to configure encryption algorithms on Cisco IOS SSH clients:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-cbc aes256-cbc
Device(config)# end
```

The following example shows how to return to the default behavior in which all encryption algorithms are enabled in the predefined order:

```
Device> enable
Device# configure terminal
Device(config)# default ip ssh client algorithm encryption
Device(config)# end
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip ssh client algorithm mac</code></td>
<td>Defines the order of MAC algorithms in a Cisco IOS SSH client.</td>
</tr>
<tr>
<td><code>ip ssh server algorithm encryption</code></td>
<td>Defines the order of encryption algorithms in a Cisco IOS SSH server.</td>
</tr>
<tr>
<td><code>show ip ssh</code></td>
<td>Displays the status of SSH server connections.</td>
</tr>
</tbody>
</table>
ip ssh client algorithm mac

To define the order of Message Authentication Code (MAC) algorithms in a Cisco IOS secure shell (SSH) client, use the `ip ssh client algorithm mac` command in global configuration mode. To disable an algorithm from the configured list, use the `no` form of this command. To return to the default behavior in which all MAC algorithms are enabled in the predefined order, use the `default` form of this command.

```
ip ssh client algorithm mac {hmac-sha1 | hmac-sha1-96}
no ip ssh client algorithm mac {hmac-sha1 | hmac-sha1-96}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hmac-sha1</td>
<td>Configures the Hashed Message Authentication Code (HMAC) algorithm of HMAC-SHA1 as a cryptographic algorithm.</td>
</tr>
<tr>
<td>hmac-sha1-96</td>
<td>Configures the HMAC algorithm of HMAC-SHA1-20 as a cryptographic algorithm with a digest size of 96 bytes.</td>
</tr>
</tbody>
</table>

**Command Default**

SSH MAC algorithms are set to the following default order:

MAC Algorithms: hmac-sha1, hmac-sha1-96

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS 15.5(2)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.15S</td>
<td>This command was integrated into Cisco IOS XE Release 3.15S.</td>
</tr>
<tr>
<td>Cisco IOS 15.5(2)T</td>
<td>This command was integrated into Cisco IOS Release 15.5(2)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The Cisco IOS SSH servers and clients must have at least one configured Hashed Message Authentication Code (HMAC) algorithm. The Cisco IOS SSH servers and clients support the MAC algorithms in the following order:

1. hmac-sha1
2. hmac-sha1-96

The default order of the MAC algorithms are:

MAC Algorithms: hmac-sha1, hmac-sha1-96
To disable more than one algorithm, use the **no** form of the command multiple times with different algorithm names. If you try to disable the last MAC algorithm in the configuration, the following message is displayed, and the command is rejected:

% SSH command rejected: All mac algorithms cannot be disabled

**Example**

The following example shows how to configure MAC algorithms on Cisco IOS SSH clients:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh client algorithm mac hmac-shal hmac-shal-96
Device(config)# end
```

The following example shows how to return to the default behavior in which all MAC algorithms are enabled in the predefined order:

```
Device> enable
Device# configure terminal
Device(config)# default ip ssh client algorithm mac
Device(config)# end
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip ssh client algorithm encryption</strong></td>
<td>Defines the order of encryption algorithms in a Cisco IOS SSH client.</td>
<td></td>
</tr>
<tr>
<td><strong>ip ssh server algorithm mac</strong></td>
<td>Defines the order of MAC algorithms in a Cisco IOS SSH server.</td>
<td></td>
</tr>
<tr>
<td><strong>show ip ssh</strong></td>
<td>Displays the status of SSH server connections.</td>
<td></td>
</tr>
</tbody>
</table>
**ip ssh dh min size**

To configure the modulus size on the IOS Secure Shell (SSH) server and client, use the `ip ssh dh min size` command in global configuration mode. To configure the default value of 2048 bits, use the `no` form or the `default` form of this command.

```
ip ssh dh min size number
no ip ssh dh min size
default ip ssh dh min size
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Minimum number of bits in the key size. The available options are 2048, and 4096. The default value is 2048.</td>
</tr>
</tbody>
</table>

**Command Default**

Minimum size of Diffie-Hellman (DH) key on IOS SSH server and client is 2048 bits.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(2)S</td>
<td>This command was integrated into Cisco IOS Release 15.1(2)S.</td>
</tr>
<tr>
<td>15.1(1)SY</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)SY.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ip ssh dh min size` command to ensure that the CLI is successfully parsed from either the client side or the server side.

IOS SSH supports the following Diffie-Hellman (DH) key exchange methods:

- Fixed Group Method (`diffie-hellman-group14-sha1 [2048 bits]`)
- Group Exchange Method (`diffie-hellman-group-exchange-sha1 [2048 bits, 4096 bits]`)

In both DH key exchange methods, IOS SSH server and client negotiates and establishes connections with only groups (ranges) whose modulus sizes are equal to or higher than the value configured in the CLI.

**Examples**

The following example shows how to set the minimum modulus size to 2048 bits:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh dh min size 2048
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip ssh</code></td>
<td>Displays the status of SSH server connections.</td>
</tr>
</tbody>
</table>
ip ssh dscp

To specify the IP differentiated services code point (DSCP) value that can be set for a Secure Shell (SSH) configuration, use the `ip ssh dscp` command in global configuration mode. To restore the default value, use the `no` form of this command.

```
ip ssh dscp number
no ip ssh dscp number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Value that can be set. The default value is 0 (zero).</td>
</tr>
<tr>
<td></td>
<td>• number --0 through 63.</td>
</tr>
</tbody>
</table>

**Command Default**
The IP DSCP value is not specified.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2SR</td>
<td>This command is supported in the Cisco IOS Release 12.2SR train. Support in a specific 12.2SR train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>12.4(22)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(22)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
IP DSCP values can be configured on both the SSH client and the SSH server for SSH traffic that is generated on either end.

**Examples**
The following example shows that the DSCP value is set to 35:

```
Router(config)# ip ssh dscp 35
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ssh precedence</td>
<td>Specifies the IP precedence value that may be set.</td>
</tr>
</tbody>
</table>
ip ssh maxstartups

To set the maximum concurrent sessions allowed on a Secure Shell (SSH), use the `ip ssh maxstartups` command in global configuration mode. To disable the configuration, use the `no` form of this command.

```
ip ssh maxstartups [number]
no ip ssh maxstartups [number]
```

**Syntax Description**

| number | (Optional) Number of connections to be accepted concurrently. The range is from 2 to 128. The default is 128. |

**Command Default**

The number of maximum concurrent sessions is 128.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must create RSA keys to enable SSH. The RSA key must be at least 768 bits for SSHv2.

**Examples**

The following example shows how to set the maximum concurrent sessions allowed on a SSH to 100:

```
Router# configure terminal
Router(config)# ip ssh maxstartups 100
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip ssh</td>
<td>Displays debugging messages for SSH.</td>
</tr>
<tr>
<td>ip ssh</td>
<td>Configures SSH control parameters on your router.</td>
</tr>
</tbody>
</table>
ip ssh port

To enable secure access to tty (asynchronous) lines, use the `ip ssh port` command in global configuration mode. To disable this functionality, use the `no` form of this command.

```
ip ssh port port-num rotary group
no ip ssh port port-num rotary group
```

### Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>port-num</code></td>
<td>Specifies the port, such as 2001, to which Secure Shell (SSH) needs to connect.</td>
</tr>
<tr>
<td><code>rotary group</code></td>
<td>Specifies the defined rotary that should search for a valid name.</td>
</tr>
</tbody>
</table>

### Command Default

This command is disabled by default.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `ip ssh port` command supports a functionality that replaces reverse Telnet with SSH. Use this command to securely access the devices attached to the serial ports of a router and to perform the following tasks:

- Connect to a router with multiple terminal lines that are connected to consoles of other devices.
- Allow network available modems to be securely accessed for dial-out.

### Examples

The following example shows how to configure the SSH Terminal-Line Access feature on a modem that is used for dial-out on lines 1 through 200:

```
line 1 200
no exec
login authentication default
transport input ssh
ip ssh port 2000 rotary 1
```

The following example shows how to configure the SSH Terminal-Line Access feature to access the console ports of various devices that are attached to the serial ports of the router. For this type of access, each line is put into its own rotary, and each rotary is used for a single port. In this example, lines 1 through 3 are used, and the port (line) mappings of the configuration are as follows: Port 2001 = Line 1, Port 2002 = Line 2, and Port 2003 = Line 3.

```
line 1
no exec
login authentication default
transport input ssh
line 2
```
no exec
login authentication default
rotary 2
transport input ssh
line 3
no exec
login authentication default
rotary 3
transport input ssh
ip ssh port 2001 rotary 1 3

From any UNIX or UNIX-like device, the following command is typically used to form an S SH session:

```
ssh -c 3des -p 2002 router.example.com
```

This command will initiate an SSH session using the Triple DES cipher to the device known as “router.example.com,” which uses port 2002. This device will connect to the device on Line 2, which was associated with port 2002. Similarly, many Windows SSH packages have related methods of selecting the cipher and the port for this access.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto key generate rsa</td>
<td>Enables the SSH server.</td>
</tr>
<tr>
<td>debug ip ssh</td>
<td>Displays debugging messages for SSH.</td>
</tr>
<tr>
<td>ip ssh</td>
<td>Configures SSH control variables on your router.</td>
</tr>
<tr>
<td>line</td>
<td>Identifies a specific line for configuration and begins the command in line configuration mode.</td>
</tr>
<tr>
<td>rotary</td>
<td>Defines a group of lines consisting of one or more lines.</td>
</tr>
<tr>
<td>ssh</td>
<td>Starts an encrypted session with a remote networking device.</td>
</tr>
<tr>
<td>transport input</td>
<td>Defines which protocols to use to connect to a specific line of the router.</td>
</tr>
</tbody>
</table>
ip ssh precedence

To specify the IP precedence value that can be set for a Secure Shell (SSH) configuration, use the **ip ssh precedence** command in global configuration mode. To restore the default value, use the **no** form of this command.

**ip ssh precedence number**
**no ip ssh precedence number**

| Syntax Description | number | Value that can be set. The default value is 0 (zero).
|--------------------|--------|------------------------------------------------------
|                    |        | • number --0 through 7.                             |

**Command Default**
The IP precedence value is not specified.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(20)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2SR</td>
<td>This command is supported in the Cisco IOS Release 12.2SR train. Support in a specific 12.2SR train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>12.4(22)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(22)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
IP precedence values can be configured on both the SSH client and the SSH server for SSH traffic that is generated on either end.

**Examples**
The following example shows that up to six IP precedence values can be set:

```
Router(config)# ip precedence value 6
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip ssh dscp</strong></td>
<td>Specifies the IP DSCP value that can be set for an SSH configuration.</td>
</tr>
</tbody>
</table>
**ip ssh pubkey-chain**

To configure Secure Shell RSA (SSH-RSA) keys for user and server authentication on the SSH server, use the `ip ssh pubkey-chain` command in global configuration mode. To remove SSH-RSA keys for user and server authentication on the SSH server, use the `no` form of this command.

```
  ip ssh pubkey-chain
  no ip ssh pubkey-chain
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

SSH-RSA keys are not configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(1)S</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ip ssh pubkey-chain` command to ensure SSH server and user public key authentication.

**Examples**

The following example shows how to enable public key generation:

```
Router(config)# ip ssh pubkey-chain
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip ssh stricthostkeycheck</code></td>
<td>Enables strict host key checking on the SSH server.</td>
</tr>
</tbody>
</table>
**ip ssh rekey**

To configure a time-based rekey or a volume-based rekey for a secure shell (SSH) session, use the `ip ssh rekey` command in global configuration mode. To disable the rekey, use the `no` form of this command.

`ip ssh rekey {time time | volume volume}`

`no ip ssh rekey`

---

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>time</code></td>
<td>Rekey time, in minutes. The range is from 10 minutes to 1440 minutes.</td>
</tr>
<tr>
<td><code>volume</code></td>
<td>Amount of rekeyed data, in kilobytes. The range is from 100 KB to 4194303 KB.</td>
</tr>
</tbody>
</table>

**Command Default**

The rekey time or volume is not configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(2)SE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(1)SY</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)SY.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

SSH rekey initiation occurs when the session key negotiated at connection startup is used for an unusually long time. A server or a client initiates a new key exchange based on the maximum number of packets transmitted or based on a specified time. The `ip ssh rekey time` command enables you to specify a time for the rekey initiation. The `ip ssh rekey volume` command enables you to specify a volume that is based on the maximum number of packets transmitted for the rekey initiation. When you use the `no ip ssh rekey` command, the configured time-based rekey or volume-based rekey is disabled.

**Examples**

The following example shows how to configure a time-based rekey for an SSH session:

```
Device(config)# ip ssh rekey time 108
```

The following example shows how to configure a volume-based rekey for an SSH session:

```
Device(config)# ip ssh rekey volume 500
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip ssh</code></td>
<td>Configures SSH control parameters on a device.</td>
</tr>
</tbody>
</table>
**ip ssh rsa keypair-name**

To specify which Rivest, Shamir, and Adelman (RSA) key pair to use for a Secure Shell (SSH) connection, use the `ip ssh rsa keypair-name` command in global configuration mode. To disable the key pair that was configured, use the `no` form of this command.

```
ip ssh rsa keypair-name  keypair-name
no ip ssh rsa keypair-name  keypair-name
```

### Syntax Description

| keypair-name | Name of the key pair. |

### Command Default

If this command is not configured, SSH will use the first RSA key pair that is enabled.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(2)XE</td>
<td>This command was integrated into Cisco IOS Release 12.3(2)XE.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.3(7)JA</td>
<td>This command was integrated into Cisco IOS Release 12.3(7)JA.</td>
</tr>
<tr>
<td>12.0(32)SY</td>
<td>This command was integrated into Cisco IOS Release 12.0(32)SY.</td>
</tr>
<tr>
<td>12.2(33)SXI4</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI4.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Using the `ip ssh rsa keypair-name` command, you can enable an SSH connection using RSA keys that you have configured using the `keypair-name` argument. Previously, SSH was tied to the first RSA keys that were generated (that is, SSH was enabled when the first RSA key pair was generated). The previous behavior still exists, but by using the `ip ssh rsa keypair-name` command, you can overcome that behavior. If you configure the `ip ssh rsa keypair-name` command with a key pair name, SSH is enabled if the key pair exists, or SSH will be enabled if the key pair is generated later. If you use this command, you are not forced to configure a hostname and a domain name.

---

**Note**

A Cisco IOS router can have many RSA key pairs.

### Examples

The following example shows how to specify the RSA key pair “sshkeys” for an SSH connection:

```
Router# configure terminal
Router(config)# ip ssh rsa keypair-name sshkeys
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip ssh</td>
<td>Displays debug messages for SSH.</td>
</tr>
<tr>
<td>disconnect ssh</td>
<td>Terminates a SSH connection on your router.</td>
</tr>
<tr>
<td>ip ssh</td>
<td>Configures SSH control parameters on your router.</td>
</tr>
<tr>
<td>ip ssh version</td>
<td>Specifies the version of SSH to be run on a router.</td>
</tr>
<tr>
<td>show ip ssh</td>
<td>Displays the SSH connections of your router.</td>
</tr>
</tbody>
</table>
**ip ssh server algorithm authentication**

To define the order of user authentication algorithms in a Cisco IOS Secure Shell (SSH) server, use the `ip ssh server algorithm authentication` command in global configuration mode. To disable an algorithm from the configured list, use the `no` form of this command. To return to the default behavior in which all user authentication algorithms are enabled in the predefined order, use the `default` form of this command.

```
ip ssh server algorithm authentication {publickey | keyboard | password}

no ip ssh server algorithm authentication {publickey | keyboard | password}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>publickey</code></td>
<td>Enables the public-key-based authentication method.</td>
</tr>
<tr>
<td><code>keyboard</code></td>
<td>Enables the keyboard-interactive-based authentication method.</td>
</tr>
<tr>
<td><code>password</code></td>
<td>Enables the password-based authentication method.</td>
</tr>
</tbody>
</table>

### Command Default

SSH user authentication algorithms are set to the following default order:

```
Authentication methods: publickey, keyboard-interactive, password
```

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS 15.5(2)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.15S</td>
<td>This command was integrated into Cisco IOS XE Release 3.15S.</td>
</tr>
<tr>
<td>Cisco IOS 15.5(2)T</td>
<td>This command was integrated into Cisco IOS Release 15.5(2)T.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To start a session between an SSH client and server, the preferred mode of user authentication needs to be decided. The IOS SSH server must have at least one configured user authentication algorithm.

The default order of the encryption algorithms are:

```
Authentication methods: publickey, keyboard-interactive, password
```

To disable more than one algorithm, use the `no` form of the command multiple times with different algorithm names. If you try to disable the last user authentication algorithm in the configuration, the following message is displayed, and the command is rejected:
% SSH command rejected: All authentication algorithms can not be disabled.

Example

The following example shows how to configure user authentication algorithms on Cisco IOS SSH servers:

Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm authentication publickey keyboard password
Device(config)# end

The following example shows how to return to the default behavior in which all user authentication algorithms are enabled in the predefined order:

Device> enable
Device# configure terminal
Device(config)# default ip ssh server algorithm authentication
Device(config)# end

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ssh client algorithm encryption</td>
<td>Defines the order of encryption algorithms in a Cisco IOS SSH client.</td>
</tr>
<tr>
<td>ip ssh server algorithm hostkey</td>
<td>Defines the order of host key algorithms in a Cisco IOS SSH server.</td>
</tr>
<tr>
<td>ip ssh server algorithm mac</td>
<td>Defines the order of MAC algorithms in a Cisco IOS SSH server.</td>
</tr>
<tr>
<td>ip ssh server algorithm publickey</td>
<td>Defines the order of public key algorithms in a Cisco IOS SSH server.</td>
</tr>
<tr>
<td>show ip ssh</td>
<td>Displays the status of SSH server connections.</td>
</tr>
</tbody>
</table>
ip ssh server algorithm encryption

To define the order of encryption algorithms in a Cisco IOS secure shell (SSH) server, use the `ip ssh server algorithm encryption` command in global configuration mode. To disable an algorithm from the configured list, use the `no` form of this command. To return to the default behavior in which all encryption algorithms are enabled in the predefined order, use the `default` form of this command.

```
ip ssh server algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | 3des-cbc | aes192-cbc | aes256-cbc}
```

```
oip ssh server algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | 3des-cbc | aes192-cbc | aes256-cbc}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aes128-ctr</code></td>
<td>Configures Advanced Encryption Standard Counter Mode (AES-CTR) encryption for 128-bit key length.</td>
</tr>
<tr>
<td><code>aes192-ctr</code></td>
<td>Configures AES-CTR encryption for 192-bit key length.</td>
</tr>
<tr>
<td><code>aes256-ctr</code></td>
<td>Configures AES-CTR encryption for 256-bit key length.</td>
</tr>
<tr>
<td><code>aes128-cbc</code></td>
<td>Configures AES Cipher Block Chaining (AES-CBC) 128-bit key length.</td>
</tr>
<tr>
<td><code>3des-cbc</code></td>
<td>Configures Triple Data Encryption Standard (3DES) CBC algorithm.</td>
</tr>
<tr>
<td><code>aes192-cbc</code></td>
<td>Configures AES-CBC encryption for 192-bit key length.</td>
</tr>
<tr>
<td><code>aes256-cbc</code></td>
<td>Configures AES-CBC encryption for 256-bit key length.</td>
</tr>
</tbody>
</table>

### Command Default

SSH encryption algorithms are set to the following default order:

```
```

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS 15.5(2)S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**Release** | **Modification**
---|---
Cisco IOS XE 3.15S | This command was integrated into Cisco IOS XE Release 3.15S.
Cisco IOS 15.5(2)T | This command was integrated into Cisco IOS Release 15.5(2)T.

**Usage Guidelines**

To start an encrypted session between an SSH client and server, the preferred mode of encryption needs to be decided. For increased security, the preferred crypto algorithm for an SSH session is AES-CTR.

SSH Version 2 (SSHv2) supports AES-CTR encryption for 128-bit, 192-bit, and 256-bit key length. From the supported AES-CTR algorithms, the preferred algorithm is chosen based on the processing capability. The greater the length of the key, the stronger the encryption.

The Cisco IOS SSH servers and clients support three types of crypto algorithms to encrypt data and select an encryption mode in the following order of preferred encryption:

1. AES-CTR
2. AES-CBC
3. 3DES

If the SSH session uses a remote device that does not support AES-CTR encryption mode, the encryption mode for the session falls back to AES-CBC mode.

The default order of the encryption algorithms are:


To disable more than one algorithm, use the `no` form of the command multiple times with different algorithm names. If you try to disable the last encryption algorithm in the configuration, the following message is displayed, and the command is rejected:

```
% SSH command rejected: All encryption algorithms cannot be disabled
```

**Example**

The following example shows how to configure encryption algorithms on Cisco IOS SSH servers:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-cbc aes256-cbc
Device(config)# end
```

The following example shows how to return to the default behavior in which all encryption algorithms are enabled in the predefined order:

```
Device> enable
Device# configure terminal
Device(config)# default ip ssh server algorithm encryption
Device(config)# end
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ip ssh client algorithm encryption</code></td>
<td>Defines the order of encryption algorithms in a Cisco IOS SSH client.</td>
</tr>
<tr>
<td></td>
<td><code>ip ssh server algorithm hostkey</code></td>
<td>Defines the order of host key algorithms in a Cisco IOS SSH server.</td>
</tr>
<tr>
<td></td>
<td><code>ip ssh server algorithm mac</code></td>
<td>Defines the order of MAC algorithms in a Cisco IOS SSH server.</td>
</tr>
<tr>
<td></td>
<td><code>show ip ssh</code></td>
<td>Displays the status of SSH server connections.</td>
</tr>
</tbody>
</table>
**ip ssh server algorithm hostkey**

To define the order of host key algorithms in a Cisco IOS secure shell (SSH) server, use the `ip ssh server algorithm hostkey` command in global configuration mode. To disable an algorithm from the configured list, use the `no` form of this command. To return to the default behavior in which all host key algorithms are enabled in the predefined order, use the `default` form of this command.

```
ip ssh server algorithm hostkey \{x509v3-ssh-rsa | ssh-rsa\}
no ip ssh server algorithm hostkey \{x509v3-ssh-rsa | ssh-rsa\}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>x509v3-ssh-rsa</th>
<th>Configures certificate-based authentication.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ssh-rsa</td>
<td>Configures public key based authentication.</td>
</tr>
</tbody>
</table>

**Command Default**

SSH host key algorithms are set to the following default order:

Hostkey Algorithms: x509v3-ssh-rsa, ssh-rsa

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS 15.5(1)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.14S</td>
<td>This command was integrated into Cisco IOS XE Release 3.14S.</td>
</tr>
<tr>
<td>Cisco IOS 15.5(2)T</td>
<td>This command was integrated into Cisco IOS Release 15.5(2)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The IOS SSH server and client must have at least one configured host key algorithm. The Cisco IOS SSH servers support the host key algorithms in the following order:

1. x509v3-ssh-rsa
2. ssh-rsa

The default order of the host key algorithms are:

Hostkey Algorithms: x509v3-ssh-rsa, ssh-rsa

To disable more than one algorithm, use the `no` form of the command multiple times with different algorithm names. If you try to disable the last host key algorithm in the configuration, the following message is displayed, and the command is rejected:
% SSH command rejected: All hostkey algorithms cannot be disabled

Example

The following example shows how to configure host key algorithms on Cisco IOS SSH servers:

Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa ssh-rsa
Device(config)# end

The following example shows how to return to the default behavior in which all host key algorithms are enabled in the predefined order:

Device> enable
Device# configure terminal
Device(config)# default ip ssh server algorithm hostkey
Device(config)# end

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>ip ssh server algorithm encryption</strong></td>
<td>Defines the order of encryption algorithms in a Cisco IOS SSH server.</td>
</tr>
<tr>
<td></td>
<td><strong>ip ssh server algorithm mac</strong></td>
<td>Defines the order of MAC algorithms in a Cisco IOS SSH server.</td>
</tr>
<tr>
<td></td>
<td><strong>ip ssh server algorithm publickey</strong></td>
<td>Defines the order of public key algorithms in a Cisco IOS SSH server.</td>
</tr>
<tr>
<td></td>
<td><strong>show ip ssh</strong></td>
<td>Displays the status of SSH server connections.</td>
</tr>
</tbody>
</table>
ip ssh server algorithm mac

To define the order of Message Authentication Code (MAC) algorithms in a Cisco IOS secure shell (SSH) server and client, use the `ip ssh server algorithm mac` command in global configuration mode. To disable an algorithm from the configured list, use the `no` form of this command. To return to the default behavior in which all MAC algorithms are enabled in the predefined order, use the `default` form of this command.

```
ip ssh server algorithm mac {hmac-sha1|hmac-sha1-96|hmac-sha2-256|hmac-sha2-512} | hmac-sha1-96|hmac-sha1|hmac-sha2-256|hmac-sha2-512} | hmac-sha1-96|hmac-sha2-256|hmac-sha1|hmac-sha1-96|hmac-sha2-512} | hmac-sha1-96|hmac-sha2-512|hmac-sha1|hmac-sha1-96|hmac-sha2-256|hmac-sha2-512}
```

**Syntax Description**

- **hmac-sha1**
  - Configures the Hashed Message Authentication Code (HMAC) algorithm of HMAC-SHA1 as a cryptographic algorithm with a digest size of 160 bits and key length of 160 bits.

- **hmac-sha1-96**
  - Configures the HMAC algorithm of HMAC-SHA1-20 as a cryptographic algorithm with a digest size of 96 bits and key length of 160 bits.

- **hmac-sha2-256**
  - Configures the HMAC algorithm of HMAC-SHA2-256 as a cryptographic algorithm with a digest size of 256 bits and a key length of 256 bits.

- **hmac-sha2-512**
  - Configures the HMAC algorithm of HMAC-SHA2-512 as a cryptographic algorithm with a digest size of 512 bits and a key length of 512 bits.

**Command Default**

SSH MAC algorithms are set to the following default order:

MAC Algorithms: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS 15.5(2)S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Release | Modification
--- | ---
Cisco IOS XE 3.15S | This command was integrated into Cisco IOS XE Release 3.15S.
Cisco IOS 15.5(2)T | This command was integrated into Cisco IOS Release 15.5(2)T.
Cisco IOS XE Everest 16.5.1b | The Hmac-SHA2 mac algorithm for SSH was introduced.

### Usage Guidelines

The Cisco IOS SSH servers and clients must have at least one configured Hashed Message Authentication Code (HMAC) algorithm and can have more than one HMAC algorithm configured. The Cisco IOS SSH servers and clients support the MAC algorithms in the following order:

1. hmac-sha1
2. hmac-sha1-96
3. hmac-sha2-256
4. hmac-sha2-512

The default order of the MAC algorithms are:

MAC Algorithms: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512

To disable more than one algorithm, use the `no` form of the command multiple times with different algorithm names. If you try to disable the last MAC algorithm in the configuration, the following message is displayed, and the command is rejected:

```
% SSH command rejected: All mac algorithms cannot be disabled
```

### Example

The following example shows how to configure MAC algorithms on Cisco IOS SSH servers:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm mac hmac-sha1 hmac-sha1-96
Device(config)# end
```

The following example shows how to return to the default behavior in which all MAC algorithms are enabled in the predefined order:

```
Device> enable
Device# configure terminal
Device(config)# default ip ssh server algorithm mac
Device(config)# end
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip ssh client algorithm mac</code></td>
<td>Defines the order of MAC algorithms in a Cisco IOS SSH client.</td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip ssh server algorithm encryption</code></td>
<td>Defines the order of encryption algorithms in a Cisco IOS SSH server.</td>
</tr>
<tr>
<td><code>ip ssh server algorithm hostkey</code></td>
<td>Defines the order of host key algorithms in a Cisco IOS SSH server.</td>
</tr>
<tr>
<td><code>show ip ssh</code></td>
<td>Displays the status of SSH server connections.</td>
</tr>
</tbody>
</table>
ip ssh server algorithm publickey

To define the order of public key algorithms in a Cisco IOS secure shell (SSH) server for user authentication, use the `ip ssh server algorithm publickey` command in global configuration mode. To disable an algorithm from the configured list, use the no form of this command. To return to the default behavior in which all public key algorithms are enabled in the predefined order, use the default form of this command.

```
ip ssh server algorithm publickey {x509v3-ssh-rsa | ssh-rsa}
no ip ssh server algorithm publickey {x509v3-ssh-rsa | ssh-rsa}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>x509v3-ssh-rsa</td>
<td>Configures certificate-based authentication.</td>
</tr>
<tr>
<td>ssh-rsa</td>
<td>Configures public key based authentication.</td>
</tr>
</tbody>
</table>

**Command Default**

SSH public key algorithms are set to the following default order:

```
Authentication Publickey Algorithms: x509v3-ssh-rsa, ssh-rsa
```

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS 15.5(1)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.14S</td>
<td>This command was integrated into Cisco IOS XE Release 3.14S.</td>
</tr>
<tr>
<td>Cisco IOS 15.5(2)T</td>
<td>This command was integrated into Cisco IOS Release 15.5(2)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The IOS SSH server and client must have at least one configured public key algorithm. The Cisco IOS SSH servers support the public key algorithms in the following order:

1. x509v3-ssh-rsa
2. ssh-rsa

The default order of the host key algorithms are:

```
Authentication Publickey Algorithms: x509v3-ssh-rsa, ssh-rsa
```

To disable more than one algorithm, use the no form of the command multiple times with different algorithm names. If you try to disable the last public key algorithm in the configuration, the following message is displayed, and the command is rejected:

```
% SSH command rejected: All publickey algorithms cannot be disabled.
```
Example

The following example shows how to configure public key algorithms on Cisco IOS SSH servers:

Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm publickey x509v3-ssh-rsa ssh-rsa
Device(config)# end

The following example shows how to return to the default behavior in which all public key algorithms are enabled in the predefined order:

Device> enable
Device# configure terminal
Device(config)# default ip ssh server algorithm publickey
Device(config)# end

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip ssh client algorithm encryption</strong></td>
<td>Defines the order of encryption algorithms in a Cisco IOS SSH client.</td>
</tr>
<tr>
<td><strong>ip ssh client algorithm mac</strong></td>
<td>Defines the order of MAC algorithms in a Cisco IOS SSH client.</td>
</tr>
<tr>
<td><strong>ip ssh server algorithm encryption</strong></td>
<td>Defines the order of encryption algorithms in a Cisco IOS SSH server.</td>
</tr>
<tr>
<td><strong>ip ssh server algorithm hostkey</strong></td>
<td>Defines the order of host key algorithms in a Cisco IOS SSH server.</td>
</tr>
<tr>
<td><strong>ip ssh server algorithm mac</strong></td>
<td>Defines the order of MAC algorithms in a Cisco IOS SSH server.</td>
</tr>
<tr>
<td><strong>show ip ssh</strong></td>
<td>Displays the status of SSH server connections.</td>
</tr>
</tbody>
</table>
To enable the user authentication methods available in a Cisco IOS Secure Shell (SSH) server, use the **ip ssh server authenticate user** command in global configuration mode. To disable the user authentication methods available in a Cisco IOS SSH server, use the **no** form of this command. To return to the default behavior in which all user authentication methods are enabled in the predefined order, use the **default** form of this command.

```
ip ssh server authenticate user {publickey | keyboard | password}
```

```
no ip ssh server authenticate user {publickey | keyboard | password}
```

```
default ip ssh server authenticate user
```

**Syntax Description**

- **publickey** Enables the public-key-based authentication method.
- **keyboard** Enables the keyboard-interactive-based authentication method.
- **password** Enables the password-based authentication method.

**Command Default**

All three user authentication methods are enabled in the following predefined order:

- Public-key authentication method
- Keyboard-interactive authentication method
- Password authentication method

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3(3)M</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.10S</td>
<td>This command was integrated into Cisco IOS XE Release 3.10S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **no ip ssh authenticate user {publickey | keyboard | password}** command enables the SSH server to choose a preferred user authentication method by disabling any of the other supported user authentication methods. By default, all user authentication methods are enabled on the SSH server in the following predefined order:

- Public-key authentication method
- Keyboard-interactive authentication method
- Password authentication method

The following messages are displayed during specific scenarios:
If the public-key-based authentication method is disabled using the `no ip ssh server authenticate user publickey` command, the RFC 4252 (The Secure Shell (SSH) Authentication Protocol) behavior in which public-key authentication is mandatory is overridden and the following warning message is displayed:

```
%SSH: Publickey disabled. Overriding RFC
```

If all three authentication methods are disabled, the following warning message is displayed:

```
%SSH: No auth method configured. Incoming connection will be dropped
```

In the event of an incoming SSH session request from the SSH client when all three user authentication methods are disabled on the SSH server, the connection request is dropped at the SSH server and a system log message is available in the following format:

```
%SSH-3-NO_USERAUTH: No auth method configured for SSH Server. Incoming connection from <ip address> (tty = <ttynum>) dropped
```

The following example shows how to disable the public-key-based authentication and keyboard-interactive-based authentication methods, allowing the SSH client to connect to the SSH server using password-based authentication:

```
Device> enable
Device# configure terminal
Device(config)# no ip ssh server authenticate user publickey
%SSH: Publickey disabled. Overriding RFC
Device(config)# no ip ssh server authenticate user keyboard
Device(config)# exit
```

The following example shows how to enable the public-key-based authentication and keyboard-interactive-based authentication methods:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server authenticate user publickey
Device(config)# ip ssh server authenticate user keyboard
Device(config)# exit
```

The following example shows how to return to the default behavior in which all user authentication methods are enabled in the predefined order:

```
Device> enable
Device# configure terminal
Device(config)# default ip ssh server authenticate user
Device(config)# exit
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip ssh</code></td>
<td>Displays the version and configuration data for SSH.</td>
</tr>
</tbody>
</table>
**ip ssh source-interface**

To specify the IP address of an interface as the source address for a Secure Shell (SSH) client device, use the `ip ssh source-interface` command in global configuration mode. To remove the IP address as the source address, use the `no` form of this command.

```
ip ssh source-interface interface
no ip ssh source-interface interface
```

**Syntax Description**
- `interface` - The interface whose address is used as the source address for the SSH client.

**Command Default**
The address of the closest interface to the destination is used as the source address (the closest interface is the output interface through which the SSH packet is sent).

**Command Modes**
- Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
By specifying this command, you can force the SSH client to use the IP address of the source interface as the source address.

**Examples**
In the following example, the IP address assigned to Ethernet interface 0 will be used as the source address for the SSH client:

```
ip ssh source-interface ethernet0
```
ip ssh stricthostkeycheck

To enable strict host key checking on the Secure Shell (SSH) server, use the `ip ssh stricthostkeycheck` command in global configuration mode. To disable strict host key checking, use the `no` form of this command.

```
ip ssh stricthostkeycheck
no ip ssh stricthostkeycheck
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Strict host key checking on the SSH server is not enabled.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(1)S</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `ip ssh stricthostkeycheck` command to ensure SSH server side strict checking. Configuring the `ip ssh stricthostkeycheck` command authenticates all servers.

**Note**
This command is not available on SSH Version 1.

- If the `ip ssh pubkey-chain` command is not configured, the `ip ssh stricthostkeycheck` command will lead to connection failure in SSH Version 2.

**Examples**
The following example shows how to enable strict host key checking:

```
Router(config)# ip ssh stricthostkeycheck
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ssh pubkey-chain</td>
<td>Configures SSH-RSA keys for user and server authentication on the SSH server.</td>
</tr>
</tbody>
</table>
**ip ssh version**

To specify the version of Secure Shell (SSH) to be run on a router, use the `ip ssh version` command in global configuration mode. To disable the version of SSH that was configured and to return to compatibility mode, use the `no` form of this command.

```
ip ssh version [{1|2}]
no ip ssh version [{1|2}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`{1</td>
<td>2}`</td>
</tr>
<tr>
<td>`{1</td>
<td>2}`</td>
</tr>
</tbody>
</table>

**Command Default**

If this command is not configured, SSH operates in compatibility mode, that is, Version 1 and Version 2 are both supported.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(2)XE</td>
<td>This command was integrated into Cisco IOS Release 12.3(2)XE.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.3(7)JA</td>
<td>This command was integrated into Cisco IOS Release 12.3(7)JA.</td>
</tr>
<tr>
<td>12.0(32)SY</td>
<td>This command was integrated into Cisco IOS Release 12.0(32)SY.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
<tr>
<td>15.2(2)SA2</td>
<td>This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can use this command with the `2` keyword to ensure that your router will not inadvertently establish a weaker SSH Version 1 connection.

**Examples**

The following example shows that only SSH Version 1 support is configured:

```
Router (config)# ip ssh version 1
```

The following example shows that only SSH Version 2 is configured:

```
Router (config)# ip ssh version 2
```

The following example shows that SSH Versions 1 and 2 are configured:

```
Router (config)# no ip ssh version
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip ssh</td>
<td>Displays debug messages for SSH.</td>
</tr>
<tr>
<td>disconnect ssh</td>
<td>Terminates a SSH connection on your router.</td>
</tr>
<tr>
<td>ip ssh</td>
<td>Configures SSH control parameters on your router.</td>
</tr>
<tr>
<td>ip ssh rsa keypair-name</td>
<td>Specifies which RSA key pair to use for a SSH connection.</td>
</tr>
<tr>
<td>show ip ssh</td>
<td>Displays the SSH connections of your router.</td>
</tr>
</tbody>
</table>
ip tacacs source-interface

To use the IP address of a specified interface for all outgoing TACACS+ packets, use the `ip tacacs source-interface` command in global configuration or server-group configuration mode. To disable use of the specified interface IP address, use the `no` form of this command.

```
ip tacacs source-interface subinterface-name vrf vrf-name
no ip tacacs source-interface
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>subinterface-name</code></td>
<td>Name of the interface that TACACS+ uses for all of its outgoing packets.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>VPN routing/forwarding parameter name.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global configuration (config)

Server-group configuration (server-group)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced in server-group configuration mode.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>12.2(54)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(54)SG.</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>The <code>vrf vrf-name</code> keyword-argument pair was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to set the IP address of a subinterface for all outgoing TACACS+ packets. This address is used as long as the interface is in the `up` state. In this way, the TACACS+ server can use one IP address entry associated with the network access client instead of maintaining a list of all IP addresses.

This command is especially useful in cases where the router has many interfaces and you want to ensure that all TACACS+ packets from a particular router have the same IP address.

The specified sub-interface should have a valid IP address and should be in the `up` state for a valid configuration. If the specified sub-interface does not have a valid IP address or is in the `down` state, TACACS+ enforces the
source-interface configuration. In case the interface has no IP address, a null IP address is sent. To avoid this, add a valid IP address to the sub-interface or bring the sub-interface to the up state.

**Note**

This command can be configured globally or in server-group configuration mode. If this command is configured in the server-group configuration mode, the IP address of the specified interface is used for packets that are going only to servers that are defined in that server group. If this command is not configured in server-group configuration mode, the global configuration applies.

**Examples**

The following example makes TACACS+ use the IP address of subinterface “s2” for all outgoing TACACS+ packets:

```
ip tacacs source-interface s2
```

In the following example, TACACS+ is to use the IP address of Loopback0 for packets that are going only to server 10.1.1.1:

```
aaa group server tacacs+ tacacs1
    server-private 10.1.1.1 port 19 key cisco
    ip vrf forwarding cisco
    ip tacacs source-interface Loopback0
    ip vrf cisco
    rd 100:1
interface Loopback0
    ip address 10.0.0.2 255.0.0.0
    ip vrf forwarding cisco
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip radius source-interface</strong></td>
<td>Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.</td>
</tr>
<tr>
<td><strong>ip telnet source-interface</strong></td>
<td>Allows a user to select an address of an interface as the source address for Telnet connections.</td>
</tr>
<tr>
<td><strong>ip tftp source-interface</strong></td>
<td>Allows a user to select the interface whose address will be used as the source address for TFTP connections.</td>
</tr>
<tr>
<td><strong>ip vrf forwarding (server-group)</strong></td>
<td>Configures the VRF reference of an AAA RADIUS or TACACS+ server group.</td>
</tr>
<tr>
<td><strong>server-private</strong></td>
<td>Configures the IP address of the private RADIUS or TACACS+ server for the group server.</td>
</tr>
</tbody>
</table>
**ip tcp intercept connection-timeout**

To change how long a TCP connection will be managed by the TCP intercept after no activity, use the `ip tcp intercept connection-timeout` command in global configuration mode. To restore the default, use the `no` form of this command.

```
ip tcp intercept connection-timeout seconds
no ip tcp intercept connection-timeout [seconds]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>seconds</th>
<th>Time (in seconds) that the software will still manage the connection after no activity. The minimum value is 1 second. The default is 86,400 seconds (24 hours).</th>
</tr>
</thead>
</table>

**Command Default**

86,400 seconds (24 hours)

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 F</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ip tcp intercept connection-timeout` command to change how long a TCP connection will be managed by the TCP intercept after a period of inactivity.

**Examples**

The following example sets the software to manage the connection for 12 hours (43,200 seconds) after no activity:

```
ip tcp intercept connection-timeout 43200
```
ip tcp intercept drop-mode

To set the TCP intercept drop mode, use the `ip tcp intercept drop-mode` command in global configuration mode. To restore the default, use the `no` form of this command.

```
ip tcp intercept drop-mode [{oldest|random}]
no ip tcp intercept drop-mode [{oldest|random}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>oldest</td>
<td>(Optional) Software drops the oldest partial connection. This is the default.</td>
</tr>
<tr>
<td>random</td>
<td>(Optional) Software drops a randomly selected partial connection.</td>
</tr>
</tbody>
</table>

**Command Default**

`oldest`

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 F</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the number of incomplete connections exceeds 1100 or the number of connections arriving in the last 1 minute exceeds 1100, the TCP intercept feature becomes more aggressive. When this happens, each new arriving connection causes the oldest partial connection to be deleted, and the initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection will be cut in half).

Note that the 1100 threshold can be configured with the `ip tcp intercept max-incomplete high` and `ip tcp intercept one-minute high` commands.

Use the `ip tcp intercept drop-mode` command to change the dropping strategy from oldest to a random drop.

**Examples**

The following example sets the drop mode to random:

```
ip tcp intercept drop-mode random
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip tcp intercept max-incomplete high</code></td>
<td>Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.</td>
</tr>
<tr>
<td><code>ip tcp intercept max-incomplete low</code></td>
<td>Defines the number of incomplete connections below which the software leaves aggressive mode.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>ip tcp intercept one-minute high</strong></td>
<td>Defines the number of connection requests received in the last one-minute sample period before the software enters aggressive mode.</td>
</tr>
<tr>
<td><strong>ip tcp intercept one-minute low</strong></td>
<td>Defines the number of connection requests below which the software leaves aggressive mode.</td>
</tr>
</tbody>
</table>
ip tcp intercept finrst-timeout

To change how long after receipt of a reset or FIN-exchange the software ceases to manage the connection, use the `ip tcp intercept finrst-timeout` command in global configuration mode. To restore the default, use the `no` form of this command.

```
ip tcp intercept finrst-timeout seconds
no ip tcp intercept finrst-timeout [seconds]
```

**Syntax Description**

| `seconds` | Time (in seconds) after receiving a reset or FIN-exchange that the software ceases to manage the connection. The minimum value is 1 second. The default is 5 seconds. |

**Command Default**

5 seconds

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 F</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Even after the two ends of the connection are joined, the software intercepts packets being sent back and forth. Use this command if you need to adjust how soon after receiving a reset or FIN-exchange the software stops intercepting packets.

**Examples**

The following example sets the software to wait for 10 seconds before it leaves intercept mode:

```
ip tcp intercept finrst-timeout 10
```
ip tcp intercept list

To enable TCP intercept, use the `ip tcp intercept list` command in global configuration mode. To disable TCP intercept, use the `no` form of this command.

```
ip tcp intercept list access-list-number
no ip tcp intercept list access-list-number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list-number</code></td>
<td>Extended access list number in the range from 100 to 199.</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 F</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The TCP intercept feature intercepts TCP connection attempts and shields servers from TCP SYN-flood attacks, also known as denial-of-service attacks.

TCP packets matching the access list are presented to the TCP intercept code for processing, as determined by the `ip tcp intercept mode` command. The TCP intercept code either intercepts or watches the connections.

To have all TCP connection attempts submitted to the TCP intercept code, have the access list match everything.

**Examples**

The following example configuration defines access list 101, causing the software to intercept packets for all TCP servers on the 192.168.1.0/24 subnet:

```
ip tcp intercept list 101
!
access-list 101 permit tcp any 192.168.1.0 0.0.0.255
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list (IP extended)</code></td>
<td>Defines an extended IP access list.</td>
</tr>
<tr>
<td><code>ip tcp intercept mode</code></td>
<td>Changes the TCP intercept mode.</td>
</tr>
<tr>
<td><code>show tcp intercept connections</code></td>
<td>Displays TCP incomplete and established connections.</td>
</tr>
<tr>
<td><code>show tcp intercept statistics</code></td>
<td>Displays TCP intercept statistics.</td>
</tr>
</tbody>
</table>
ip tcp intercept max-incomplete

To define either the number of incomplete connections below which the software leaves aggressive mode or the maximum number of incomplete connections allowed before the software enters aggressive mode, use the `ip tcp intercept max-incomplete` command in global configuration mode. To restore the default, use the `no` form of this command.

```
ip tcp intercept max-incomplete low number high number
no ip tcp intercept max-incomplete [low number high number]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>low number</th>
<th>Defines the number of incomplete connections below which the software leaves aggressive mode. The range is 1 to 2147483647. The default is 900</th>
</tr>
</thead>
<tbody>
<tr>
<td>high number</td>
<td>Defines the number of incomplete connections allowed, above which the software enters aggressive mode. The range is from 1 to 2147483647. The default is 1100.</td>
</tr>
</tbody>
</table>

**Command Default**

The number of incomplete connections below which the software leaves aggressive mode is 900.

The maximum number of incomplete connections allowed before the software enters aggressive mode is 1100.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)T</td>
<td>This command was introduced in Cisco IOS Release 12.4(15)T. This command replaces the <code>ip tcp intercept max-incomplete low</code> and the <code>ip tcp intercept max-incomplete high</code> commands.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

There are two factors that determine aggressive mode: connection requests and incomplete connections.

By default, if both the number of connection requests and the number of incomplete connections is 900 or lower, aggressive mode ends.

By default, if either the number of connection requests or the number of incomplete connections is 1100 or greater, aggressive mode begins.

The number of connection requests may be defined by the `ip tcp intercept one-minute` command and the number of incomplete connections may be defined by the `ip tcp intercept max-incomplete` command.

**Characteristics of Aggressive Mode**

The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.
- The initial retransmission timeout, the total time the router attempts to establish the connection, is reduced from 1 second to 0.5 seconds.
- The watch-timeout period is reduced from 30 seconds to 15 seconds.
Examples

The following example sets the software to leave aggressive mode when the number of incomplete connections falls below 1000 and allows 1500 incomplete connections before the software enters aggressive mode. The running configuration is also shown.

```
Router(config)# ip tcp intercept max-incomplete low 1000 high 1500
Router(config)# show running config | i ip tcp
    ip tcp intercept one-minute low 1000 high 1400
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip tcp intercept drop-mode</td>
<td>Sets the TCP intercept drop mode.</td>
</tr>
<tr>
<td>ip tcp intercept one-minute</td>
<td>Defines the number of connection requests below which the software leaves aggressive mode and the number of connection requests received before the software enters aggressive mode.</td>
</tr>
</tbody>
</table>
ip tcp intercept max-incomplete high

**Note**
Effective with Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(15)T, the `ip tcp intercept max-incomplete high` command is replaced by the `ip tcp intercept max-incomplete` command. See the `ip tcp intercept max-incomplete` command for more information.

To define the maximum number of incomplete connections allowed before the software enters aggressive mode, use the `ip tcp intercept max-incomplete high number` command in global configuration mode. To restore the default, use the `no` form of this command.

```plaintext
ip tcp intercept max-incomplete high number
no ip tcp intercept max-incomplete high [number]
```

**Syntax Description**
- `number`: Defines the number of incomplete connections allowed, above which the software enters aggressive mode. The range is from 1 to 2147483647. The default is 1100.

**Command Default**
1100 incomplete connections

**Command Modes**
- Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 F</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(15)T</td>
<td>This command was replaced by the <code>ip tcp intercept max-incomplete</code> command.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was replaced by the <code>ip tcp intercept max-incomplete</code> command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Note**
If you are running Cisco IOS Release 12.2(33)SXH or Cisco IOS Release 12.4(15)T and issue the `ip tcp intercept max-incomplete high` command, it will be accepted by the router, but a message will be displayed stating that the `ip tcp intercept max-incomplete high` command has been replaced by the `ip tcp intercept max-incomplete` command.

If the number of incomplete connections exceeds the `number` configured, the TCP intercept feature becomes aggressive. The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.
- The initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection is cut in half).
- The watch-timeout is cut in half (from 30 seconds to 15 seconds).
You can change the drop strategy from the oldest connection to a random connection with the `ip tcp intercept drop-mode` command.

---

**Note**

The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* `ip tcp intercept one-minute high` or `ip tcp intercept max-incomplete high` is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of `ip tcp intercept one-minute low` and `ip tcp intercept max-incomplete low`, aggressive mode ends.

The software will back off from its aggressive mode when the number of incomplete connections falls below the number specified by the `ip tcp intercept max-incomplete low` command.

---

**Examples**

The following example allows 1500 incomplete connections before the software enters aggressive mode:

```
ip tcp intercept max-incomplete high 1500
```

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip tcp intercept drop-mode</code></td>
<td>Sets the TCP intercept drop mode.</td>
</tr>
<tr>
<td><code>ip tcp intercept max-incomplete low</code></td>
<td>Defines the number of incomplete connections below which the software leaves aggressive mode.</td>
</tr>
<tr>
<td><code>ip tcp intercept one-minute high</code></td>
<td>Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.</td>
</tr>
<tr>
<td><code>ip tcp intercept one-minute low</code></td>
<td>Defines the number of connection requests below which the software leaves aggressive mode.</td>
</tr>
</tbody>
</table>
ip tcp intercept max-incomplete low

---

**Note**

Effective with Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(15)T, the `ip tcp intercept max-incomplete low` command is replaced by the `ip tcp intercept max-incomplete` command. See the `ip tcp intercept max-incomplete` command for more information.

To define the number of incomplete connections below which the software leaves aggressive mode, use the `ip tcp intercept max-incomplete low` command in global configuration mode. To restore the default, use the `no` form of this command.

```
ip tcp intercept max-incomplete low number
no ip tcp intercept max-incomplete low [number]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>number</th>
<th>Defines the number of incomplete connections below which the software leaves aggressive mode. The range is 1 to 2147483647. The default is 900.</th>
</tr>
</thead>
</table>

**Command Default**

900 incomplete connections

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 F</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(15)T</td>
<td>This command was replaced by the <code>ip tcp intercept max-incomplete</code> command.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was replaced by the <code>ip tcp intercept max-incomplete</code> command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Note**

If you are running Cisco IOS Release 12.2(33)SXH, or Cisco IOS Release 12.4(15)T and issue the `ip tcp intercept max-incomplete low` command, it will be accepted by the router, but a message will be displayed stating that the `ip tcp intercept max-incomplete high` command has been replaced by the `ip tcp intercept max-incomplete` command.

When both connection requests and incomplete connections fall below the values of `ip tcp intercept one-minute low` and `ip tcp intercept max-incomplete low`, the TCP intercept feature leaves aggressive mode.
The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of either `ip tcp intercept one-minute high` or `ip tcp intercept max-incomplete high` is exceeded, aggressive mode begins. When both connection requests and incomplete connections fall below the values of `ip tcp intercept one-minute low` and `ip tcp intercept max-incomplete low`, aggressive mode ends.

See the `ip tcp intercept max-incomplete high` command for a description of aggressive mode.

**Examples**

The following example sets the software to leave aggressive mode when the number of incomplete connections falls below 1000:

```plaintext
ip tcp intercept max-incomplete low 1000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip tcp intercept drop-mode</code></td>
<td>Sets the TCP intercept drop mode.</td>
</tr>
<tr>
<td><code>ip tcp intercept max-incomplete high</code></td>
<td>Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.</td>
</tr>
<tr>
<td><code>ip tcp intercept one-minute high</code></td>
<td>Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.</td>
</tr>
<tr>
<td><code>ip tcp intercept one-minute low</code></td>
<td>Defines the number of connection requests below which the software leaves aggressive mode.</td>
</tr>
</tbody>
</table>
ip tcp intercept mode

To change the TCP intercept mode, use the `ip tcp intercept mode` command in global configuration mode. To restore the default, use the `no` form of this command.

```
ip tcp intercept mode {intercept|watch}
no ip tcp intercept mode [{intercept|watch}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>intercept</td>
<td>Active mode in which the TCP intercept software intercepts TCP packets from clients to servers that match the configured access list and performs intercept duties. This is the default.</td>
</tr>
<tr>
<td>watch</td>
<td>Monitoring mode in which the software allows connection attempts to pass through the router and watches them until they are established.</td>
</tr>
</tbody>
</table>

**Command Default**

`intercept`

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 F</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When TCP intercept is enabled, it operates in intercept mode by default. In intercept mode, the software actively intercepts TCP SYN packets from clients to servers that match the specified access list. For each SYN, the software responds on behalf of the server with an ACK and SYN, and waits for an ACK of the SYN from the client. When that ACK is received, the original SYN is sent to the server, and the code then performs a three-way handshake with the server. Then the two half-connections are joined.

In watch mode, the software allows connection attempts to pass through the router, but watches them until they become established. If they fail to become established in 30 seconds (or the value set by the `ip tcp intercept watch-timeout` command), a Reset is sent to the server to clear its state.

**Examples**

The following example sets the mode to watch mode:

```
ip tcp intercept mode watch
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip tcp intercept watch-timeout</td>
<td>Defines how long the software will wait for a watched TCP intercept connection to reach established state before sending a reset to the server.</td>
</tr>
</tbody>
</table>
### ip tcp intercept one-minute

To define both the number of connection requests below which the software leaves aggressive mode and the number of connection requests that can be received before the software enters aggressive mode, use the `ip tcp intercept one-minute` command in global configuration mode. To restore the default connection request settings, use the `no` form of this command.

**Syntax**

```
ip tcp intercept one-minute low number high number
no ip tcp intercept one-minute [low number high number]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>low number</th>
<th>Specifies the number of connection requests in the last one-minute sample period below which the software leaves aggressive mode. The range is from 1 to 2147483647. The default is 900.</th>
</tr>
</thead>
<tbody>
<tr>
<td>high number</td>
<td>Specifies the number of connection requests that can be received in the last one-minute sample period before the software enters aggressive mode. The range is 1 to 2147483647. The default is 1100.</td>
</tr>
</tbody>
</table>

**Command Default**

The default number of connection requests below which the software leaves aggressive mode is 900.

The default number of connection requests received before the software enters aggressive mode is 1100.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)T</td>
<td>This command was introduced in Cisco IOS Release 12.4(15)T. This command replaces the <code>ip tcp intercept one-minute low</code> and the <code>ip tcp intercept one-minute high</code> commands.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

There are two factors that determine aggressive mode: connection requests and incomplete connections.

By default, if both the number of connection requests and the number of incomplete connections is 900 or lower, aggressive mode ends.

By default, if either the number of connection requests or the number of incomplete connections is 1100 or greater, aggressive mode begins.

The number of connection requests may be defined by the `ip tcp intercept one-minute` command and the number of incomplete connections may be defined by the `ip tcp intercept max-incomplete` command. The default number of connection requests

**Characteristics of Aggressive Mode**

The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.
- The initial retransmission timeout, the total time the router attempts to establish the connection, is reduced from 1 second to 0.5 seconds.
• The watch-timeout period is reduced from 30 seconds to 15 seconds.

Examples

The following example sets the software to leave aggressive mode when the number of connection requests falls below 1000 and allows 1400 connection requests before the software enters aggressive mode. The the running configuration is then shown.

```
Router(config)# ip tcp intercept one-minute low 1000 high 1400
Router(config)# show running configuration | i ip tcp
    ip tcp intercept one-minute low 1000 high 1400
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip tcp intercept drop-mode</td>
<td>Sets the TCP intercept drop mode.</td>
</tr>
<tr>
<td>ip tcp intercept max-incomplete</td>
<td>Defines the number of incomplete connections below which the software leaves aggressive mode or the maximum number of incomplete connections allowed before the software enters aggressive mode.</td>
</tr>
</tbody>
</table>
ip tcp intercept one-minute high

**Note**

Effective with Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(15)T the `ip tcp intercept one-minute high` command is replaced by the `ip tcp intercept one-minute` command. See the `ip tcp intercept one-minute` command for more information.

To define the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode, use the `ip tcp intercept one-minute high` command in global configuration mode.

To restore the default, use the `no` form of this command.

```
ip tcp intercept one-minute high number
no ip tcp intercept one-minute high [number]
```

**Syntax Description**

- `number` Specifies the number of connection requests that can be received in the last one-minute sample period before the software enters aggressive mode. The range is 1 to 2147483647. The default is 1100.

**Command Default**

1100 connection requests

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 F</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(15)T</td>
<td>This command was replaced by the <code>ip tcp intercept one-minute</code> command.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was replaced by the <code>ip tcp intercept one-minute</code> command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If you are running Cisco IOS Release 12.2(33)SXH or Cisco IOS Release 12.4(15)T and issue the `ip tcp intercept one-minute high` command, it will be accepted by the router, but a message will be displayed stating that the `ip tcp intercept one-minute high` command has been replaced by the `ip tcp intercept one-minute` command.

- If the number of connection requests exceeds the `number` value configured, the TCP intercept feature becomes aggressive. The following are the characteristics of aggressive mode:
  - Each new arriving connection causes the oldest partial connection to be deleted.
  - The initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection is cut in half).
  - The watch-timeout is cut in half (from 30 seconds to 15 seconds).
You can change the drop strategy from the oldest connection to a random connection with the **ip tcp intercept drop-mode** command.

**Note**
The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of either **ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When both connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, aggressive mode ends.

**Examples**
The following example allows 1400 connection requests before the software enters aggressive mode:

```
ip tcp intercept one-minute high 1400
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip tcp intercept drop-mode</strong></td>
<td>Sets the TCP intercept drop mode.</td>
</tr>
<tr>
<td><strong>ip tcp intercept max-incomplete high</strong></td>
<td>Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.</td>
</tr>
<tr>
<td><strong>ip tcp intercept max-incomplete low</strong></td>
<td>Defines the number of incomplete connections below which the software leaves aggressive mode.</td>
</tr>
<tr>
<td><strong>ip tcp intercept one-minute low</strong></td>
<td>Defines the number of connection requests below which the software leaves aggressive mode.</td>
</tr>
</tbody>
</table>
ip tcp intercept one-minute low

Effective with Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(15)T, the `ip tcp intercept one-minute low` command is replaced by the `ip tcp intercept one-minute` command. See the `ip tcp intercept one-minute` command for more information.

To define the number of connection requests below which the software leaves aggressive mode, use the `ip tcp intercept one-minute low` command in global configuration mode. To restore the default, use the `no` form of this command.

```
ip tcp intercept one-minute low number
no ip tcp intercept one-minute low [number]
```

**Syntax Description**

- `number` Defines the number of connection requests in the last one-minute sample period below which the software leaves aggressive mode. The range is from 1 to 2147483647. The default is 900.

**Command Default**

900 connection requests

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 F</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(15)T</td>
<td>This command was replaced by the <code>ip tcp intercept one-minute</code> command.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was replaced by the <code>ip tcp intercept one-minute</code> command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you are running Cisco IOS Release 12.2(33)SXH or Cisco IOS Release 12.4(15)T and issue the `ip tcp intercept one-minute low` command, it will be accepted by the router, but a message will be displayed stating that the `ip tcp intercept one-minute low` command has been replaced by the `ip tcp intercept one-minute` command.

When both connection requests and incomplete connections fall below the values of `ip tcp intercept one-minute low` and `ip tcp intercept max-incomplete low`, the TCP intercept feature leaves aggressive mode.
The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of either `ip tcp intercept one-minute high` or `ip tcp intercept max-incomplete high` is exceeded, aggressive mode begins. When both connection requests and incomplete connections fall below the values of `ip tcp intercept one-minute low` and `ip tcp intercept max-incomplete low`, aggressive mode ends.

See the `ip tcp intercept one-minute high` command for a description of aggressive mode.

### Examples

The following example sets the software to leave aggressive mode when the number of connection requests falls below 1000:

```
ip tcp intercept one-minute low 1000
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip tcp intercept drop-mode</code></td>
<td>Sets the TCP intercept drop mode.</td>
</tr>
<tr>
<td><code>ip tcp intercept max-incomplete high</code></td>
<td>Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.</td>
</tr>
<tr>
<td><code>ip tcp intercept max-incomplete low</code></td>
<td>Defines the number of incomplete connections below which the software leaves aggressive mode.</td>
</tr>
<tr>
<td><code>ip tcp intercept one-minute high</code></td>
<td>Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.</td>
</tr>
</tbody>
</table>
**ip tcp intercept watch-timeout**

To define how long the software will wait for a watched TCP intercept connection to reach established state before sending a reset to the server, use the `ip tcp intercept watch-timeout` command in global configuration mode. To restore the default, use the `no` form of this command.

```
ip tcp intercept watch-timeout seconds
no ip tcp intercept watch-timeout [seconds]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
<th>Time (in seconds) that the software waits for a watched connection to reach established state before sending a Reset to the server. The minimum value is 1 second. The default is 30 seconds.</th>
</tr>
</thead>
</table>

**Command Default**

30 seconds

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 F</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command if you have set the TCP intercept to passive watch mode and you want to change the default time the connection is watched. During aggressive mode, the watch timeout time is cut in half.

**Examples**

The following example sets the software to wait 60 seconds for a watched connection to reach established state before sending a Reset to the server:

```
ip tcp intercept watch-timeout 60
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip tcp intercept mode</code></td>
<td>Changes the TCP intercept mode.</td>
</tr>
</tbody>
</table>
ip traffic-export apply

To apply an IP traffic export profile or an IP traffic capture profile to a specific interface, use the `ip traffic-export apply` command in interface configuration mode. To remove an IP traffic export profile or an IP traffic capture profile from an interface, use the `no` form of this command.

```
ip traffic-export apply profile-name
no ip traffic-export apply profile-name
```

Cisco 1841, Cisco 2800 Series, and Cisco 3800 Series

```
ip traffic-export apply profile-name size
no ip traffic-export apply profile-name
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile-name</td>
<td>Name of the profile that is to be applied to a specified interface. The <code>profile-name</code> argument must match a name that was specified in the <code>ip traffic-export profile</code> command.</td>
</tr>
<tr>
<td>size</td>
<td>Optional. Used in IP traffic capture mode to set up a local capture buffer.</td>
</tr>
<tr>
<td>size</td>
<td>Optional. Specifies the size of the local capture buffer, in bytes.</td>
</tr>
</tbody>
</table>

### Command Default

If you do not use this command, a successfully configured profile is not active.

### Command Modes

Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was updated to incorporate the <code>size</code> keyword and <code>size</code> argument for IP traffic capture mode on the Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

After you configure at least one export profile, use the `ip traffic-export apply` command to activate IP traffic export on the specified ingress interface.

After you configure a capture profile, use the `ip traffic-export apply` command to activate IP traffic capture on the specified ingress interface, and to specify the size of the local capture buffer.

### Examples

The following example shows how to apply the export profile “corp1” to interface Fast Ethernet 0/0.

```
Router(config)# ip traffic-export profile corp1
Router(config)# interface FastEthernet 0/1
Router(config)# bidirectional
Router(config)# mac-address 00a.8aab.90a0
Router(config)# outgoing sample one-in-every 50
Router(config)# incoming access-list spam_acl
```
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1

The following example shows how to apply the capture profile “corp2” to interface Fast Ethernet 0/0, and specify a capture buffer of 10,000,000 bytes.

Router(config)# ip traffic-export profile corp2 mode_capture
Router(config-rite)# bidirectional
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# length 512
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp2 size 10000000

After a profile is activated on the interface, a logging message such as the following will appear:

%RITE-5-ACTIVATE: Activated IP traffic export on interface FastEthernet 0/0.

After a profile is removed from the interface, a logging message such as the following will appear:

%RITE-5-DEACTIVATE: Deactivated IP traffic export on interface FastEthernet 0/0.

If you attempt to apply an incomplete profile to an interface, you will receive the following message:

Router(config-if)# ip traffic-export apply newone
RITE: profile newone has missing outgoing interface

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip traffic-export profile</td>
<td>Creates or edits an IP traffic export profile and enables the profile on an ingress interface.</td>
</tr>
<tr>
<td>traffic-export</td>
<td>Controls the operation of IP traffic capture mode.</td>
</tr>
</tbody>
</table>
ip traffic-export profile

To create or edit an IP traffic export profile or an IP traffic capture profile and enable the profile on an ingress interface, use the `ip traffic-export profile` command in global configuration mode. To remove an IP traffic export profile from your router configuration, use the `no` form of this command.

```plaintext
ip traffic-export profile profile-name
no ip traffic-export profile profile-name
```

Cisco 1841, Cisco 2800 Series, and Cisco 3800 Series Routers

```plaintext
ip traffic-export profile profile-name mode {capture|export}
no ip traffic-export profile profile-name
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile-name</td>
<td>IP traffic export profile name.</td>
</tr>
<tr>
<td>mode {capture</td>
<td>export}</td>
</tr>
</tbody>
</table>

- **capture** -- Captures data to memory.
- **export** -- Exports data to an interface.

Command Default

A profile does not exist.

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was updated to incorporate the mode, capture, and export keywords on the Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The `ip traffic-export profile` command allows you to begin a profile that can be configured to capture or export IP packets as they arrive on or leave from a selected router ingress interface.

When exporting IP packets, a designated egress interface exports IP packets out of the router. So, the router can export unaltered IP packets to a directly connected device.

When capturing IP packets, the packets are stored in local router memory. They may then be dumped to an external device.

**IP Traffic Export Profiles**

All exported IP traffic configurations are specified by profiles, which consist of RITE-related command-line interface (CLI) commands that control various attributes of both incoming and outgoing IP traffic. You can
configure a router with multiple profiles. (Each profile must have a different name.) You can apply different profiles on different interfaces.

The two profiles to configure are:

- Global configuration profile, which you configure using the `ip traffic-export profile` command.

- Submode configuration profile, which you configure using any of the following RITE commands—`bidirectional`, `incoming`, `interface`, `mac-address`, and `outgoing`.

Use `interface` and `mac-address` commands to successfully create a profile. If you do not issue these commands, the user will receive a profile incomplete messages such as the following:

```
ip traffic-export profile newone
! No outgoing interface configured
! No destination mac-address configured
```

After you configure your profiles, you can apply the profiles to an interface with the `ip traffic-export apply profile` command, which will activate it.

**IP Traffic Capture Profiles**

On the Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers, you can also configure IP traffic capture. A captured IP traffic configuration is specified by a profile, which consists of RITE-related command-line interface (CLI) commands that control various attributes of both incoming and outgoing IP traffic.

The two profiles that you should configure are:

- Global configuration profile, which you configure using the `ip traffic-export profile mode capture` command.

- Submode configuration profile, which you configure using any of the following RITE commands—`bidirectional`, `incoming`, `length`, and `outgoing`.

After you configure your profiles, you can apply the profiles to an interface with the `ip traffic-export apply profile` command, which will activate it.

When the IP traffic capture profile is applied to an interface, use the `traffic-export` command to control the capture of the traffic.

---

**Note**

Cisco IOS Release 12.4(9)T and 12.4(15)T cannot capture outgoing router-generated Internet Control Message Protocol (ICMP) or IPsec traffic.

---

**Examples**

The following example shows how to configure the profile "corp1," which sends captured IP traffic to host "00a.8aab.90a0" at the interface "FastEthernet 0/1." This profile is also configured to export 1 in every 50 packets and to allow incoming traffic only from the access control list (ACL) "ham_ACL."

```console
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
```
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1

The following example shows how to configure the profile "corp2," which captures IP traffic and stores it in a local router memory buffer of 10,000,000 bytes. This profile also captures 1 in every 50 packets and allows incoming traffic only from the access control list (ACL) "ham_ACL."

Router(config)# ip traffic-export profile corp2 mode capture
Router(config-rite)# bidirectional
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# length 512
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp2 size 10000000

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bidirectional</td>
<td>Enables incoming and outgoing IP traffic to be exported or captured across a monitored interface.</td>
</tr>
<tr>
<td>incoming</td>
<td>Configures filtering for incoming export or capture traffic.</td>
</tr>
<tr>
<td>interface (RITE)</td>
<td>Specifies the outgoing interface for exporting traffic.</td>
</tr>
<tr>
<td>ip traffic-export apply profile</td>
<td>Applies an IP traffic export or IP traffic capture profile to a specific interface.</td>
</tr>
<tr>
<td>length</td>
<td>Specifies the length of the packet in capture mode.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Specifies the Ethernet address of the destination host in traffic export.</td>
</tr>
<tr>
<td>outgoing</td>
<td>Configures filtering for outgoing export or capture traffic.</td>
</tr>
<tr>
<td>traffic-export interface</td>
<td>Controls the operation of IP traffic capture mode.</td>
</tr>
</tbody>
</table>
ip trigger-authentication (global)

To enable the automated part of double authentication at a device, use the `ip trigger-authentication` command in global configuration mode. To disable the automated part of double authentication, use the `no` form of this command.

```
ip trigger-authentication [timeout seconds] [port number]
no ip trigger-authentication
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>timeout seconds</code></td>
<td>(Optional) Specifies how frequently the local device sends a User Datagram Protocol (UDP) packet to the remote host to request the user’s username and password (or PIN). The default is 90 seconds. See “The Timeout Keyword” in the Usage Guidelines section for details.</td>
</tr>
<tr>
<td><code>port number</code></td>
<td>(Optional) Specifies the UDP port to which the local router should send the UDP packet requesting the user’s username and password (or PIN). The default is port 7500. See “The Port Keyword” in the Usage Guidelines section for details.</td>
</tr>
</tbody>
</table>

**Command Default**

The default timeout is 90 seconds, and the default port number is 7500.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Configure this command on the local device (router or network access server) that remote users dial in to. Use this command only if the local device has already been configured to provide double authentication; this command enables automation of the second authentication of double authentication.

The **timeout** Keyword

During the second authentication stage of double authentication—when the remote user is authenticated—the remote user must send a username and password (or PIN) to the local device. With automated double authentication, the local device sends a UDP packet to the remote user’s host during the second user-authentication stage. This UDP packet triggers the remote host to launch a dialog box requesting a username and password (or PIN).

If the local device does not receive a valid response to the UDP packet within a timeout period, the local device will send another UDP packet. The device will continue to send UDP packets at the timeout intervals until it receives a response and can authenticate the user.

By default, the UDP packet timeout interval is 90 seconds. Use the **timeout** keyword to specify a different interval.
(This timeout also applies to how long entries will remain in the remote host table; see the `show ip trigger-authentication` command for details.)

**The port Keyword**

As described in the previous section, the local device sends a UDP packet to the remote user’s host to request the user’s username and password (or PIN). This UDP packet is sent to UDP port 7500 by default. (The remote host client software listens to UDP port 7500 by default.) If you need to change the port number because port 7500 is used by another application, you should change the port number using the `port` keyword. If you change the port number you need to change it in both places—both on the local device and in the remote host client software.

**Examples**

The following example globally enables automated double authentication and sets the timeout to 120 seconds:

```plaintext
ip trigger-authentication timeout 120
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip trigger-authentication (interface)</code></td>
<td>Specifies automated double authentication at an interface.</td>
</tr>
<tr>
<td><code>show ip trigger-authentication</code></td>
<td>Displays the list of remote hosts for which automated double authentication has been attempted.</td>
</tr>
</tbody>
</table>
ip trigger-authentication (interface)

To specify automated double authentication at an interface, use the `ip trigger-authentication` command in interface configuration mode. To turn off automated double authentication at an interface, use the `no` form of this command.

```
ip trigger-authentication
no ip trigger-authentication
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Automated double authentication is not enabled for specific interfaces.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Configure this command on the local router or network access server that remote users dial into. Use this command only if the local device has already been configured to provide double authentication and if automated double authentication has been enabled with the `ip trigger-authentication (global)` command.

This command causes double authentication to occur automatically when users dial into the interface.

**Examples**

The following example turns on automated double authentication at the ISDN BRI interface BRI0:

```
interface BRI0
ip trigger-authentication
encapsulation ppp
ppp authentication chap
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip trigger-authentication (global)</code></td>
<td>Enables the automated part of double authentication at a device.</td>
</tr>
</tbody>
</table>
**ip urlfilter alert**

To enable URL filtering system alert messages, use the `ip urlfilter alert` command in global configuration mode. To disable the system alert, use the `no` form of this command.

```
ip urlfilter alert [vrf vrf-name]
no ip urlfilter alert
```

**Syntax Description**

| **vrf vrf-name** | (Optional) Enables URL filtering system alert messages only for the specified Virtual Routing and Forwarding (VRF) interface. |

**Command Default**

URL filtering messages are enabled.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(11)YU</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>vrf vrf-name</code> keyword/argument pair was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ip urlfilter alert` command to display system messages, such as a server entering allow mode, a server going down, or a URL that is too long for the lookup request.

**Examples**

The following example shows how to enable URL filtering alert messages:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 192.168.3.1
```

Afterward, system alert messages such as the following are displayed:

```
%URLF-3-SERVER_DOWN: Connection to the URL filter server 10.92.0.9 is down
This level three LOG_ERR-type message is displayed when a configured URL filter server (UFS) goes down. When this happens, the firewall will mark the configured server as secondary and try to bring up one of the other secondary servers and mark that server as the primary server. If there is no other server configured, the firewall will enter into allow mode and display the URLF-3-ALLOW_MODE message described.

%URLF-3-ALLOW_MODE: Connection to all URL filter servers are down and ALLOW MODE is OFF
This LOG_ERR type message is displayed when all UFSs are down and the system enters into allow mode.
```
Whenever the system goes into allow mode (all filter servers are down), a periodic keepalive timer will be triggered that will try to bring up a server by opening a TCP connection.

Note
%URLF-5-SERVER_UP: Connection to an URL filter server 10.92.0.9 is made, the system is returning from ALLOW MODE

This LOG_NOTICE-type message is displayed when the UFSs are detected as being up and the system is returning from allow mode.

%URLF-4-URL_TOO_LONG: URL too long (more than 3072 bytes), possibly a fake packet?

This LOG_WARNING-type message is displayed when the URL in a lookup request is too long; any URL longer than 3K will be dropped.

%URLF-4-MAX_REQ: The number of pending request exceeds the maximum limit <1000>

This LOG_WARNING-type message is displayed when the number of pending requests in the system exceeds the maximum limit and all further requests are dropped.
**ip urlfilter allowmode**

To turn on the default mode (allow mode) of the filtering algorithm, use the `ip urlfilter allowmode` command in global configuration mode. To disable the default mode, use the `no` form of this command.

```
ip urlfilter allowmode [{on|off}] [vrf vrf-name]
no ip urlfilter allowmode [{on|off}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>on</code></td>
<td>(Optional) Allow mode is on.</td>
</tr>
<tr>
<td><code>off</code></td>
<td>(Optional) Allow mode is off.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Turns on the default mode of the filtering algorithm only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

Allow mode is off.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(11)YU</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>vrf vrf-name</code> keyword and argument pair was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The system will go into allow mode when connections to all vendor servers (Websense or N2H2) are down. The system will return to normal mode when a connection to at least one web vendor server is up. Allow mode directs your system to forward or drop all packets on the basis of the configurable allow mode setting: if allow mode is on and the vendor servers are down, the HTTP requests will be allowed to pass; if allow mode is off and the vendor servers are down, the HTTP requests will be forbidden.

**Examples**

The following example shows how to enable allow mode on your system:

```
ip urlfilter allowmode on
```

Afterward, the following alert message will be displayed when the system goes into allow mode:

```
%URLF-3-ALLOW_MODE: Connection to all URL filter servers are down and ALLOW MODE if OFF
```

The following alert message will be displayed when the system returns from allow mode:

```
%URLF-5-SERVER_UP: Connection to an URL filter server 12.0.0.3 is made, the system is returning from allow mode
```
ip urlfilter audit-trail

To log messages into the syslog server or router, use the **ip urlfilter audit-trail** command in global configuration mode. To disable this functionality, use the **no** form of this command.

```
ip urlfilter audit-trail [vrf vrf-name]
no ip urlfilter audit-trail
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vrf</strong> vrf-name</td>
<td>(Optional) Logs messages into the syslog server or router only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

This command is disabled.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(11)YU</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <strong>vrf</strong> vrf-name keyword and argument pair was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **ip urlfilter audit-trail** command to log messages such as URL request status (allow or deny) into your syslog server.

**Examples**

The following example shows how to enable syslog message logging:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 209.165.202.130
```

Afterward, audit trail messages such as the following are displayed and logged into the log server:

```
%URLF-6-SITE_ALLOWED:Client 209.165.201.15:12543 accessed server 10.76.82.21:8080
```

This message is logged for each request whose destination IP address is found in the cache. It includes the source IP address, source port number, destination IP address, and destination port number. The URL is not logged in this case because the IP address of the request is found in the cache; thus, parsing the request and extracting the URL is a waste of time.

```
```

This message is logged when a request finds a match against one of the blocked domains in the exclusive-domain list or the corresponding entry in the IP cache.
This message is logged for each URL request that is allowed by the vendor server (Websense or N2H2). It includes the allowed URL, source IP address, source port number, destination IP address, and destination port number. Longer URLs will be truncated to 300 bytes and then logged.

This message is logged for each URL request that is blocked by the vendor server. It includes the blocked URL, source IP address, source port number, destination IP address, and destination port number. Longer URLs will be truncated to 300 bytes and then logged.
ip urlfilter cache

To configure cache parameters, use the `ip urlfilter cache` command in global configuration mode. To clear the configuration, use the `no` form of this command.

```
ip urlfilter cache number [vrf vrf-name]
no ip urlfilter cache number
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>number</strong></td>
</tr>
<tr>
<td><strong>vrf vrf-name</strong></td>
</tr>
</tbody>
</table>

**Command Default**
Maximum number of destination IP addresses is 5000.
The cache table is cleared out every 12 hours.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(11)YU</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <strong>vrf vrf-name</strong> keyword and argument pair was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The cache table consists of the most recently requested IP addresses and respective authorization status for each IP address.

The caching algorithm involves three parameters--the maximum number of IP addresses that can be cached, an idle time, and an absolute time. The algorithm also involves two timers--idle timer and absolute timer. The idle timer is a small periodic timer (1 minute) that checks to see whether the number of cached IP addresses in the cache table exceeds 80 percent of the maximum limit. If the cached IP addresses have exceeded 80 percent, it will start removing idle entries; if it has not exceeded 80 percent, it will quit and wait for the next cycle. The absolute timer is a large periodic timer (1 hour) that is used to remove all of the elapsed entries. (The age of an elapsed entry is greater than the absolute time.) An elapsed entry will also be removed during cache lookup.

The idle time value is fixed at 10 minutes. The absolute time value is taken from the vendor server look-up response, which is often greater than 15 hours. The absolute value for cache entries made out of exclusive-domains is 12 hours. The maximum number of cache entries is configurable by enabling the `ip urlfilter cache` command.

**Note**
The vendor server is not able to inform the Cisco IOS firewall of filtering policy changes in the database.
The following example shows how to configure the cache table to hold a maximum of five destination IP addresses:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 192.168.3.1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip urlfilter cache</td>
<td>Clears the cache table.</td>
</tr>
<tr>
<td>show ip urlfilter cache</td>
<td>Displays the destination IP addresses that are cached into the cache table.</td>
</tr>
</tbody>
</table>
**ip urlfilter exclusive-domain**

To add or remove a domain name to or from the exclusive domain list so that the firewall does not have to send lookup requests to the vendor server, use the `ip urlfilter exclusive-domain` command in global configuration mode. To remove a domain name from the exclusive domain name list, use the `no` form of this command.

```
ip urlfilter exclusive-domain {permit|deny} domain-name [vrf vrf-name]
no ip urlfilter exclusive-domain {permit|deny} domain-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>permit</code></td>
<td>Permits all traffic destined for the specified domain name.</td>
</tr>
<tr>
<td><code>deny</code></td>
<td>Blocks all traffic destined for the specified domain name.</td>
</tr>
<tr>
<td><code>domain-name</code></td>
<td>Domain name that is added or removed from the exclusive domain name list; for example, <a href="http://www.cisco.com">www.cisco.com</a>.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Adds or removes a domain name only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

This command is not enabled.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(11)YU</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>vrf vrf-name</code> keyword and argument pair was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ip urlfilter exclusive-domain` command allows you to specify a list of domain names (exclusive domains) so that the firewall will not create a lookup request for the HTTP traffic that is destined for one of the domains in the exclusive list. Thus, you can avoid sending look-up requests to the web server for HTTP traffic that is destined for a host that is completely allowed to all users.

Flexibility when entering domain names is also provided; that is, the user can enter the complete domain name or a partial domain name.

**Complete Domain Name**

If the user adds a complete domain name, such as “www.cisco.com,” to the exclusive domain list, all HTTP traffic whose URLs are destined for this domain (such as www.cisco.com/news and www.cisco.com/index) will be excluded from the URL filtering policies of the vendor server (Websense or N2H2), and on the basis of the configuration, the URLs will be permitted or blocked (denied).

**Partial Domain Name**

If the user adds only a partial domain name to the exclusive domain list, such as “.cisco.com,” all URLs whose domain names end with this partial domain name (such as www.cisco.com/products and www.cisco.com/eng)
will be excluded from the URL filtering policies of the vendor server (Websense or N2H2), and on the basis of the configuration, the URLs will be permitted or blocked (denied).

Examples

The following example shows how to add the complete domain name “www.cisco.com” to the exclusive domain name list. This configuration will block all traffic destined to the www.cisco.com domain.

```
ip urlfilter exclusive-domain deny www.cisco.com
```

The following example shows how to add the partial domain name “.cisco.com” to the exclusive domain name list. This configuration will permit all traffic destined to domains that end with .cisco.com.

```
ip urlfilter exclusive-domain permit .cisco.com
```
ip urlfilter max-request

To set the maximum number of outstanding requests that can exist at any given time, use the `ip urlfilter max-request` command in global configuration mode. To disable this function, use the `no` form of this command.

```
ip urlfilter max-request number [vrf vrf-name]
no ip urlfilter max-request number
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>number</strong></td>
<td>Maximum number of outstanding requests. The default value is 1000.</td>
</tr>
<tr>
<td><strong>vrf vrf-name</strong></td>
<td>(Optional) Sets the maximum number of outstanding requests only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

Maximum number of requests is 1000.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(11)YU</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>vrf vrf-name</code> keyword and argument pair was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the specified maximum number of outstanding requests is exceeded, new requests will be dropped.

Allow mode is not considered because it should be used only when servers are down.

**Examples**

The following example shows how to configure the maximum number of outstanding requests to 950:

```
ip inspect name url_filter http
ip urlfilter max-request 950
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip inspect name</td>
<td>Defines a set of inspection rules.</td>
</tr>
<tr>
<td>ip urlfilter server vendor</td>
<td>Configures a vendor server for URL filtering.</td>
</tr>
</tbody>
</table>
ip urlfilter max-resp-pak

To configure the maximum number of HTTP responses that the firewall can keep in its packet buffer, use the `ip urlfilter max-resp-pak` command in global configuration mode. To return to the default, use the `no` form of this command.

```
ip urlfilter max-resp-pak number [vrf vrf-name]
no ip urlfilter max-resp-pak number
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Maximum number of HTTP responses that can be stored in the packet buffer of the firewall. After the maximum number has been reached, the firewall will drop further responses. The default, and absolute maximum, value is 200.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Sets the maximum number of HTTP responses only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>200 HTTP responses</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Global configuration</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.2(11)YU</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td></td>
<td>12.3(14)T</td>
<td>The <code>vrf vrf-name</code> keyword and argument pair was added.</td>
</tr>
</tbody>
</table>

| Usage Guidelines | When an HTTP request arrives at a Cisco IOS firewall, the firewall forwards the request to the web server while simultaneously sending a URL look-up request to the vendor server (Websense or N2H2). If the vendor server reply arrives before the HTTP response, the firewall will know whether to permit or block the HTTP response; if the HTTP response arrives before the vendor server reply, the firewall will not know whether to allow or block the response, so the firewall will drop the response until it hears from the vendor server. The `ip urlfilter max-resp-pak` command allows you to configure your firewall to store the HTTP responses in a buffer, which allows your firewall to store a maximum of 200 HTTP responses. Each response will remain in the buffer until an allow or deny message is received from the vendor server. If the vendor server reply allows the URL, the firewall will release the HTTP response from the buffer to the end user; if the vendor server reply denies the URL, the firewall will discard the HTTP response from the buffer and close the connection to both ends. |

<table>
<thead>
<tr>
<th>Examples</th>
<th>The following example shows how to configure your firewall to hold 150 HTTP responses:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ip urlfilter max-resp-pak 150</code></td>
</tr>
</tbody>
</table>
ip urlfilter server vendor

Effective with Cisco IOS Release 15.4(3)M, the **ip urlfilter server vendor** command is not available in Cisco IOS software.

To configure a vendor server for URL filtering, use the **ip urlfilter server vendor** command in global configuration mode. To remove a server from your configuration, use the **no** form of this command.

```
ip urlfilter server vendor {websense|n2h2} ip-address [port port-number] [timeout seconds] [retransmit number] [outside] [vrf vrf-name]
oip urlfilter server vendor {websense|n2h2} ip-address [port port-number] [timeout seconds] [retransmit number] [outside]
```

### Syntax Description

- **websense**
  - Websense server will be used.
- **n2h2**
  - N2H2 server will be used.
- **ip-address**
  - IP address of the vendor server.
- **port port-number**
  - (Optional) Port number that the vendor server listens on. The default port number is 15868.
- **timeout seconds**
  - (Optional) Length of time, in seconds, that the Cisco IOS firewall will wait for a response from the vendor server. The default timeout is 5 seconds.
- **retransmit number**
  - (Optional) Number of times the Cisco IOS firewall will retransmit the request when a response does not arrive for the request. The default value is two times.
- **outside**
  - (Optional) Vendor server will be deployed on the outside network.
- **vrf vrf-name**
  - (Optional) Configures a vendor server for URL filtering only for the specified Virtual Routing and Forwarding (VRF) interface.

### Command Default

A vendor server is not configured.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(11)YU</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.3(2)T</td>
<td>The <strong>outside</strong> keyword was added.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <strong>vrf vrf-name</strong> keyword and argument pair was added.</td>
</tr>
<tr>
<td>15.4(3)M</td>
<td>This command was removed.</td>
</tr>
</tbody>
</table>
Usage Guidelines

Use the `ip urlfilter server vendor` command to configure a Websense or N2H2 server, which will interact with the Cisco IOS Firewall to filter HTTP requests on the basis of a specified policy—global filtering, user- or group-based filtering, keyword-based filtering, category-based filtering, or customized filtering.

If the firewall has not received a response from the vendor server within the time specified in the `timeout seconds` keyword and argument, the firewall will check the `retransmit number` keyword and argument configured for the vendor server. If the firewall has not exceeded the maximum retransmit tries allowed, it will resend the HTTP lookup request. If the firewall has exceeded the maximum retransmit tries allowed, it will delete the outstanding request from the queue and check the status of the allow mode value. The firewall will forward the request if the allow mode is on; otherwise, it will drop the request.

By default, URL lookup requests that are made to the vendor server contain non-natted client IP addresses because the vendor server is deployed on the inside network. The `outside` keyword allows the vendor server to be deployed on the outside network, thereby, allowing Cisco IOS software to send the natted IP address of the client in the URL lookup request.

Primary and Secondary Servers

When users configure multiple vendor servers, the firewall will use only one server at a time—the primary server; all other servers are called secondary servers. When the primary server becomes unavailable for any reason, it becomes a secondary server and one of the secondary servers becomes the primary server.

A firewall marks a primary server as down when sending a request to or receiving a response from the server fails. When a primary server goes down, the system will go to the beginning of the configured servers list and try to activate the first server on the list. If the first server on the list is unavailable, it will try the second server on the list; the system will keep trying to activate a server until it is successful or until it reaches the end of the server list. If the system reaches the end of the server list, it will set a flag indicating that all of the servers are down, and it will enter allow mode.

Examples

The following example shows how to configure the Websense server for URL filtering:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 192.168.3.1
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip urlfilter allowmode</td>
<td>Turns on the default mode (allow mode) of the filtering algorithm.</td>
</tr>
<tr>
<td>ip urlfilter max-request</td>
<td>Sets the maximum number of outstanding requests that can exist at any given time.</td>
</tr>
</tbody>
</table>
**ip urlfilter source-interface**

To allow the URL filter to specify the interface whose IP address is used as the source IP address while a TCP connection is made to the URL filter server (Websense or N2H2), use the `ip urlfilter source-interface` command in global configuration mode. To disable the option, use the `no` form of this command.

```
ip urlfilter source-interface interface-type [vrf vrf-name]
no ip urlfilter source-interface [vrf vrf-name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface-type</code></td>
<td>The interface type that is used as the source IP address.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Specifies the Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

The URL filter to specify a source interface for TCP is not defined.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ip urlfilter source-interface` command is used to define the source interface from which the URL filter request is sent. This command is recommended to be configured if the URL filter server can only be routed through certain interfaces on the router.

**Examples**

The following example shows that the URL filtering server is routed to the Ethernet interface type:

```
Router(config)# ip urlfilter source-interface ethernet
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ip urlfilter</code></td>
<td>Enables debug information of URL filter subsystems.</td>
</tr>
</tbody>
</table>
ip urlfilter truncate

To allow the URL filter to truncate long URLs to the server, use the **ip urlfilter truncate** command in global configuration mode. To disable the truncating option, use the **no** form of this command.

```
ip urlfilter truncate {script-parameters|hostname} [vrf vrf-name]
no ip urlfilter truncate {script-parameters|hostname} [vrf vrf-name]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>script-parameters</td>
<td>Specifies that only the URL up to the script options is sent.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies that only the hostname is sent.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies the Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

URLs that are longer than the maximum supported length are not truncated, and the HTTP request is rejected.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If both the **script-parameters** and **hostname** keywords are configured, the **script-parameters** keyword takes precedence over the **hostname** keyword. If both the keywords are configured and the script parameters URL is truncated and the maximum supported URL length is exceeded, the URL is truncated up to the hostname.

**Note**

If both **script-parameters** and **hostname** keywords are configured, they must be on separate lines as shown in the “Examples” section. They cannot be combined in one line.

**Examples**

The following example shows that the URL is to be truncated up to the script options:

```
ip urlfilter truncate script-parameters
```

The following example shows that the URL is to be truncated up to the hostname:

```
ip urlfilter truncate hostname
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>debug ip urlfilter</td>
<td>Enables debug information of URL filter subsystems.</td>
</tr>
</tbody>
</table>
ip urlfilter urlf-server-log

Effective with Cisco IOS Release 15.4(3)M, the `ip urlfilter urlf-server-log` command is not available in Cisco IOS software.

To enable the logging of system messages on the URL filtering server, use the `ip urlfilter urlf-server-log` command in global configuration mode. To disable the logging of system messages, use the `no` form of this command.

```
ip urlfilter urlf-server-log [vrf vrf-name]
o  ip urlfilter urlf-server-log
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Enables the logging of system messages on the URL filtering server only for the specified Virtual Routing and Forwarding (VRF) interface.</td>
</tr>
</tbody>
</table>

**Command Default**

This command is disabled.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(11)YU</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
<tr>
<td>12.3(14)T</td>
<td>The <code>vrf vrf-name</code> keyword and argument pair was added.</td>
</tr>
<tr>
<td>15.4(3)M</td>
<td>This command was removed.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ip urlfilter urlf-server-log` command to enable Cisco IOS to send a log request immediately after the URL lookup request. The firewall will not make a URL lookup request if the destination IP address is in the cache, but it will still make a log request to the server. (The log request contains the URL, hostname, source IP address, and the destination IP address.) The server records the log request into its own log server so you can view this information as necessary.

**Examples**

The following example shows how to enable system message logging on the URL filter server:

```
ip urlfilter urlf-server-log
```
ip verify drop-rate compute interval

To configure the interval of time between Unicast Reverse Path Forwarding (RPF) drop rate computations, use the `ip verify drop-rate compute interval` command in global configuration mode. To reset the interval to the default value, use the `no` form of this command.

`ip verify drop-rate compute interval seconds`
`no ip verify drop-rate compute interval`

**Syntax Description**

| `seconds` | Interval, in seconds, between Unicast RPF drop rate computations. The range is from 30 to 300. The default is 30. |

**Command Default**
The drop rate is not computed.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(31)SB2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
<tr>
<td>12.2(33)SX12</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SX12.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The configured value applies for the computation of all Unicast RPF drop rates (global and per interface).

The value for the compute interval must be less than or equal to the value configured using the `ip verify drop-rate compute window` command. If you configure the `no` form of the `ip verify drop-rate compute interval` command while the `ipUrpfDropRateWindow` value is configured to be less than the default compute interval value, the following message appears on the console:

"urpf drop rate window < interval"

This error message means the command was not executed. The compute interval remains at the configured value rather than changing to the default value.

**Examples**
The following example shows how to configure a compute interval of 45 seconds:

Router> enable
Router# configure terminal
Router(config)# ip verify drop-rate compute interval 45

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip verify drop-rate compute window</code></td>
<td>Configures the interval of time during which the Unicast RPF drop count is collected for the drop rate computation.</td>
</tr>
</tbody>
</table>
### Command Reference: Commands D to L

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip verify drop-rate notify hold-down</code></td>
<td>Configures the minimum time between Unicast RPF drop rate notifications.</td>
</tr>
<tr>
<td><code>ip verify unicast notification threshold</code></td>
<td>Configures the threshold value used to determine whether to send a Unicast RPF drop rate notification.</td>
</tr>
</tbody>
</table>
ip verify drop-rate compute window

To configure the interval of time during which the Unicast Reverse Path Forwarding (RPF) drop count is collected for the drop rate computation, use the `ip verify drop-rate compute window` command in global configuration mode. To reset the window to the default value, use the `no` form of this command.

```
ip verify drop-rate compute window seconds
no ip verify drop-rate compute window
```

**Syntax Description**

| seconds | Interval, in seconds, during which the Unicast RPF drop count is accumulated for the drop rate computation. The range is from 30 to 300. The default is 300. |

**Command Default**

The drop rate is not calculated.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(31)SB2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
<tr>
<td>12.2(33)SXI2</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI2.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command configures the sliding window that begins the configured number of seconds prior to the computation and ends with the Unicast RPF drop rate computation. The configured value applies for the computation of all Unicast RPF drop rates (global and per interface).

The value configured for the "compute window" must be greater than or equal to the value configured using the `ip verify drop-rate compute interval` command. If you configure the `no` form of the `ip verify drop-rate compute window` command while the cipUrpfDropRateInterval value is configured to be greater than the default compute window value, the following message appears on the console:

```
"urpf drop rate window < interval"
```

This error message means that the command was not executed. The compute window remains at the configured value rather than changing to the default value.

**Examples**

The following example shows how to configure a compute window of 60 seconds:

```
Router> enable
Router# configure terminal
Router(config)# ip verify drop-rate compute window 60
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip verify drop-rate compute interval</td>
<td>Configures the interval between Unicast RPF drop rate computations.</td>
</tr>
<tr>
<td>ip verify drop-rate notify hold-down</td>
<td>Configures the minimum time between Unicast RPF drop rate notifications.</td>
</tr>
<tr>
<td>ip verify unicast notification threshold</td>
<td>Configures the threshold value used to determine whether to send a Unicast RPF drop rate notification.</td>
</tr>
</tbody>
</table>

**Related Commands**

- **ip source-track through ivrf**
- **ip verify drop-rate compute window**
**ip verify drop-rate notify hold-down**

To configure the minimum time between Unicast Reverse Path Forwarding (RPF) drop rate notifications, use the `ip verify drop-rate notify hold-down` command in global configuration mode. To reset the hold-down time to the default value, use the `no` form of this command.

```
ip verify drop-rate notify hold-down seconds
no ip verify drop-rate notify hold-down
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Minimum time, in seconds, between Unicast RPF drop rate notifications. The range is from 30 to 300. The default is 300.</td>
</tr>
</tbody>
</table>

**Command Default**

No notifications are sent.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(31)SB2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
<tr>
<td>12.2(33)SXI2</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI2.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The configured value applies for the computation of all Unicast RPF drop rates (global and per interface).

**Examples**

The following example shows how to configure a notify hold-down time of 40 seconds:

```
Router> enable
Router# configure terminal
Router(config)# ip verify drop-rate notify hold-down 40
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip verify drop-rate compute interval</strong></td>
<td>Configures the interval of time between Unicast RPF drop rate computations.</td>
</tr>
<tr>
<td><strong>ip verify drop-rate compute window</strong></td>
<td>Configures the interval of time over which the Unicast RPF drop count used in the drop rate computation is collected.</td>
</tr>
<tr>
<td><strong>ip verify unicast notification threshold</strong></td>
<td>Configures the threshold value used to determine whether to send a Unicast RPF drop rate notification.</td>
</tr>
</tbody>
</table>
ip verify unicast notification threshold

To configure the threshold value used to determine whether to send a Unicast Reverse Path Forwarding (RPF) drop rate notification, use the `ip verify unicast notification threshold` command in interface configuration mode. To set the notification threshold back to the default value, use the `no` form of this command.

```
ip verify unicast notification threshold packets-per-second
no ip verify unicast notification threshold
```

**Syntax Description**

- **packets-per-second**: Threshold value, in packets per second, used to determine whether to send a Unicast RPF drop rate notification. The range is from 0 to 4294967295. The default is 1000.

**Command Default**

No notifications are sent.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(31)SB2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
<tr>
<td>12.2(33)SXI2</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI2.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command configures the threshold Unicast RPF drop rate which, when exceeded, triggers a notification. Configuring a value of 0 means that any Unicast RPF packet drop triggers a notification.

**Examples**

The following example shows how to configure a notification threshold value of 900 on Ethernet interface 3/0:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 3/0
Router(config-if)# ip verify unicast notification threshold 900
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip verify drop-rate compute interval</td>
<td>Configures the interval of time between Unicast RPF drop rate computations.</td>
</tr>
<tr>
<td>ip verify drop-rate compute window</td>
<td>Configures the interval of time during which the Unicast RPF drop count is collected for the drop rate computation.</td>
</tr>
<tr>
<td>ip verify drop-rate notify hold-down</td>
<td>Configures the minimum time between Unicast RPF drop rate notifications.</td>
</tr>
</tbody>
</table>
ip verify unicast reverse-path

This command was replaced by the `ip verify unicast source reachable-via` command effective with Cisco IOS Release 12.0(15)S. The `ip verify unicast source reachable-via` command allows for more flexibility and functionality, such as supporting asymmetric routing, and should be used for any Reverse Path Forward implementation. The `ip verify unicast reverse-path` command is still supported.

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the `ip verify unicast reverse-path` command in interface configuration mode. To disable Unicast RPF, use the `no` form of this command.

```
no ip verify unicast reverse-path [list]
```

### Syntax Description

```
list  (Optional) Specifies a numbered access control list (ACL) in the following ranges:

- 1 to 99 (IP standard access list)
- 100 to 199 (IP extended access list)
- 1300 to 1999 (IP standard access list, expanded range)
- 2000 to 2699 (IP extended access list, expanded range)
```

### Command Default

Unicast RPF is disabled.

### Command Modes

Interface configuration (config-if)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1(CC)</td>
<td>This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3</td>
</tr>
<tr>
<td>12.0</td>
<td>Added ACL support using the <code>list</code> argument. Added per-interface statistics on dropped or suppressed packets.</td>
</tr>
<tr>
<td>12.0(15)S</td>
<td>The <code>ip verify unicast source reachable-via</code> command replaced this command, and the following keywords were added to the <code>ip verify unicast source reachable-via</code> command: <code>allow-default</code>, <code>allow-self-ping</code>, <code>rx</code>, and <code>any</code>.</td>
</tr>
<tr>
<td>12.1(8a)E</td>
<td>The <code>ip verify unicast reverse-path</code> command was integrated into Cisco IOS Release 12.1(8a)E.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>The <code>ip verify unicast reverse-path</code> command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
</tbody>
</table>
The `ip verify unicast reverse-path` command was integrated into Cisco IOS Release 12.2(14)SX.

The `ip verify unicast reverse-path` command was integrated into Cisco IOS Release 12.2(33)SRA.

**Usage Guidelines**

Use the `ip verify unicast reverse-path interface` command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that are received by a router. Malformed or forged source addresses can indicate denial of service (DoS) attacks on the basis of source IP address spoofing.

When Unicast RPF is enabled on an interface, the router examines all packets that are received on that interface. The router checks to ensure that the source address appears in the Forwarding Information Base (FIB) and that it matches the interface on which the packet was received. This "look backwards" ability is available only when Cisco Express Forwarding is enabled on the router because the lookup relies on the presence of the FIB. Cisco Express Forwarding generates the FIB as part of its operation.

To use Unicast RPF, enable Cisco Express Forwarding switching or distributed Cisco Express Forwarding switching in the router. There is no need to configure the input interface for Cisco Express Forwarding switching. As long as Cisco Express Forwarding is running on the router, individual interfaces can be configured with other switching modes.

---

**Note**

It is very important for Cisco Express Forwarding to be configured globally in the router. Unicast RPF will not work without Cisco Express Forwarding.

---

**Note**

Unicast RPF is an input function and is applied on the interface of a router only in the ingress direction.

The Unicast Reverse Path Forwarding feature checks to determine whether any packet that is received at a router interface arrives on one of the best return paths to the source of the packet. The feature does this by doing a reverse lookup in the Cisco Express Forwarding table. If Unicast RPF does not find a reverse path for the packet, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast Reverse Path Forwarding command. If an ACL is specified in the command, then when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a `deny` statement in the ACL) or forwarded (using a `permit` statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the Unicast Reverse Path Forwarding command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries used by the Unicast Reverse Path Forwarding command. Log information can be used to gather information about the attack, such as source address, time, and so on.

**Where to Use RPF in Your Network**

Unicast RPF may be used on interfaces in which only one path allows packets from valid source networks (networks contained in the FIB). Unicast RPF may also be used in cases for which a router has multiple paths...
to a given network, as long as the valid networks are switched via the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an Internet service provider (ISP) are likely to have symmetrical reverse paths. Unicast RPF may still be applicable in certain multi-homed situations, provided that optional Border Gateway Protocol (BGP) attributes such as weight and local preference are used to achieve symmetric routing.

With Unicast RPF, all equal-cost "best" return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

For example, routers at the edge of the network of an ISP are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network. Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. In this scenario, you should use the new form of the command, `ip verify unicast source reachable-via`, if there is a chance of asymmetrical routing.

**Examples**

The following example shows that the Unicast Reverse Path Forwarding feature has been enabled on a serial interface:

```bash
ip cef
! or "ip cef distributed" for RSP+VIP based routers
! interface serial 5/0/0
  ip verify unicast reverse-path
```

The following example uses a very simple single-homed ISP to demonstrate the concepts of ingress and egress filters used in conjunction with Unicast RPF. The example illustrates an ISP-allocated classless interdomain routing (CIDR) block 192.168.202.128/28 that has both inbound and outbound filters on the upstream interface. Be aware that ISPs are usually not single-homed. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) need to be designed into the filters on the border routers of the ISP.

```bash
ip cef distributed
!
interface Serial 5/0/0
description Connection to Upstream ISP
ip address 192.168.200.225 255.255.255.255
no ip redirects
no ip directed-broadcast
no ip proxy-arp
ip verify unicast reverse-path
ip access-group 111 in
ip access-group 110 out
!
access-list 110 permit ip 192.168.202.128 10.0.0.31 any
access-list 110 deny ip any any log
access-list 111 deny ip host 10.0.0.0 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 10.0.0.0 255.255.255.255 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 192.168.0.0 255.255.255.255 any log
access-list 111 deny ip 209.165.202.129 10.0.0.31 any log
access-list 111 permit ip any any
```
The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on Ethernet interface 0 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at Ethernet interface 0 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 192.168.201.100 arriving at Ethernet interface 0 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
  ip address 192.168.200.1 255.255.255.255
  ip verify unicast reverse-path 197
!
int eth0/1/2
  ip address 192.168.201.1 255.255.255.255
!
access-list 197 deny ip 192.168.201.0 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 10.0.0.63 any log-input
access-list 197 deny ip 192.168.201.128 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 10.0.0.63 any log-input
access-list 197 deny ip host 10.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 255.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 192.168.0.0 255.255.255.255 any log-input
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip cef</code></td>
<td>Enables Cisco Express Forwarding on the route processor card.</td>
</tr>
</tbody>
</table>
**ip verify unicast source reachable-via**

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the `ip verify unicast source reachable-via` command in interface configuration mode. To disable Unicast RPF, use the `no` form of this command.

```
ip verify unicast source reachable-via {any|rx [l2-src]} [allow-default] [allow-self-ping] [access-list]  
no ip verify unicast source reachable-via
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>Examines incoming packets to determine whether the source address is in the Forwarding Information Base (FIB) and permits the packet if the source is reachable through any interface (sometimes referred to as loose mode).</td>
</tr>
<tr>
<td>rx</td>
<td>Examines incoming packets to determine whether the source address is in the FIB and permits the packet only if the source is reachable through the interface on which the packet was received (sometimes referred to as strict mode).</td>
</tr>
<tr>
<td>l2-src</td>
<td>(Optional) Enables source IPv4 and source MAC address binding.</td>
</tr>
<tr>
<td>allow-default</td>
<td>(Optional) Allows the use of the default route for RPF verification.</td>
</tr>
<tr>
<td>allow-self-ping</td>
<td>(Optional) Allows a router to ping its own interface or interfaces.</td>
</tr>
<tr>
<td>Caution</td>
<td>Use caution when enabling the <code>allow-self-ping</code> keyword. This keyword opens a denial-of-service (DoS) hole.</td>
</tr>
<tr>
<td>access-list</td>
<td>(Optional) Specifies a numbered access control list (ACL) in the following ranges:</td>
</tr>
<tr>
<td></td>
<td>• 1 to 99 (IP standard access list)</td>
</tr>
<tr>
<td></td>
<td>• 100 to 199 (IP extended access list)</td>
</tr>
<tr>
<td></td>
<td>• 1300 to 1999 (IP standard access list, expanded range)</td>
</tr>
<tr>
<td></td>
<td>• 2000 to 2699 (IP extended access list, expanded range)</td>
</tr>
</tbody>
</table>

**Command Default**

Unicast RPF is disabled.

Source IPv4 and source MAC address binding is disabled.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1(CC), 12.0</td>
<td>This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3.</td>
</tr>
<tr>
<td>12.1(2)T</td>
<td>Added access control list (ACL) support using the <code>access-list</code> argument. Added per-interface statistics on dropped or suppressed packets.</td>
</tr>
<tr>
<td>12.0(15)S</td>
<td>This command replaced the <code>ip verify unicast reverse-path</code> command, and the following keywords were added: <code>allow-default</code>, <code>allow-self-ping</code>, <code>rx</code>, and <code>any</code>.</td>
</tr>
</tbody>
</table>
## Usage Guidelines

Use the **ip verify unicast source reachable-via** interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate DoS attacks based on source IP address spoofing.

To use Unicast RPF, enable Cisco Express Forwarding or distributed Cisco Express Forwarding in the router. There is no need to configure the input interface for Cisco Express Forwarding. As long as Cisco Express Forwarding is running on the router, individual interfaces can be configured with other switching modes.

### Note

It is important for Cisco Express Forwarding to be configured globally on the router. Unicast RPF does not work without Cisco Express Forwarding.

### Note

Unicast RPF is an input function and is applied on the interface of a router only in the ingress direction.

When Unicast RPF is enabled on an interface, the router examines all packets that are received on that interface. The router checks to make sure that the source address appears in the FIB. If the **rx** keyword is selected, the source address must match the interface on which the packet was received. If the **any** keyword is selected, the source address must be present only in the FIB. This ability to “look backwards” is available only when Cisco Express Forwarding is enabled on the router because the lookup relies on the presence of the FIB. Cisco Express Forwarding generates the FIB as part of its operation.

### Note

If the source address of an incoming packet is resolved to a null adjacency, the packet will be dropped. The null interface is treated as an invalid interface by the new form of the Unicast RPF command. The older form of the command syntax did not exhibit this behavior.

Unicast RPF checks to determine whether any packet that is received at a router interface arrives on one of the best return paths to the source of the packet. If a reverse path for the packet is not found, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast RPF command. If an ACL is specified in the command, when (and only when) a packet fails the Unicast RPF check, the ACL is

### Release and Modification History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(8a)E</td>
<td>This command was integrated into Cisco IOS Release 12.1(8a)E.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(14)SX</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command was introduced on the Supervisor Engine 2.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was modified. The <strong>l2-src</strong> keyword was added to support the source IPv4 and source MAC address binding feature on platforms that support the Cisco Express Forwarding software switching path.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was integrated into Cisco IOS Release 15.0(1)M.</td>
</tr>
</tbody>
</table>
checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the `ip verify unicast source reachable-via` command, the router drops the forged or malformed packet immediately, and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries that are used by the `ip verify unicast source reachable-via` command. Log information can be used to gather information about the attack, such as source address, time, and so on.

**Strict Mode RPF**

If the source address is in the FIB and reachable only through the interface on which the packet was received, the packet is passed. The syntax for this method is `ip verify unicast source reachable-via rx`.

**Exists-Only (or Loose Mode) RPF**

If the source address is in the FIB and reachable through any interface on the router, the packet is passed. The syntax for this method is `ip verify unicast source reachable-via any`.

Because this Unicast RPF option passes packets regardless of which interface the packet enters, it is often used on Internet service provider (ISP) routers that are “peered” with other ISP routers (where asymmetrical routing typically occurs). Packets using source addresses that have not been allocated on the Internet, which are often used for spoofed source addresses, are dropped by this Unicast RPF option. All other packets that have an entry in the FIB are passed.

**allow-default**

Normally, sources found in the FIB but only by way of the default route will be dropped. Specifying the `allow-default` keyword option will override this behavior. You must specify the `allow-default` keyword in the command to permit Unicast RPF to successfully match on prefixes that are known through the default route to pass these packets.

**allow-self-ping**

This keyword allows the router to ping its own interface or interfaces. By default, when Unicast RPF is enabled, packets that are generated by the router and destined to the router are dropped, thereby, making certain troubleshooting and management tasks difficult to accomplish. Issue the `allow-self-ping` keyword to enable self-pinging.

---

**Caution**

Caution should be used when enabling the `allow-self-ping` keyword because this option opens a potential DoS hole.

**Using RPF in Your Network**

Use Unicast RPF strict mode on interfaces where only one path allows packets from valid source networks (networks contained in the FIB). Also, use Unicast RPF strict mode when a router has multiple paths to a given network, as long as the valid networks are switched through the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an ISP are likely to have symmetrical reverse paths. Unicast RPF strict mode is applicable in certain multihomed situations, provided that optional Border Gateway Protocol (BGP) attributes, such as weight and local preference, are used to achieve symmetric routing.
With Unicast RPF, all equal-cost “best” return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

Use Unicast RPF loose mode on interfaces where asymmetric paths allow packets from valid source networks (networks contained in the FIB). Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router.

**IP and MAC Address Spoof Prevention**

In Release 15.0(1)M and later, you can use the `l2-src` keyword to enable source IPv4 and source MAC address binding. To disable source IPv4 and source MAC address binding, use the `no` form of the `ip verify unicast source reachable-via` command.

If an inbound packet fails this security check, it will be dropped and the Unicast RPF dropped-packet counter will be incremented. The only exception occurs if a numbered access control list has been specified as part of the Unicast RPF command in strict mode, and the ACL permits the packet. In this case the packet will be forwarded and the Unicast RPF suppressed-drops counter will be incremented.

The `l2-src` keyword cannot be used with the loose uRPF command, `ip verify unicast source reachable-via any` command.

Not all platforms support the `l2-src` keyword. Therefore, not all the possible keyword combinations for strict Unicast RPF in the following list will apply to your platform:

Possible keyword combinations for strict Unicast RPF include the following:

- `allow-default`
- `allow-self-ping`
- `12-src`<br>  `<ACL-number>`
- `allow-default allow-self-ping 12-src`<br>  `<ACL-number>`
- `allow-self-ping 12-src`<br>  `<ACL-number>`
- `12-src allow-self-ping`<br>  `<ACL-number>`
- `allow-default allow-self-ping 12-src`<br>  `<ACL-number>`
- `allow-default allow-self-ping`<br>  `<ACL-number>`
- `allow-default 12-src`<br>  `<ACL-number>`
- `allow-self-ping 12-src`<br>  `<ACL-number>`
- `allow-default allow-self-ping`<br>  `<ACL-number>`
- `allow-default 12-src`<br>  `<ACL-number>`
- `allow-self-ping 12-src`<br>  `<ACL-number>`
- `allow-default allow-self-ping 12-src`<br>  `<ACL-number>`

**Examples**

**Single-Homed ISP Connection with Unicast RPF**

The following example uses a very simple single-homed ISP connection to demonstrate the concept of Unicast RPF. In this example, an ISP peering router is connected through a single serial interface
to one upstream ISP. Hence, traffic flows into and out of the ISP will be symmetric. Because traffic flows will be symmetric, a Unicast RPF strict-mode deployment can be configured.

```
ip cef
! or “ip cef distributed” for Route Switch Processor+Versatile Interface Processor-(RSP+VIP-) based routers.
!
interface Serial5/0/0
 description - link to upstream ISP (single-homed)
ip address 192.168.200.225 255.255.255.252
no ip redirects
no ip directed-broadcasts
no ip proxy-arp
ip verify unicast source reachable-via
```

### ACLs and Logging with Unicast RPF

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0/1 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at interface Ethernet 0/1 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 192.168.201.100 arriving at interface Ethernet 0/1 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.0
 ip verify unicast source reachable-via rx 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.0
!
access-list 197 deny ip 192.168.201.0 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 0.0.0.63 any log-input
access-list 197 deny ip 192.168.201.128 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input
access-list 197 deny ip host 0.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 0.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 0.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 0.15.255.255 any log-input
access-list 197 deny ip 192.168.0.0 0.0.255.255 any log-input
```

### MAC Address Binding on Software Switching Platforms Like the Cisco 7200 Series Routers

The following example shows how to enable source IPv4 and source MAC address binding on Ethernet 0/0:

```
Router# configure terminal
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# ip verify unicast source reachable-via rx 12-src
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip cef</td>
<td>Enables Cisco Express Forwarding on the route processor card.</td>
</tr>
<tr>
<td>ip cef distributed</td>
<td>Enables Cisco Express Forwarding on the line card.</td>
</tr>
</tbody>
</table>
ip virtual-reassembly

To enable virtual fragment reassembly (VFR) on an interface, use the `ip virtual-reassembly` command in interface configuration mode. To disable VFR on an interface, use the `no` form of this command.

```
ip virtual-reassembly [max-reassemblies number] [max-fragments number] [timeout seconds] [drop-fragments]
oip virtual-reassembly [max-reassemblies number] [max-fragments number] [timeout seconds] [drop-fragments]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>max-reassemblies number</code></td>
<td>(Optional) Maximum number of IP datagrams that can be reassembled at any given time. Default value: 16. If the maximum value is reached, all fragments within the following fragment set is dropped and an alert message is logged to the syslog server.</td>
</tr>
<tr>
<td><code>max-fragments number</code></td>
<td>(Optional) Maximum number of fragments that are allowed per IP datagram (fragment set). Default value: 32. If an IP datagram that is being reassembled receives more than the maximum allowed fragments, the IP datagram is dropped and an alert message is logged to the syslog server.</td>
</tr>
<tr>
<td><code>timeout seconds</code></td>
<td>(Optional) Timeout value, from 0 to 60 seconds, for an IP datagram that is being reassembled. Default value: 3 seconds. If an IP datagram does not receive all of the fragments within the specified time, the IP datagram (and all of its fragments) are dropped.</td>
</tr>
<tr>
<td><code>drop-fragments</code></td>
<td>(Optional) Enables the VFR to drop all fragments that arrive on the configured interface. By default, this function is disabled.</td>
</tr>
</tbody>
</table>

### Command Default

VFR is not enabled.

### Command Modes

Interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>IOS XE 3.2S</td>
<td>This command was introduced in Cisco IOS XE Release 3.2S.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

A buffer overflow attack can occur when an attacker continuously sends a large number of incomplete IP fragments, causing the firewall to lose time and memory while trying to reassemble the fake packets.

The `max-reassemblies number` option and the `max-fragments number` option allow you to configure maximum threshold values to avoid a buffer overflow attack and to control memory usage.

In addition to configuring the maximum threshold values, each IP datagram is associated with a managed timer. If the IP datagram does not receive all of the fragments within the specified time (which can be configured through the `timeout seconds` option), the timer expires and the IP datagram (and all of its fragments) is dropped.
If you are upgrading to Cisco IOS XE Release 3.4 or later and the configured timeout was set to more than 60 seconds, then your configured timeout value is cleared and reset to the default value of 3 seconds.

Automatically Enabling or Disabling VFR

VFR is designed to work with any feature that requires fragment reassembly (such as Cisco IOS Firewall and NAT). Currently, NAT enables and disables VFR internally; that is, when NAT is enabled on an interface, VFR is automatically enabled on that interface.

If more than one feature attempts to automatically enable VFR on an interface, then the VFR maintains a reference count to keep track of the number of features that have enabled VFR. When the reference count is reduced to zero, VFR is automatically disabled.

Examples

The following example shows how to configure VFR on interfaces ethernet2/1, ethernet2/2, and serial3/0 to facilitate the firewall that is enabled in the outbound direction on interface serial3/0. In this example, the firewall rules that specify the list of LAN1 and LAN2 originating protocols (FTP, HTTP and SMTP) are to be inspected.

```
ip inspect name INTERNET-FW ftp
ip inspect name INTERNET-FW http
ip inspect name INTERNET-FW smtp!

interface Loopback0
  ip address 10.0.1.1 255.255.255.255

interface Ethernet2/0
  ip address 10.4.21.9 255.255.0.0
  no ip proxy-arp
  no ip mroute-cache
duplex half
  no cdp enable
!
interface Ethernet2/1
  description LAN1
  ip address 10.4.0.2 255.255.255.0
  ip virtual-reassembly
duplex half
!
interface Ethernet2/2
  description LAN2
  ip address 10.15.0.2 255.255.255.0
  ip virtual-reassembly
duplex half
!
interface Ethernet2/3
  no ip address
  no ip mroute-cache
  shutdown
duplex half
!
interface Serial3/0
  description Internet
  ip unnumbered Loopback0
  encapsulation ppp
  ip access-group 102 in
  ip inspect INTERNET-FW out
```
### ip virtual-reassembly

```
ip virtual-reassembly
serial restart-delay 0
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip virtual-reassembly</code></td>
<td>Displays the configuration and statistical information of the VFR on a given interface.</td>
</tr>
</tbody>
</table>
ip virtual-reassembly-out

To enable virtual fragment reassembly (VFR) on outbound interface traffic after it was disabled by the `no ip virtual-reassembly` command, use the `ip virtual-reassembly-out` command in interface configuration mode. To disable VFR on outbound interface traffic, use the `no` form of this command.

```
ip virtual-reassembly-out [max-reassemblies number] [max-fragments number] [timeout seconds] [drop-fragments]
no ip virtual-reassembly-out [max-reassemblies number] [max-fragments number] [timeout seconds] [drop-fragments]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>max-reassemblies number</code></td>
<td>(Optional) Specifies the maximum number of IP datagrams that can be reassembled at any given time. Default value: 16. If the maximum value is reached, all fragments within the following fragment set will be dropped and an alert message will be logged to the syslog server.</td>
</tr>
<tr>
<td><code>max-fragments number</code></td>
<td>(Optional) Specifies the maximum number of fragments that are allowed per IP datagram (fragment set). Default value: 32. If an IP datagram that is being reassembled receives more than the maximum number of allowed fragments, the IP datagram will be dropped and an alert message will be logged to the syslog server.</td>
</tr>
<tr>
<td><code>timeout seconds</code></td>
<td>(Optional) Specifies the timeout value, in seconds, for an IP datagram that is being reassembled. Default value: 3. If an IP datagram does not receive all of the fragments within the specified time, the IP datagram (and all of its fragments) will be dropped.</td>
</tr>
<tr>
<td><code>drop-fragments</code></td>
<td>(Optional) Enables the VFR to drop all fragments that arrive on the configured interface. By default, this function is disabled.</td>
</tr>
</tbody>
</table>

**Command Default**
VFR on outbound interface traffic is not enabled.

**Command Modes**
Interface configuration (config-if)

**Command History**
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release XE 3.2S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
You can use this command to reenable VFR on outbound interface traffic after it was disabled by the `no ip virtual-reassembly` command. If VFR is enabled on both inbound and outbound interface traffic, you can use the `no ip virtual-reassembly-out` command to disable it on only the outbound interface traffic.

**Examples**
The following example shows how to manually enable VFR on outbound traffic on interfaces GigabitEthernet0/0/1, GigabitEthernet0/0/0.773, and Serial 3/0:

```
interface Loopback 0
```
ip address 10.0.1.1 255.255.255.255
!
interface GigabitEthernet0/0/1
description LAN1
ip address 10.4.0.2 255.255.255.0
ip virtual-reassembly-out
!
interface GigabitEthernet0/0/0.773
encapsulation dot1Q 773
description LAN2
ip address 10.15.0.2 255.255.255.0
ip virtual-reassembly-out
!
interface Serial 3/0
description Internet
ip unnumbered Loopback0
encapsulation ppp
ip virtual-reassembly-out
serial restart-delay 0

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip virtual-reassembly</td>
<td>Enables VFR on an interface.</td>
</tr>
<tr>
<td>show ip virtual-reassembly</td>
<td>Displays the configuration and statistical information of the VFR on a given interface.</td>
</tr>
</tbody>
</table>
**ip vrf**

To define a VPN routing and forwarding (VRF) instance and to enter VRF configuration mode, use the `ip vrf` command in global configuration mode. To remove a VRF instance, use the `no` form of this command.

```
  ip vrf vrf-name
  no ip vrf vrf-name
```

**Syntax Description**

| `vrf-name` | Name assigned to a VRF. |

**Command Default**

No VRFs are defined. No import or export lists are associated with a VRF. No route maps are associated with a VRF.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(5)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(21)ST</td>
<td>This command was integrated into Cisco IOS Release 12.0(21)ST.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(22)S.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS 12.2(14)S.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
<tr>
<td>15.1(1)SY</td>
<td>This command was integrated into Cisco IOS Release 15.1(1)SY.</td>
</tr>
<tr>
<td>Cisco IOS XE 3.3SE</td>
<td>This command was implemented in Cisco IOS XE Release 3.3SE.</td>
</tr>
<tr>
<td>15.4(3)S</td>
<td>This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ip vrf vrf-name` command creates a VRF instance named `vrf-name`. To make the VRF functional, a route distinguisher (RD) must be created using the `rd route-distinguisher` command in VRF configuration mode. The `rd route-distinguisher` command creates the routing and forwarding tables and associates the RD with the VRF instance named `vrf-name`.

The `ip vrf default` command can be used to configure a VRF instance that is a NULL value until a default VRF name can be configured. This is typically before any VRF related AAA commands are configured.

**Examples**

The following example shows how to import a route map to a VRF instance named VPN1:

```
```
Router(config)# ip vrf vpn1
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target both 100:2
Router(config-vrf)# route-target import 100:1

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip vrf forwarding (interface configuration)</td>
<td>Associates a VRF with an interface or subinterface.</td>
</tr>
<tr>
<td>rd</td>
<td>Creates routing and forwarding tables for a VRF and specifies the default route distinguisher for a VPN.</td>
</tr>
</tbody>
</table>
**ip vrf forwarding**

To associate a Virtual Private Network (VPN) routing and forwarding (VRF) instance with a Diameter peer, use the `ip vrf forwarding` command in Diameter peer configuration mode. To enable Diameter peers to use the global (default) routing table, use the no form of this command.

```
ip vrf forwarding name
no ip vrf forwarding name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name assigned to a VRF.</td>
</tr>
</tbody>
</table>

**Command Default**

Diameter peers use the global routing table.

**Command Modes**

Diameter peer configuration (config-dia-peer)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(54)SG</td>
<td>This command was integrated into Cisco IOS Release 12.2(54)SG.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ip vrf forwarding` command to specify a VRF for a Diameter peer. If a VRF name is not configured for a Diameter server, the global routing table will be used.

If the VRF associated with the specified name has not been configured, the command will have no effect and this error message will appear: **No VRF found with the name name**.

**Examples**

The following example shows how to configure the VRF for a Diameter peer:

```
Router (config-dia-peer)# ip vrf forwarding diam_peer_1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diameter peer</td>
<td>Configures a Diameter peer and enters Diameter peer configuration submode.</td>
</tr>
<tr>
<td>ip vrf forwarding (server-group)</td>
<td>Configures the VRF reference of an AAA RADIUS or TACACS+ server group.</td>
</tr>
</tbody>
</table>
ip vrf forwarding (server-group)

To configure the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an authentication, authorization, and accounting (AAA) RADIUS or TACACS+ server group, use the `ip vrf forwarding` command in server-group configuration mode. To enable server groups to use the global (default) routing table, use the no form of this command.

```
ip vrf forwarding vrf-name
no ip vrf forwarding vrf-name
```

**Syntax Description**
- **vrf-name** Name assigned to a VRF.

**Command Default**
Server groups use the global routing table.

**Command Modes**
Server-group configuration (server-group)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)DD</td>
<td>This command was introduced on the Cisco 7200 series and Cisco 7401ASR.</td>
</tr>
<tr>
<td>12.2(4)B</td>
<td>This command was integrated into Cisco IOS Release 12.2(4)B.</td>
</tr>
<tr>
<td>12.2(13)T</td>
<td>This command was integrated into Cisco IOS Release 12.2(13)T.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>Functionality was added for TACACS+ servers.</td>
</tr>
<tr>
<td>12.2(28)SB</td>
<td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td>
</tr>
<tr>
<td>12.2(33)SRA1</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA1.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `ip vrf forwarding` command to specify a VRF for a AAA RADIUS or TACACS+ server group. This command enables dial users to utilize AAA servers in different routing domains.

**Examples**
The following example shows how to configure the VRF user to reference the RADIUS server in a different VRF server group:

```
aaa group server radius sg_global
  server-private 172.16.0.0 timeout 5 retransmit 3
!
```

The following example shows how to configure the VRF user to reference the TACACS+ server in the server group tacacs1:

```
```
aaa group server tacacs+tacacs1
  server-private 10.1.1.1 port 19 key cisco
  ip vrf forwarding cisco
  ip tacacs source-interface Loopback0
  ip vrf cisco
  rd 100:1
  interface Loopback0
  ip address 10.0.0.2 255.0.0.0
  ip vrf forwarding cisco

---

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>aaa group server radius</strong></td>
<td>Groups different RADIUS server hosts into distinct lists and distinct methods.</td>
</tr>
<tr>
<td><strong>ip tacacs source-interface</strong></td>
<td>Uses the IP address of a specified interface for all outgoing TACACS+ packets.</td>
</tr>
<tr>
<td><strong>ip vrf forwarding (server-group)</strong></td>
<td>Configures the VRF reference of an AAA RADIUS or TACACS+ server group.</td>
</tr>
<tr>
<td><strong>server-private</strong></td>
<td>Configures the IP address of the private RADIUS server for the group server.</td>
</tr>
</tbody>
</table>
ip wccp web-cache accelerated

To enable the hardware acceleration for WCCP version 1, use the **ip wccp web-cache accelerated** command in global configuration mode. To disable hardware acceleration, use the **no** form of this command.

```
ip wccp web-cache accelerated
[{{group-address group-address}}][{{redirect-list access-list}}][{{group-list access-list}}][{{password password}}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>group-address</strong> <strong>group-address</strong></td>
<td>(Optional) Directs the router to use a specified multicast IP address for communication with the WCCP service group. See the “Usage Guidelines” section for additional information.</td>
</tr>
<tr>
<td><strong>redirect-list</strong> <strong>access-list</strong></td>
<td>(Optional) Directs the router to use an access list to control traffic that is redirected to this service group. See the “Usage Guidelines” section for additional information.</td>
</tr>
<tr>
<td><strong>group-list</strong> <strong>access-list</strong></td>
<td>(Optional) Directs the router to use an access list to determine which cache engines are allowed to participate in the service group. See the “Usage Guidelines” section for additional information.</td>
</tr>
<tr>
<td><strong>password</strong> <strong>password</strong></td>
<td>(Optional) Specifies a string that directs the router to apply MD5 authentication to messages received from the service group specified by the service name given. See the “Usage Guidelines” section for additional information.</td>
</tr>
</tbody>
</table>

**Command Default**

When this command is not configured, hardware acceleration for WCCPv1 is not enabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.</td>
</tr>
<tr>
<td>12.2(18)SXD1</td>
<td>This command was changed to support the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **group-address** **group-address** option requires a multicast address that is used by the router to determine which cache engine should receive redirected messages. This option instructs the router to use the specified multicast IP address to coalesce the “I See You” responses for the “Here I Am” messages that it has received on this group address. In addition, the response is sent to the group address. The default is for no **group-address** to be configured, so that all “Here I Am” messages are responded to with a unicast reply.

The **redirect-list** **access-list** option instructs the router to use an access list to control the traffic that is redirected to the cache engines of the service group that is specified by the service-name given. The **access-list** argument specifies either a number from 1 to 99 to represent a standard or extended access list number, or a name to represent a named standard or extended access list. The access list itself specifies the traffic that is permitted to be redirected. The default is for no **redirect-list** to be configured (all traffic is redirected).
The **group-list access-list** option instructs the router to use an access list to control the cache engines that are allowed to participate in the specified service group. The **access-list** argument specifies either a number from 1 to 99 to represent a standard access list number, or a name to represent a named standard access list. The access list specifies which cache engines are permitted to participate in the service group. The default is for no **group-list** to be configured, so that all cache engines may participate in the service group.

The password can be up to seven characters. When you designate a password, the messages that are not accepted by the authentication are discarded. The password name is combined with the HMAC MD5 value to create security for the connection between the router and the cache engine.

### Examples

The following example shows how to enable the hardware acceleration for WCCP version 1:

```
Router(config)# ip wccp web-cache accelerated
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip wccp version</strong></td>
<td>Specifies which version of WCCP to configure on your router.</td>
</tr>
</tbody>
</table>
**ips signature update cisco**

To initiate a one-time download of Cisco IOS Intrusion Prevention System (IPS) signatures from Cisco.com, use the `ips signature update cisco` command in Privileged EXEC mode.

```
ips signature update cisco {next|latest|signature} [username name password password]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>next</td>
<td>Specifies the next signature file version from the current signature file on the router.</td>
</tr>
<tr>
<td>latest</td>
<td>Specifies the IOS IPS to search for the latest signature file.</td>
</tr>
<tr>
<td>signature</td>
<td>This argument specifies a specific signature file on Cisco.com.</td>
</tr>
<tr>
<td>username name password</td>
<td>Defines the username for the automatic signature update function.</td>
</tr>
<tr>
<td>password password</td>
<td>Defines the password for the automatic signature update function.</td>
</tr>
</tbody>
</table>

**Command Default**

Privileged EXEC mode (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ips signature update cisco` command is used to initiate a one-time download of IPS signatures from Cisco.com. If you want IPS signatures to be periodically downloaded from Cisco.com, use the `ip ips auto-update` command in global configuration mode and subsequently the `cisco` command in IPS-auto-update configuration mode to enable automatic signature updates from Cisco.com.

If the `username` and `password` is not specified, then the username and password that is specified in the IPS auto update configuration is used. A user name and password must be configured for updating signatures directly from Cisco.com.

**Examples**

The following example shows how to get the latest automatic signature update from Cisco.com:

```
Router# ips signature update cisco latest
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip ips auto-update</code></td>
<td>Enables automatic signature updates for Cisco IOS IPS.</td>
</tr>
<tr>
<td><code>cisco</code></td>
<td>Enables automatic signature updates from Cisco.com.</td>
</tr>
</tbody>
</table>
ipsec profile

To associate an IPsec profile to an Easy VPN tunnel and to avoid fragmentation of Quick Mode (QM) packets, use the `ipsec profile` command. To disable, use the `no` form of this command.

```
ipsec profile name
no crypto ipsec profile
```

**Syntax Description**

<table>
<thead>
<tr>
<th>name</th>
<th>The profile name.</th>
</tr>
</thead>
</table>

**Command Default**

If no IPsec profile is configured, Easy VPN Remote router sends all supported transform-sets during ISAKMP QM negotiations, which makes ISAKMP packets bigger and can cause fragmentation.

**Command Modes**

Cisco Easy VPN Remote configuration (config-crypto-ezvpn)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(20)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ipsec profile` command to configure IPsec transform-sets to avoid fragmentation of ISAKMP QM packets.

**Example**

```
crypto ipsec transform-set set1 esp-aes esp-sha-hmac
crypto ipsec profile prof1
set transform-set set1
set pfs group2
crypto ipsec client ezvpn EZVPN_CLIENT
connect auto
group hw-clients key cisco
mode network-extension
peer 10.1.1.2
ipsec-profile prof1
virtual-interface 1
username router1 password cisco
xauth userid mode local
```
**ipv4 (ldap)**

To create an IPv4 address within a Lightweight Directory Access Protocol (LDAP) server address pool, use the `ipv4` command in LDAP server configuration mode. To delete an IPv4 address within an LDAP server address pool, use the `no` form of this command.

```
ipv4 ipv4-address
no ipv4 ipv4-address
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv4-address</code></td>
<td>IPv4 address of the LDAP server.</td>
</tr>
</tbody>
</table>

**Command Default**

No IPv4 addresses are created in the LDAP server address pool.

**Command Modes**

LDAP server configuration (config-ldap-server)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to create an IPv4 address in an LDAP server address pool:

```
Router(config)# ldap server server1
Router(config-ldap-server)# ipv4 10.0.0.1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap server</td>
<td>Defines an LDAP server and enters LDAP server configuration mode.</td>
</tr>
<tr>
<td>transport port</td>
<td>Configures the transport protocol for establishing a connection with the LDAP server.</td>
</tr>
</tbody>
</table>
ipv6 crypto map

To enable an IPv6 crypto map on an interface, use the `ipv6 crypto map` command in interface configuration mode. To disable, use the `no` form of this command.

```
ipv6 crypto map map-name
no ipv6 crypto map
```

**Syntax Description**

- `map-name`: Identifies the crypto map set.

**Command Default**

No IPv6 crypto maps are enabled on the interface.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(4)M</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command differentiates IPv6 and IPv4 crypto maps.

**Examples**

The following example shows how to enable an IPv6 crypto map on an interface:

```
Router# configure terminal
Router(config)
  )# interface ethernet 0/0
Router(config-if)
  )# ipv6 crypto map CM_V4
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto map (global IPsec)</td>
<td>Creates or modifies a crypto map entry.</td>
</tr>
</tbody>
</table>
ipv6 cga modifier rsakeypair

To generate an IPv6 cryptographically generated address (CGA) modifier for a specified Rivest, Shamir, and Adelman (RSA) key pair, use the `ipv6 cga modifier rsakeypair` command in global configuration mode. To disable this function, use the `no` form of this command.

```
ipv6 cga modifier rsakeypair key-label sec-level sec-level-value [max-iterations value cga-modifier]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key-label</td>
<td>The name to be used for RSA key pair</td>
</tr>
<tr>
<td>sec-level</td>
<td>Specifies the security level, which can be a number from 0 through 3. The most secure level is 1.</td>
</tr>
<tr>
<td>sec-level-value</td>
<td>(Optional) Maximum iteration for modifier generation. The value can be a number from 0 through 40000000.</td>
</tr>
<tr>
<td>max-iterations</td>
<td>(Optional) An IPv6 address used as a CGA modifier.</td>
</tr>
<tr>
<td>cga-modifier</td>
<td></td>
</tr>
</tbody>
</table>

### Command Default

No CGA exists for an RSA key.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(3)T</td>
<td>The <code>max-iterations</code> keyword and <code>cga-modifier</code> argument were added.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to generate the CGA modifier for a specified RSA key pair, which enables the key to be used by Secure Neighbor Discovery (SeND).

Once the RSA key is generated, the modifier must be generated as well, using the `ipv6 cga modifier rsakeypair` command.

A CGA has a security parameter that determines its strength against brute-force attacks. The security level can be either 0 or 1.

### Examples

The following example enables the specified key to be used by SeND (that is, generates the modifier):

```
Router(config)# ipv6 cga modifier rsakeypair SEND sec-level 1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto key generate rsa</td>
<td>Generates RSA key pairs.</td>
</tr>
<tr>
<td>ipv6 cga modifier rsakeypair</td>
<td>Generates the CGA modifier for a specified RSA key.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>ipv6 cga modifier rsakeypair (interface)</td>
<td>Binds a SeND key to a specified interface.</td>
</tr>
<tr>
<td>ipv6 cga rsakeypair</td>
<td>Specifies which RSA key should be used on an interface.</td>
</tr>
</tbody>
</table>
ipv6 cga rsakeypair

To bind a Secure Neighbor Discovery (SeND) key to a specified interface, use the `ipv6 cga rsakeypair` command in interface configuration mode. To disable this function, use the `no` form of this command.

```
ipv6 cga rsakeypair key-label
no ipv6 cga rsakeypair
```

**Syntax Description**

- `key-label` The name to be used for the Rivest, Shamir, and Adelman (RSA) key pair.

**Command Default**

A SeND key is not bound to an interface.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The SeND key is used to generate an IPv6 modifier for a specified Rivest, Shamir and Adelman (RSA) key pair. A SeND key must be bound to the interface prior to its being used in the `ipv6 address` command. Use the `ipv6 cga rsakeypair` command to bind a SeND key to a specified interface.

You can then use the `ipv6 address` command to add the Cryptographic Addresses (CGA).

**Examples**

The following example binds a SeND key to Ethernet interface 0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.0.1.1 255.255.255.0
Router(config-if)# ipv6 cga rsakeypair SEND
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 address</code></td>
<td>Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.</td>
</tr>
<tr>
<td><code>crypto key generate rsa</code></td>
<td>Generates RSA key pairs.</td>
</tr>
<tr>
<td><code>ipv6 cga modifier rsakeypair (global configuration)</code></td>
<td>Generates the CGA modifier for a specified RSA key.</td>
</tr>
<tr>
<td><code>ipv6 cga modifier rsakeypair (interface configuration)</code></td>
<td>Binds a SeND key to a specified interface.</td>
</tr>
<tr>
<td><code>ipv6 cga rsakeypair</code></td>
<td>Specifies which RSA key should be used on an interface.</td>
</tr>
</tbody>
</table>
ipv6 inspect

To apply a set of inspection rules to an interface, use the `ipv6 inspect` command in interface configuration mode. To remove the set of rules from the interface, use the `no` form of this command.

```
ipv6 inspect inspection-name {in|out}
no ipv6 inspect inspection-name {in|out}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>inspection-name</code></td>
<td>Identifies which set of inspection rules to apply.</td>
</tr>
<tr>
<td><code>in</code></td>
<td>Applies the inspection rules to inbound traffic.</td>
</tr>
<tr>
<td><code>out</code></td>
<td>Applies the inspection rules to outbound traffic.</td>
</tr>
</tbody>
</table>

**Command Default**
If no set of inspection rules is applied to an interface, no traffic will be inspected by Context-Based Access Control (CBAC).

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use this command to apply a set of inspection rules to an interface.

Typically, if the interface connects to the external network, you apply the inspection rules to outbound traffic; alternately, if the interface connects to the internal network, you apply the inspection rules to inbound traffic.

If you apply the rules to outbound traffic, then return inbound packets will be permitted if they belong to a valid connection with existing state information. This connection must be initiated with an outbound packet.

If you apply the rules to inbound traffic, then return outbound packets will be permitted if they belong to a valid connection with existing state information. This connection must be initiated with an inbound packet.

**Examples**
The following example applies a set of inspection rules named "outboundrules" to an external interface’s outbound traffic. This causes inbound IP traffic to be permitted only if the traffic is part of an existing session, and to be denied if the traffic is not part of an existing session.

```
interface serial0
ipv6 inspect outboundrules out
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 inspect name</code></td>
<td>Defines a set of inspection rules.</td>
</tr>
</tbody>
</table>
**ipv6 inspect alert-off**

To disable Context-based Access Control (CBAC) alert messages, which are displayed on the console, use the `ipv6 inspect alert off` command in global configuration mode. To enable Cisco IOS firewall alert messages, use the `no` form of this command.

```
ipv6 inspect alert-off
no ipv6 inspect alert-off
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Alert messages are displayed.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example turns off CBAC alert messages:

```
ipv6 inspect alert-off
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 inspect audit trail</code></td>
<td>Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.</td>
</tr>
<tr>
<td><code>ipv6 inspect name</code></td>
<td>Applies a set of inspection rules to an interface.</td>
</tr>
</tbody>
</table>
ipv6 inspect audit trail

To turn on Context-based Access Control (CBAC) audit trail messages, which will be displayed on the console after each Cisco IOS firewall session closes, use the `ipv6 inspect audit trail` command in global configuration mode. To turn off Cisco IOS firewall audit trail message, use the no form of this command.

```
ipv6 inspect audit trail
no ipv6 inspect audit trail
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Audit trail messages are not displayed.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7T)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use this command to turn on CBAC audit trail messages.

**Examples**
The following example turns on CBAC audit trail messages:

```
ipv6 inspect audit trail
```

Afterward, audit trail messages such as the following are displayed:

```
%FW-6-SESS_AUDIT_TRAIL: tcp session initiator (192.168.1.13:33192) sent 22 bytes -- responder (192.168.129.11:25) sent 208 bytes
%FW-6-SESS_AUDIT_TRAIL: ftp session initiator 192.168.1.13:33194) sent 336 bytes -- responder (192.168.129.11:21) sent 325 bytes
```

These messages are examples of audit trail messages. To determine which protocol was inspected, refer to the responder’s port number. The port number follows the responder’s IP address.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 inspect alert-off</td>
<td>Disables CBAC alert messages.</td>
</tr>
<tr>
<td>ipv6 inspect name</td>
<td>Applies a set of inspection rules to an interface.</td>
</tr>
</tbody>
</table>
**ipv6 inspect max-incomplete high**

To define the number of existing half-open sessions that will cause the software to start deleting half-open sessions, use the `ipv6 inspect max-incomplete high` command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the `no` form of this command.

```
ipv6 inspect max-incomplete high number
no ipv6 inspect max-incomplete high
```

**Syntax Description**

| `number` | Specifies the rate of new unestablished TCP sessions that will cause the software to start deleting half-open sessions. The default is 500 half-open sessions. The value range is 1 through 4294967295. |

**Command Default**

The default is 500 half-open sessions.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the `max-incomplete high` number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the `max-incomplete low` number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

**Examples**

```
The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions when the number drops below 800:

ipv6 inspect max-incomplete high 900
ipv6 inspect max-incomplete low 800
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 inspect max-incomplete low</code></td>
<td>Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>ipv6 inspect one-minute high</code></td>
<td>Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.</td>
</tr>
<tr>
<td><code>ipv6 inspect one-minute low</code></td>
<td>Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.</td>
</tr>
<tr>
<td><code>ipv6 inspect tcp max-incomplete host</code></td>
<td>Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.</td>
</tr>
</tbody>
</table>
**ipv6 inspect max-incomplete low**

To define the number of existing half-open sessions that will cause the software to stop deleting half-open sessions, use the `ipv6 inspect max-incomplete low` command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the `no` form of this command.

```
ipv6 inspect max-incomplete low number
no ipv6 inspect max-incomplete low
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Specifies the number of existing half-open sessions that will cause the software to stop deleting half-open sessions. The default is 400 half-open sessions. Value range is 1 through 4294967295.</td>
</tr>
</tbody>
</table>

**Command Default**

The default is 400 half-open sessions.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the `max-incomplete high` number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the `max-incomplete low` number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

**Examples**

The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions when the number drops below 800:

```
ipv6 inspect max-incomplete high 900
ipv6 inspect max-incomplete low 800
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 inspect max-incomplete high</code></td>
<td>Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ipv6 inspect one-minute high</td>
<td>Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.</td>
</tr>
<tr>
<td>ipv6 inspect one-minute low</td>
<td>Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.</td>
</tr>
<tr>
<td>ipv6 inspect tcp max-incomplete host</td>
<td>Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.</td>
</tr>
</tbody>
</table>
**ipv6 inspect name**

To define a set of ipv6 inspection rules, use the `ipv6 inspect name` command in global configuration mode. To remove the inspection rule for a protocol or to remove the entire set of inspection rules, use the `no` form of this command.

```
ipv6 inspect name inspection-name protocol [alert {on|off}] [audit-trail {on|off}] [timeout seconds]
no ipv6 inspect name inspection-name [protocol]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>inspection-name</td>
<td>Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same inspection name as the existing set of rules.</td>
</tr>
<tr>
<td>protocol</td>
<td>A specified protocol. Possible protocol values are <code>icmp</code>, <code>udp</code>, <code>tcp</code>, and <code>ftp</code>. This value is optional in the <code>no</code> version of this command.</td>
</tr>
<tr>
<td>alert</td>
<td>(Optional) For each inspected protocol, the generation of alert messages can be set be on or off. If no option is selected, alerts are generated based on the setting of the <code>ipv6 inspect alert-off</code> command.</td>
</tr>
<tr>
<td>audit-trail</td>
<td>(Optional) For each inspected protocol, the audit trail can be set on or off. If no option is selected, audit trail messages are generated based on the setting of the <code>ipv6 inspect audit-trail</code> command.</td>
</tr>
<tr>
<td>timeout seconds</td>
<td>(Optional) Specifies the number of seconds for a different idle timeout to override the global TCP or User Datagram Protocol (UDP) idle timeouts for the specified protocol. This timeout overrides the global TCP and UDP timeouts but will not override the global Domain Name System (DNS) timeout.</td>
</tr>
<tr>
<td>timeout seconds</td>
<td>Configures the number of seconds that a packet state structure remains active. When the <code>timeout</code> value expires, the router drops the unassembled packet, freeing that structure for use by another packet. The default <code>timeout</code> value is 1 second. If this number is set to a value greater than 1 second, it will be automatically adjusted by the Cisco IOS software when the number of free state structures goes below certain thresholds: when the number of free states is less than 32, the timeout will be divided by 2. When the number of free states is less than 16, the timeout will be set to 1 second.</td>
</tr>
</tbody>
</table>

**Command Default**

No set of inspection rules is defined.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.3(11)T</td>
<td>FTP protocol support was added.</td>
</tr>
</tbody>
</table>
Usage Guidelines

To define a set of inspection rules, enter this command for each protocol that you want the Cisco IOS firewall to inspect, using the same `inspection-name`. Give each set of inspection rules a unique `inspection-name`, which should not exceed the 16-character limit. Define either one or two sets of rules per interface—you can define one set to examine both inbound and outbound traffic, or you can define two sets: one for outbound traffic and one for inbound traffic.

To define a single set of inspection rules, configure inspection for all the desired application-layer protocols, and for TCP, UDP, or Internet Control Message Protocol (ICMP) as desired. This combination of TCP, UDP, and application-layer protocols join together to form a single set of inspection rules with a unique name. (There are no application-layer protocols associated with ICMP.)

To remove the inspection rule for a protocol, use the `no` form of this command with the specified inspection name and protocol. To remove the entire set of named inspection rules, use the `no` form of this command with the specified inspection name.

In general, when inspection is configured for a protocol, return traffic entering the internal network will be permitted only if the packets are part of a valid, existing session for which state information is being maintained.

TCP and UDP Inspection

You can configure TCP and UDP inspection to permit TCP and UDP packets to enter the internal network through the firewall, even if the application-layer protocol is not configured to be inspected. However, TCP and UDP inspection do not recognize application-specific commands, and therefore might not permit all return packets for an application, particularly if the return packets have a different port number from the previous exiting packet.

Any application-layer protocol that is inspected will take precedence over the TCP or UDP packet inspection. For example, if inspection is configured for FTP, all control channel information will be recorded in the state table, and all FTP traffic will be permitted back through the firewall if the control channel information is valid for the state of the FTP session. The fact that TCP inspection is configured is irrelevant.

With TCP and UDP inspection, packets entering the network must exactly match an existing session: the entering packets must have the same source or destination addresses and source or destination port numbers as the exiting packet (but reversed). Otherwise, the entering packets will be blocked at the interface.

ICMP Inspection

An ICMP inspection session is on the basis of the source address of the inside host that originates the ICMP packet. Dynamic access control lists (ACLs) are created for return ICMP packets of the allowed types (destination unreachable, echo-reply, time-exceeded, and packet too big) for each session. There are no port numbers associated with an ICMP session, and the permitted IP address of the return packet is wild-carded in the ACL. The wild-card address is because the IP address of the return packet cannot be known in advance for time-exceeded and destination-unreachable replies. These replies can come from intermediate devices rather than the intended destination.

FTP Inspection

Cisco IOS Firewall uses layer 7 support for application modules such as FTP.

Cisco IOS IPv6 Firewall uses RFC 2428 to garner IPv6 addresses and corresponding ports. If an address other than an IPv6 address is present, the FTP data channel is not opened.

IPv6-specific port-to-application mapping (PAM) provides FTP inspection. PAM translates TCP or UDP port numbers into specific network services or applications. By mapping port numbers to network services or applications, an administrator can force firewall inspection on custom configurations not defined by well-known ports. PAM delivers with the standard well-known ports defined as defaults.

The table below describes the transport-layer and network-layer protocols.
### Table 15: Protocol Keywords--Transport-Layer and Network-Layer Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Keyword</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>icmp</td>
</tr>
<tr>
<td>TCP</td>
<td>tcp</td>
</tr>
<tr>
<td>UDP</td>
<td>udp</td>
</tr>
<tr>
<td>FTP</td>
<td>ftp</td>
</tr>
</tbody>
</table>

#### Use of the timeout Keyword

If you specify a timeout for any of the transport-layer or application-layer protocols, the timeout will override the global idle timeout for the interface to which the set of inspection rules is applied.

If the protocol is TCP or a TCP application-layer protocol, the timeout will override the global TCP idle timeout. If the protocol is UDP or a UDP application-layer protocol, the timeout will override the global UDP idle timeout.

If you do not specify a timeout for a protocol, the timeout value applied to a new session of that protocol will be taken from the corresponding TCP or UDP global timeout value valid at the time of session creation.

The default ICMP timeout is deliberately short (10 seconds) due to the security hole that is opened by allowing ICMP packets with a wild-carded source address back into the inside network. The timeout will occur 10 seconds after the last outgoing packet from the originating host. For example, if you send a set of 10 ping packets spaced one second apart, the timeout will expire in 20 seconds or 10 seconds after the last outgoing packet. However, the timeout is not extended for return packets. If a return packet is not seen within the timeout window, the hole will be closed and the return packet will not be allowed in. Although the default timeout can be made longer if desired, it is recommended that this value be kept relatively short.

#### Examples

The following example causes the software to inspect TCP sessions and UDP sessions:

```bash
ipv6 inspect name myrules tcp
ipv6 inspect name myrules udp audit-trail on
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 inspect alert-off</td>
<td>Disables CBAC alert messages.</td>
</tr>
<tr>
<td>ipv6 inspect audit trail</td>
<td>Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.</td>
</tr>
</tbody>
</table>
**ipv6 inspect one-minute high**

To define the rate of new unestablished sessions that will cause the software to start deleting half-open sessions, use the `ipv6 inspect one-minute high` command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the `no` form of this command.

```
ipv6 inspect one-minute high  number
no ipv6 inspect one-minute high
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>number</th>
<th>Specifies the rate of new unestablished TCP sessions that will cause the software to start deleting half-open sessions. The default is 500 half-open sessions. Value range is 1 through 4294967295</th>
</tr>
</thead>
</table>

**Command Default**
The default is 500 half-open sessions.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7T)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the `one-minute high` number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the `one-minute low` number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. (The rate is calculated as an exponentially-decayed rate.)

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

**Examples**
The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ipv6 inspect one-minute high 1000
ipv6 inspect one-minute low 950
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 inspect one-minute low</code></td>
<td>Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.</td>
</tr>
<tr>
<td><code>ipv6 inspect max-incomplete high</code></td>
<td>Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.</td>
</tr>
<tr>
<td><code>ipv6 inspect max-incomplete low</code></td>
<td>Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.</td>
</tr>
<tr>
<td><code>ipv6 inspect tcp max-incomplete host</code></td>
<td>Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.</td>
</tr>
</tbody>
</table>
ipv6 inspect one-minute low

To define the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions, use the `ipv6 inspect one-minute low` command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the `no` form of this command.

```
ipv6 inspect one-minute low number
no ipv6 inspect one-minute low
```

**Syntax Description**

| `number` | Specifies the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions. The default is 400 half-open sessions. Value range is 1 through 4294967295. |

**Command Default**

The default is 400 half-open sessions.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7T)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the `one-minute high` number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the `one-minute low` number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. (The rate is calculated as an exponentially decayed rate.)

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

**Examples**

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ipv6 inspect one-minute high 1000
ipv6 inspect one-minute low 950
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ipv6 inspect max-incomplete high</td>
<td>Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.</td>
</tr>
<tr>
<td></td>
<td>ipv6 inspect max-incomplete low</td>
<td>Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.</td>
</tr>
<tr>
<td></td>
<td>ipv6 inspect one-minute high</td>
<td>Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.</td>
</tr>
<tr>
<td></td>
<td>ipv6 inspect tcp max-incomplete host</td>
<td>Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.</td>
</tr>
</tbody>
</table>
ipv6 inspect routing-header

To specify whether Context-based Access Control (CBAC) should inspect packets containing an IPv6 routing header, use the `ipv6 inspect routing-header` command. To drop packets containing an IPv6 routing header, use the `no` form of this command.

```
ipv6 inspect routing-header
no ipv6 inspect routing-header
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Packets containing IPv6 routing header are dropped.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7T)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An IPv6 source uses the routing header to list one or more intermediate nodes to be visited between the source and destination of the packet. The Cisco IOS firewall uses this header to retrieve the destination host address. Cisco IOS firewall will establish the appropriate inspection session based on the retrieved address from the routing header.

The originating node lists all intermediate nodes that the packet must traverse. The source and destination address pair in the IPv6 header identifies the hop between the originating node and the first intermediate node. Once the first intermediate node receives the packet, it looks for a routing header. If the routing header is present, the next intermediate node address is swapped with the destination address in the IPv6 header and the packet is forwarded to the next intermediate node. This sequence continues for each intermediate node listed in the routing until no more entries exist in the routing header. The last entry in the routing header is the final destination address.

**Examples**

The following example causes the software to inspect TCP sessions and UDP sessions:

```
ip inspect routing-header
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 inspect alert-off</td>
<td>Disables CBAC alert messages.</td>
</tr>
<tr>
<td>ipv6 inspect audit trail</td>
<td>Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.</td>
</tr>
<tr>
<td>ipv6 inspect name</td>
<td>Applies a set of inspection rules to an interface.</td>
</tr>
</tbody>
</table>
**ipv6 inspect tcp idle-time**

To specify the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity), use the `ipv6 inspect tcp idle-time` command in global configuration mode. To reset the timeout to the default of 3600 seconds (1 hour), use the `no` form of this command.

```
ipv6 inspect tcp idle-time seconds
no ipv6 inspect tcp idle-time
```

**Syntax Description**

| seconds | Specifies the length of time, in seconds, for which a TCP session will still be managed while there is no activity. The default is 3600 seconds (1 hour). |

**Command Default**

The default is 3600 seconds (1 hour)

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the software detects a valid TCP packet that is the first in a session, and if Context-based Access Control (CBAC) inspection is configured for the packet’s protocol, the software establishes state information for the new session.

If the software detects no packets for the session for a time period defined by the TCP idle timeout, the software will not continue to manage state information for the session.

The global value specified for this timeout applies to all TCP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the `ipv6 inspect name` (global configuration) command.

---

**Note**

This command does not affect any of the currently defined inspection rules that have explicitly defined timeouts. Sessions created based on these rules still inherit the explicitly defined timeout value. If you change the TCP idle timeout with this command, the new timeout will apply to any new inspection rules you define or to any existing inspection rules that do not have an explicitly defined timeout. That is, new sessions based on these rules (having no explicitly defined timeout) will inherit the global timeout value.

**Examples**

The following example sets the global TCP idle timeout to 1800 seconds (30 minutes):

```
ipv6 inspect tcp idle-time 1800
```

The following example sets the global TCP idle timeout back to the default of 3600 seconds (one hour):

```
no ipv6 inspect tcp idle-time
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 inspect name</code></td>
<td>Defines a set of IPv6 inspection rules.</td>
</tr>
</tbody>
</table>
ipv6 inspect tcp max-incomplete host

To specify threshold and blocking time values for TCP host-specific denial-of-service detection and prevention, use the `ipv6 inspect tcp max-incomplete host` command in global configuration mode. To reset the threshold and blocking time to the default values, use the `no` form of this command.

`ipv6 inspect tcp max-incomplete host number block-time minutes`

`no ipv6 inspect tcp max-incomplete host`

### Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>number</strong></td>
<td>Specifies how many half-open TCP sessions with the same host destination address can exist at a time, before the software starts deleting half-open sessions to the host. Use a number from 1 to 250. The default is 50 half-open sessions. Value range is 1 through 4294967295.</td>
</tr>
<tr>
<td><strong>block-time</strong></td>
<td>Specifies blocking of connection initiation to a host. Value range is 0 through 35791.</td>
</tr>
<tr>
<td><strong>minutes</strong></td>
<td>Specifies how long the software will continue to delete new connection requests to the host. The default is 0 minutes.</td>
</tr>
</tbody>
</table>

### Command Default

The default is 50 half-open sessions and 0 minutes.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7T)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

An unusually high number of half-open sessions with the same destination host address could indicate that a denial-of-service attack is being launched against the host. For TCP, "half-open" means that the session has not reached the established state.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (the `max-incomplete host` number), the software will delete half-open sessions according to one of the following methods:

- If the `block-time minutes` timeout is 0 (the default):

  The software will delete the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.

- If the `block-time minutes` timeout is greater than 0:

  The software will delete all existing half-open sessions for the host, and then block all new connection requests to the host. The software will continue to block all new connection requests until the `block-time` expires.

  The software also sends syslog messages whenever the `max-incomplete host` number is exceeded and when blocking of connection initiations to a host starts or ends.

The global values specified for the threshold and blocking time apply to all TCP connections inspected by Context-based Access Control (CBAC).
Examples

The following example changes the `max-incomplete host` number to 40 half-open sessions, and changes the `block-time` timeout to 2 minutes (120 seconds):

```
ipv6 inspect tcp max-incomplete host 40 block-time 120
```

The following example resets the defaults (50 half-open sessions and 0 seconds):

```
no ipv6 inspect tcp max-incomplete host
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 inspect max-incomplete high</code></td>
<td>Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.</td>
</tr>
<tr>
<td><code>ipv6 inspect max-incomplete low</code></td>
<td>Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.</td>
</tr>
<tr>
<td><code>ipv6 inspect one-minute high</code></td>
<td>Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.</td>
</tr>
<tr>
<td><code>ipv6 inspect one-minute low</code></td>
<td>Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.</td>
</tr>
</tbody>
</table>
**ipv6 inspect tcp synwait-time**

To define how long the software will wait for a TCP session to reach the established state before dropping the session, use the `ipv6 inspect tcp synwait-time` command in global configuration mode. To reset the timeout to the default of 30 seconds, use the `no` form of this command.

```
ipv6 inspect tcp synwait-time seconds
no ipv6 inspect tcp synwait-time
```

**Syntax Description**

| seconds | Specifies how long, in seconds, the software will wait for a TCP session to reach the established state before dropping the session. The default is 30 seconds. Value range is 1 through 2147483 |

**Command Default**

The default is 30 seconds.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7T)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to define how long Cisco IOS software will wait for a TCP session to reach the established state before dropping the session. The session is considered to have reached the established state after the session’s first SYN bit is detected.

The global value specified for this timeout applies to all TCP sessions inspected by Context-based Access Control (CBAC).

**Examples**

The following example changes the "synwait" timeout to 20 seconds:

```
ipv6 inspect tcp synwait-time 20
```

The following example changes the "synwait" timeout back to the default (30 seconds):

```
no ipv6 inspect tcp synwait-time
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 inspect udp idle-time</code></td>
<td>Specifies the User Datagram Protocol idle timeout (the length of time for which a UDP &quot;session&quot; will still be managed while there is no activity).</td>
</tr>
</tbody>
</table>
ipv6 inspect udp idle-time

To specify the User Datagram Protocol idle timeout (the length of time for which a UDP "session" will still be managed while there is no activity), use the `ipv6 inspect udp idle-time` command in global configuration mode. To reset the timeout to the default of 30 seconds, use the `no` form of this command.

```
ipv6 inspect udp idle-time seconds
no ipv6 inspect udp idle-time
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>Specifies the length of time a UDP &quot;session&quot; will still be managed while there is no activity. The default is 30 seconds. Value range is 1 through 2147483.</td>
</tr>
</tbody>
</table>

**Command Default**

The default is 30 seconds.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the software detects a valid UDP packet, if Context-based Access Control (CBAC) inspection is configured for the packet’s protocol, the software establishes state information for a new UDP "session." Because UDP is a connectionless service, there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining if the packet is similar to other UDP packets (for example, it has similar source or destination addresses) and if the packet was detected soon after another similar UDP packet.

If the software detects no UDP packets for the UDP session for the a period of time defined by the UDP idle timeout, the software will not continue to manage state information for the session.

The global value specified for this timeout applies to all UDP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the `ipv6 inspect name` command.

**Note**

This command does not affect any of the currently defined inspection rules that have explicitly defined timeouts. Sessions created based on these rules still inherit the explicitly defined timeout value. If you change the UDP idle timeout with this command, the new timeout will apply to any new inspection rules you define or to any existing inspection rules that do not have an explicitly defined timeout. That is, new sessions based on these rules (having no explicitly defined timeout) will inherit the global timeout value.

**Examples**

The following example sets the global UDP idle timeout to 120 seconds (2 minutes):

```
ipv6 inspect udp idle-time 120
```

The following example sets the global UDP idle timeout back to the default of 30 seconds:

```
no ipv6 inspect udp idle-time
```
no ipv6 inspect udp idle-time
**ipv6 nd inspection**

To apply the Neighbor Discovery Protocol (NDP) Inspection feature, use the `ipv6 nd inspection` command in interface configuration mode. To remove the NDP Inspection feature, use the `no` form of this command.

```
ipv6 nd inspection [attach-policy [policy-name] | vlan {add | except | none | remove | all} vlan vlan-id ]
no ipv6 nd inspection
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>attach-policy</code></td>
<td>(Optional) Attaches an NDP Inspection policy.</td>
</tr>
<tr>
<td><code>policy-name</code></td>
<td>(Optional) The NDP Inspection policy name.</td>
</tr>
<tr>
<td><code>vlan</code></td>
<td>(Optional) Applies the ND Inspection feature to a VLAN on the interface.</td>
</tr>
<tr>
<td><code>add</code></td>
<td>(Optional) Adds a VLAN to be inspected.</td>
</tr>
<tr>
<td><code>except</code></td>
<td>(Optional) Inspects all VLANs except the one specified.</td>
</tr>
<tr>
<td><code>none</code></td>
<td>(Optional) Specifies that no VLANs are inspected.</td>
</tr>
<tr>
<td><code>remove</code></td>
<td>(Optional) Removes the specified VLAN from NDP inspection.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>(Optional) Inspects NDP traffic from all VLANs on the port.</td>
</tr>
<tr>
<td><code>vlan-id</code></td>
<td>(Optional) A specific VLAN on the interface. More than one VLAN can be specified. The VLAN number that can be used is from 1 to 4094.</td>
</tr>
</tbody>
</table>

**Command Default**

All NDP messages are inspected. Secure Neighbor Discovery (SeND) options are ignored. Neighbors are probed based on the criteria defined in the Neighbor Tracking feature. Per-port IPv6 address limit enforcement is disabled. Layer 2 header source MAC address validations are disabled. Per-port rate limiting of the NDP messages in software is disabled.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(2)SE</td>
<td>This command was integrated into Cisco IOS Release 15.0(2)SY.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2E</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 nd inspection` command applies the NDP Inspection feature on a specified interface. If you enable the optional `attach-policy` or `vlan` keywords, NDP traffic is inspected by policy or by VLAN. If no VLANs are specified, NDP traffic from all VLANs on the port is inspected (which is equivalent to using the `vlan all` keywords).

If no policy is specified in this command, the default criteria are as follows:
• All NDP messages are inspected.
• SeND options are ignored.
• Neighbors are probed based on the criteria defined in neighbor tracking feature.
• Per-port IPv6 address limit enforcement is disabled.
• Layer 2 header source MAC address validations are disabled.
• Per-port rate limiting of the NDP messages in software is disabled.

If a VLAN is specified, its parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lesser one first, separated by a dash (for example, `vlan 1-100,200-300-400`). Do not enter any spaces between comma-separated VLAN parameters or in dash-specified ranges.

**Examples**

The following example enables NDP inspection on a specified interface:

```
Router(config-if)# ipv6 nd inspection
```
ipv6 nd inspection policy

To define the neighbor discovery (ND) inspection policy name and enter ND inspection policy configuration mode, use the `ipv6 nd inspection` command in ND inspection configuration mode. To remove the ND inspection policy, use the `no` form of this command.

```
ipv6 nd inspection policy policy-name
no ipv6 nd inspection policy policy-name
```

**Syntax Description**

| policy-name | The ND inspection policy name. |

**Command Default**

No ND inspection policies are configured.

**Command Modes**

ND inspection configuration (config-nd-inspection)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(2)SE</td>
<td>This command was integrated into Cisco IOS Release 15.0(2)SE.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 nd inspection policy` command defines the ND inspection policy name and enters ND inspection policy configuration mode. Once you are in ND inspection policy configuration mode, you can use any of the following commands:

- `device-role`
- `drop-unsecure`
- `limit address-count`
- `sec-level minimum`
- `tracking`
- `trusted-port`
- `validate source-mac`

**Examples**

The following example defines an ND policy name as policy1:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)#
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>device-role</td>
<td>Specifies the role of the device attached to the port.</td>
</tr>
<tr>
<td>drop-unsecure</td>
<td>Drops messages with no or invalid options or an invalid signature.</td>
</tr>
<tr>
<td>limit address-count</td>
<td>Limits the number of IPv6 addresses allowed to be used on the port.</td>
</tr>
<tr>
<td>sec-level minimum</td>
<td>Specifies the minimum security level parameter value when CGA options are used.</td>
</tr>
<tr>
<td>tracking</td>
<td>Overrides the default tracking policy on a port.</td>
</tr>
<tr>
<td>trusted-port</td>
<td>Configures a port to become a trusted port.</td>
</tr>
<tr>
<td>validate source-mac</td>
<td>Checks the source MAC address against the link-layer address.</td>
</tr>
</tbody>
</table>
**ipv6 nd prefix framed-ipv6-prefix**

To add the prefix in a received RADIUS framed IPv6 prefix attribute to the interface’s neighbor discovery prefix queue, use the `ipv6 nd prefix framed-ipv6-prefix` command in interface configuration mode. To disable this feature, use the `no` form of this command.

```
ipv6 nd prefix framed-ipv6-prefix
no ipv6 nd prefix framed-ipv6-prefix
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Prefix is sent in the router advertisements (RAs).

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)SXE</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXE.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ipv6 nd prefix framed-ipv6-prefix` command to add the prefix in a received RADIUS framed IPv6 prefix attribute to the interface’s neighbor discovery prefix queue and include it in RAs sent on the interface’s link. By default, the prefix is sent in RAs. If the prefix in the attribute should be used by other applications such as the Dynamic Host Configuration Protocol (DHCP) for IPv6 server, administrators can disable the default behavior with the `no` form of the command.

**Examples**

The following example adds the prefix in a received RADIUS framed IPv6 prefix attribute to the interface’s neighbor discovery prefix queue:

```
ipv6 nd prefix framed-ipv6-prefix
```
ipv6 nd raguard attach-policy

To apply the IPv6 router advertisement (RA) guard feature on a specified interface, use the `ipv6 nd raguard attach-policy` command in interface configuration mode.

```
ipv6 nd raguard attach-policy [policy-name [vlan [add|except|none|remove|all] vlan [vlan1, vlan2, vlan3...]]]
```

**Syntax Description**

- `policy-name` (Optional) IPv6 RA guard policy name.
- `vlan` (Optional) Applies the IPv6 RA guard feature to a VLAN on the interface.
- `add` Adds a VLAN to be inspected.
- `except` All VLANs are inspected except the one specified.
- `none` No VLANs are inspected.
- `remove` Removes the specified VLAN from RA guard inspection.
- `all` ND traffic from all VLANs on the port is inspected.
- `vlan` (Optional) A specific VLAN on the interface. More than one VLAN can be specified (`vlan1, vlan2, vlan3...`). The range of available VLAN numbers is from 1 through 4094.

**Command Default**

An IPv6 RA guard policy is not configured.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
<tr>
<td>15.0(2)SE</td>
<td>This command was integrated into Cisco IOS Release 15.0(2)SE.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If no policy is specified using the `policy-name` argument, the port device role is set to host and all inbound router traffic (for example, RA and redirect messages) is blocked.

If no VLAN is specified (which is equal to entering the `vlan all` keywords after the `policy-name` argument), RA guard traffic from all VLANs on the port is analyzed.

If specified, the VLAN parameter is either a single VLAN number from 1 through 4094 or a range of VLANs described by two VLAN numbers, the lesser one first, separated by a dash. Do not enter any spaces between comma-separated vlan parameters or in dash-specified ranges; for example, `vlan 1-100,200,300-400`. 
In the following example, the IPv6 RA guard feature is applied on GigabitEthernet interface 0/0:

```
Device(config)# interface GigabitEthernet 0/0
Device(config-if)# ipv6 nd raguard attach-policy
```
ipv6 nd raguard policy

To define the router advertisement (RA) guard policy name and enter RA guard policy configuration mode, use the `ipv6 nd raguard policy` command in global configuration mode.

```
ipv6 nd raguardpolicy policy-name
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy-name</td>
<td>IPv6 RA guard policy name.</td>
</tr>
</tbody>
</table>

| Command Default    | An RA guard policy is not configured. |

| Command Modes      | Global configuration (config)# |

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
<tr>
<td></td>
<td>15.0(2)SE</td>
<td>This command was integrated into Cisco IOS Release 15.0(2)SE.</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th>Use the <code>ipv6 nd raguard policy</code> command to configure RA guard globally on a router. Once the device is in ND inspection policy configuration mode, you can use any of the following commands:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• device-role</td>
</tr>
<tr>
<td></td>
<td>• drop-unsecure</td>
</tr>
<tr>
<td></td>
<td>• limit address-count</td>
</tr>
<tr>
<td></td>
<td>• sec-level minimum</td>
</tr>
<tr>
<td></td>
<td>• trusted-port</td>
</tr>
<tr>
<td></td>
<td>• validate source-mac</td>
</tr>
</tbody>
</table>

After IPv6 RA guard is configured globally, you can use the `ipv6 nd raguard attach-policy` command to enable IPv6 RA guard on a specific interface.

<table>
<thead>
<tr>
<th>Examples</th>
<th>The following example shows how to define the RA guard policy name as policy1 and place the device in policy configuration mode:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Device(config)# ipv6 nd raguard policy policy1</td>
</tr>
<tr>
<td></td>
<td>Device(config-ra-guard)#</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>device-role</code></td>
<td>Specifies the role of the device attached to the port.</td>
</tr>
<tr>
<td><code>drop-unsecure</code></td>
<td>Drops messages with no or invalid options or an invalid signature.</td>
</tr>
<tr>
<td><code>ipv6 nd raguard attach-policy</code></td>
<td>Applies the IPv6 RA guard feature on a specified interface.</td>
</tr>
<tr>
<td><code>limit address-count</code></td>
<td>Limits the number of IPv6 addresses allowed to be used on the port.</td>
</tr>
<tr>
<td><code>sec-level minimum</code></td>
<td>Specifies the minimum security level parameter value when CGA options are used.</td>
</tr>
<tr>
<td><code>trusted-port</code></td>
<td>Configures a port to become a trusted port.</td>
</tr>
<tr>
<td><code>validate source-mac</code></td>
<td>Checks the source MAC address against the link layer address.</td>
</tr>
</tbody>
</table>
ipv6 nd secured certificate-db

To configure the maximum number of entries in an IPv6 Secure Neighbor Discovery (SeND) certificate database, use the `ipv6 nd secured certificate-db` command in global configuration mode. To disable any maximum number of entries set for a SeND certificate database, use the `no` form of this command.

```
ipv6 nd secured certificate-db max-entries max-entries-value
no ipv6 nd secured certificate-db max-entries
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-entries max-entries-value</td>
<td>Specifies the maximum number of entries in the certificate database. The range is from 1 to 1000.</td>
</tr>
</tbody>
</table>

**Command Default**

No SeND certificate database is configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command allows you to set up a maximum size for the certificate database (DB), to protect against denial of service (DoS) certificate flooding. When the limit is reached, new certificates are dropped.

The certificate DB is relevant on a router in host mode only, because it stores certificates received from routers.

**Examples**

The following example configures a SeND certificate database with a maximum number of 500 entries:

```
Router(config)# ipv6 nd secured certificate-db max-entries 500
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 nd secured full-secure (global configuration)</code></td>
<td>Enables SeND security mode on a router.</td>
</tr>
<tr>
<td><code>ipv6 nd secured full-secure (interface configuration)</code></td>
<td>Enables SeND security mode on a specified interface.</td>
</tr>
<tr>
<td><code>ipv6 nd secured key-length</code></td>
<td>Configures SeND key-length options.</td>
</tr>
<tr>
<td><code>ipv6 nd secured timestamp</code></td>
<td>Configures the SeND time stamp.</td>
</tr>
<tr>
<td><code>ipv6 nd secured timestamp-db</code></td>
<td>Configures the maximum number of entries that did not reach the destination in a SeND time-stamp database.</td>
</tr>
</tbody>
</table>
ipv6 nd secured full-secure

To enable the secure mode for IPv6 Secure Neighbor Discovery (SeND) on a router, use the `ipv6 nd secured full-secure` command in global configuration mode. To disable SeND security mode, use the `no` form of this command.

`ipv6 nd secured full-secure`  
`no ipv6 nd secured full-secure`

**Syntax Description**  
This command has no arguments or keywords.

**Command Default**  
Non-SeND neighbor discovery messages are accepted by the router.

**Command Modes**  
Global configuration (config)

**Command History**  
```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**  
The `ipv6 nd secured full-secure` command in global configuration mode allows you to configure the router to accept or reject non-SeND neighbor discovery messages. If this command is enabled, non-SeND messages are rejected by the specified router.

**Examples**  
The following example enables SeND security mode on a router:

```
Router(config)# ipv6 nd secured full-secure
```

**Related Commands**  
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd secured full-secure (interface configuration)</td>
<td>Enables SeND security mode on a specified interface.</td>
</tr>
</tbody>
</table>
ipv6 nd secured full-secure (interface)

To enable the secure mode for IPv6 Secure Neighbor Discovery (SeND) on a specified interface, use the `ipv6 nd secured full-secure` command in interface configuration mode. To provide the co-existence mode for secure and nonsecure neighbor discovery messages on an interface, use the `no` form of this command.

```
ipv6 nd secured full-secure
no ipv6 nd secured full-secure
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Non-SeND messages are accepted by the interface.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 nd secured full-secure` command in interface configuration mode allows you to configure a specified interface to accept or reject non-SeND neighbor discovery messages. If this command is enabled, non-SeND messages are rejected by the interface. If this command is not enabled, secure and nonsecure neighbor discovery messages can coexist on the same interface.

**Examples**

The following example enables SeND security mode on an interface:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 nd secured full-secure
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd secured full-secure (global configuration)</td>
<td>Enables SeND security mode on a specified router.</td>
</tr>
</tbody>
</table>
ipv6 nd secured key-length

To configure IPv6 Secure Neighbor Discovery (SeND) key-length options, use the `ipv6 nd secured key-length` command in global configuration mode. To disable the key length, use the `no` form of this command.

```
ipv6 nd secured key-length [[minimum|maximum] value]
no ipv6 nd secured key-length
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>minimum value</td>
<td>(Optional) Sets the minimum key-length value, which should be at least 384 bits. The range is from 384 to 2048 bits, and the default key-length value is 1024 bits.</td>
</tr>
<tr>
<td>maximum value</td>
<td>(Optional) Sets the maximum key-length value. The range is from 384 to 2048 bits, and the default key-length value is 1024 bits.</td>
</tr>
</tbody>
</table>

### Command Default

The key length is 1024 bits.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

When used by SeND, the key length is checked against the key-length value, as set in the `ipv6 nd secured key-length` command. When packets are received from a neighbor with a key length that is out of the configured boundaries, the packets are treated as unsecure.

### Examples

The following example sets the minimum key-length value to 512 bits and the maximum value to 1024 bits:

```
Router(config)# ipv6 nd secured key-length minimum 512
Router(config)# ipv6 nd secured key-length maximum 1024
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 nd secured certificate-db</code></td>
<td>Configures the maximum number of entries in a SeND certificate database.</td>
</tr>
<tr>
<td><code>ipv6 nd secured full-secure (global configuration)</code></td>
<td>Enables SeND security mode on a specified router.</td>
</tr>
<tr>
<td><code>ipv6 nd secured full-secure (interface configuration)</code></td>
<td>Enables SeND security mode on a specified interface.</td>
</tr>
<tr>
<td><code>ipv6 nd secured timestamp</code></td>
<td>Configures the SeND time stamp.</td>
</tr>
<tr>
<td><code>ipv6 nd secured timestamp-db</code></td>
<td>Configures the maximum number of entries in a SeND time-stamp database.</td>
</tr>
</tbody>
</table>
ipv6 nd secured sec-level

To configure the minimum security value that IPv6 Secure Neighbor Discovery (SeND) will accept from its peer, use the `ipv6 nd secured sec-level` command in global configuration mode. To disable the security level, use the `no` form of this command.

```
ipv6 nd secured sec-level [minimum value]
no ipv6 nd secured sec-level
```

### Syntax Description

| minimum value | (Optional) Sets the minimum security level, which is a value from 0 through 7. The default security level is 1. |

### Command Default

The default security level is 1.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `ipv6 nd secured sec-level` command allows the user to configure the minimum security value the router will accept from its peer.

### Examples

The following example sets the minimum security level to 2:

```
Router(config)# ipv6 nd secured sec-level 2
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd secured certificate-db</td>
<td>Configures the maximum number of entries in a SeND certificate database.</td>
</tr>
<tr>
<td>ipv6 nd secured full-secure (global configuration)</td>
<td>Enables SeND security mode on a specified router.</td>
</tr>
<tr>
<td>ipv6 nd secured full-secure (interface configuration)</td>
<td>Enables SeND security mode on a specified interface.</td>
</tr>
<tr>
<td>ipv6 nd secured key-length</td>
<td>Configures SeND key-length options.</td>
</tr>
<tr>
<td>ipv6 nd secured timestamp</td>
<td>Configures the SeND time stamp.</td>
</tr>
<tr>
<td>ipv6 nd secured timestamp-db</td>
<td>Configures the maximum number of unreached entries in a SeND time-stamp database.</td>
</tr>
</tbody>
</table>
ipv6 nd secured timestamp

To configure the IPv6 Secure Neighbor Discovery (SeND) timestamp, use the `ipv6 nd secured timestamp` command in interface configuration mode. To return to the default settings, use the `no` form of this command.

```
ipv6 nd secured timestamp {delta value|fuzz value}
no ipv6 nd secured timestamp
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>delta value</code></td>
<td>Specifies the maximum time difference accepted between the sender and the receiver. Default value is 300 seconds.</td>
</tr>
<tr>
<td><code>fuzz value</code></td>
<td>Specifies the maximum age of the message, when the delta is taken into consideration; that is, the amount of time, in seconds, that a packet can arrive after the delta value before being rejected. Default value is 1 second.</td>
</tr>
</tbody>
</table>

**Command Default**
Default time-stamp values are used.

**Command Modes**
Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `ipv6 nd secured timestamp` command configures the amount of time the router waits before it accepts or rejects packets it has received.

**Examples**
The following example configures the SeND time stamp to be 600 seconds:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 nd secured timestamp delta 600
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd secured certificate-db</td>
<td>Configures the maximum number of entries in a SeND certificate database.</td>
</tr>
<tr>
<td>ipv6 nd secured full-secure (global configuration)</td>
<td>Enables SeND security mode on a specified router.</td>
</tr>
<tr>
<td>ipv6 nd secured full-secure (interface configuration)</td>
<td>Enables SeND security mode on a specified interface.</td>
</tr>
<tr>
<td>ipv6 nd secured key-length</td>
<td>Configures SeND key-length options.</td>
</tr>
<tr>
<td>ipv6 nd secured timestamp-db</td>
<td>Configures the maximum number of unreached entries in a SeND time-stamp database.</td>
</tr>
</tbody>
</table>
To configure the maximum number of unreached entries in an IPv6 Secure Neighbor Discovery (SeND) time-stamp database, use the `ipv6 nd secured timestamp-db` command in global configuration mode. To return to the default settings, use the `no` form of this command.

```
ipv6 nd secured timestamp-db max-entries max-entries-value
no ipv6 nd secured timestamp-db max-entries
```

Syntax Description

| max-entries max-entries-value | Specifies the maximum number of entries in the certificate database. The range is from 1 to 1000. |

Command Default

No time-stamp database is configured.

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following example configures the time-stamp database on a router:

```
Router(config)# ipv6 nd secured timestamp-db max-entries 345
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd secured certificate-db</td>
<td>Configures the maximum number of entries in a SeND certificate database.</td>
</tr>
<tr>
<td>ipv6 nd secured full-secure (global configuration)</td>
<td>Enables SeND security mode on a specified router.</td>
</tr>
<tr>
<td>ipv6 nd secured full-secure (interface configuration)</td>
<td>Enables SeND security mode on a specified interface.</td>
</tr>
<tr>
<td>ipv6 nd secured key-length</td>
<td>Configures SeND key-length options.</td>
</tr>
<tr>
<td>ipv6 nd secured timestamp</td>
<td>Configures the SeND time stamp.</td>
</tr>
</tbody>
</table>
ipv6 nd secured trustanchor

To specify an IPv6 Secure Neighbor Discovery (SeND) trusted anchor on an interface, use the `ipv6 nd secured trustanchor` command in interface configuration mode. To remove a trusted anchor, use the `no` form of this command.

```
ipv6 nd secured trustanchor trustanchor-name
no ipv6 nd secured trustanchor trustanchor-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>trustanchor-name</code></td>
<td>The name to be found in the certificate of the trustpoint.</td>
</tr>
</tbody>
</table>

**Command Default**

No trusted anchor is defined.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 nd secured trustanchor` command is used to select the certificate authority (CA) you want to authenticate. The trusted anchors configured by this command act as references to the trustpoints configured.

A crypto Public Key Infrastructure (PKI) trustpoint can be a self-signed root CA or a subordinate CA. The `trustpoint-name` argument refers to the name to be found in the certificate of the trustpoint.

The `ipv6 nd secured trustanchor` and `ipv6 nd secured trustpoint` commands both generate an entry in the SeND configuration database that points to the trustpoint provided. More than one trustpoint can be provided for each command, and the same trustpoint can be used in both commands.

**Examples**

The following example specifies trusted anchor anchor1 on Ethernet interface 0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 nd secured trustanchor anchor1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto pki trustpoint</td>
<td>Declares the trustpoint that your router should use.</td>
</tr>
<tr>
<td>ipv6 nd secured trustpoint</td>
<td>Specifies which trustpoint should be used for selecting the certificate to advertise.</td>
</tr>
</tbody>
</table>
ipv6 nd secured trustpoint

To specify which trustpoint should be used in the ipv6 Secure Neighbor Discovery (SeND) protocol for selecting the certificate to advertise, use the ipv6 nd secured trustpoint command in interface configuration mode. To disable the trustpoint, use the no form of this command.

```
ipv6 nd secured trustpoint trustpoint-name
no ipv6 nd secured trustpoint trustpoint-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trustpoint-name</td>
<td>The name to be found in the certificate of the trustpoint.</td>
</tr>
</tbody>
</table>

**Command Default**

SeND is not enabled on a specified interface.

**Command Modes**

Command configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(24)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The ipv6 nd secured trustpoint command enables SeND on an interface and specifies which trustpoint should be used. The trustpoint points to the Rivest, Shamir, and Adelman (RSA) key pair and the trusted anchor (which is the certificate authority [CA] signing your certificate).

The ipv6 nd secured trustpoint and ipv6 nd secured trustanchor commands both generate an entry in the SeND configuration database that points to the trustpoint provided. More than one trustpoint can be provided for each command, and the same trustpoint can be used in both commands. However, the trustpoint provided in the ipv6 nd secured trustpoint command must include a router certificate and the signing CA certificate. It may also include the certificate chain up to the root certificate provided by a CA that hosts (connected to the router) will trust.

The trustpoint provided in the ipv6 nd secured trustanchor command must only include a CA certificate.

**Examples**

The following example specifies trusted anchor anchor1 on Ethernet interface 0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 nd secured trustpoint trustpoint1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto pki trustpoint</td>
<td>Declares the trustpoint that your router should use.</td>
</tr>
<tr>
<td>ipv6 nd secured trustanchor</td>
<td>Specifies a trusted anchor on an interface.</td>
</tr>
</tbody>
</table>
ipv6 nd suppress-ra

Note
Effective with Cisco IOS Release 12.4(2)T, the **ipv6 nd suppress-ra** command is replaced by the **ipv6 nd ra suppress** command. See the **ipv6 nd ra suppress** command for more information.

To suppress IPv6 router advertisement transmissions on a LAN interface, use the **ipv6 nd suppress-ra** command in interface configuration mode. To reenable the sending of IPv6 router advertisement transmissions on a LAN interface, use the no form of this command.

```
ipv6 nd suppress-ra
no ipv6 nd suppress-ra
```

Syntax Description
This command has no arguments or keywords.

Command Default
IPv6 router advertisements are automatically sent on Ethernet and FDDI interfaces if IPv6 unicast routing is enabled on the interfaces. IPv6 router advertisements are not sent on other types of interfaces.

Command Modes
Interface configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.0(21)ST</td>
<td>This command was integrated into Cisco IOS Release 12.0(21)ST.</td>
</tr>
<tr>
<td>12.0(22)S</td>
<td>This command was integrated into Cisco IOS Release 12.0(22)S.</td>
</tr>
<tr>
<td>12.2(14)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(14)S.</td>
</tr>
<tr>
<td>12.4(2)T</td>
<td>This command was replaced by the <strong>ipv6 nd ra suppress</strong> command.</td>
</tr>
</tbody>
</table>

Usage Guidelines
Use the no **ipv6 nd suppress-ra** command to enable the sending of IPv6 router advertisement transmissions on non-LAN interface types (for example, serial or tunnel interfaces).

Examples
The following example suppresses IPv6 router advertisements on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd suppress-ra
```

The following example enables the sending of IPv6 router advertisements on serial interface 0/1:

```
Router(config)# interface serial 0/1
Router(config-if)# no ipv6 nd suppress-ra
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 interface</code></td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
ipv6 neighbor binding

To change the defaults of neighbor binding entries in a binding table, use the `ipv6 neighbor binding` command in global configuration mode. To return the networking device to its default, use the `no` form of this command.

```
ipv6 neighbor binding [{reachable-lifetime value|stale-lifetime value}]
no ipv6 neighbor binding
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>reachable-lifetime value</td>
<td>(Optional) The maximum time, in seconds, an entry is considered reachable without getting a proof of reachability (direct reachability through tracking, or indirect reachability through Neighbor Discovery protocol [NDP] inspection). After that, the entry is moved to stale. The range is from 1 through 3600 seconds, and the default is 300 seconds (or 5 minutes).</td>
</tr>
<tr>
<td>stale-lifetime value</td>
<td>(Optional) The maximum time, in seconds, a stale entry is kept in the binding table before the entry is deleted or proof is received that the entry is reachable.</td>
</tr>
<tr>
<td>down-lifetime value</td>
<td>(Optional) The maximum time, in seconds, an entry learned from a down interface is kept in the binding table before the entry is deleted or proof is received that the entry is reachable.</td>
</tr>
</tbody>
</table>

**Command Default**

Reachable lifetime: 300 seconds Stale lifetime: 24 hours Down lifetime: 24 hours

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ipv6 neighbor binding` command to configure information about individual entries in a binding table. If no keywords or arguments are configured, the IPv6 neighbor binding entry defaults are used.

If the `tracking reachable-lifetime` command is configured, it overrides `ipv6 neighbor binding reachable-lifetime` configuration. If the `tracking stale-lifetime` command is configured, it overrides `ipv6 neighbor binding stale-lifetime` configuration.

**Examples**

The following example shows how to change the reachable lifetime for binding entries to 100 seconds:

```
Router(config)# ipv6 neighbor binding reachable-entries 100
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 neighbor tracking</code></td>
<td>Tracks entries in the binding table.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>tracking</td>
<td>Overrides the default tracking policy on a port.</td>
</tr>
</tbody>
</table>
ipv6 neighbor binding down-lifetime

To change the default of a neighbor binding entry’s down lifetime, use the `ipv6 neighbor binding down-lifetime` command in global configuration mode. To return the networking device to its default, use the `no` form of this command.

```
ipv6 neighbor binding down-lifetime {value|infinite}
no ipv6 neighbor binding down-lifetime
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| `value`       | The maximum time, in minutes, an entry learned from a down interface is kept in the table before deletion. The range is from 1 to 3600 minutes.  
|               | • The default is 24 hours (86,400 seconds). |
| `infinite`    | Keeps an entry in the binding table for an infinite amount of time. |

**Command Default**

A neighbor binding entry is down for 24 hours before it is deleted from the binding table.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ipv6 neighbor binding down-lifetime` command to change the amount of time a neighbor binding is down before that binding is removed from the binding table.

**Examples**

The following example shows how to change a binding entry’s down lifetime to 2 minutes before it is deleted from the binding table:

```
Router(config)# ipv6 neighbor binding down-lifetime 2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 neighbor tracking</code></td>
<td>Tracks entries in the binding table.</td>
</tr>
</tbody>
</table>
ipv6 neighbor binding logging

To enable the logging of binding table main events, use the `ipv6 neighbor binding logging` command in global configuration mode. To disable this function, use the `no` form of this command.

```
ipv6 neighbor binding logging
no ipv6 neighbor binding logging
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Binding table events are not logged.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(2)SE</td>
<td>This command was integrated into Cisco IOS Release 15.0(2)SE.</td>
</tr>
<tr>
<td>15.3(1)S</td>
<td>This command was integrated into Cisco IOS Release 15.3(1)S.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 neighbor binding logging` command enables the logging of the following binding table events:

- An entry is inserted into the binding table.
- A binding table entry was updated.
- A binding table entry was deleted from the binding table.
- A binding table entry was not inserted into the binding table, possibly because of a collision with an existing entry, or because the maximum number of entries has been reached.

**Examples**

The following example shows how to enable binding table event logging:

```
Router(config)# ipv6 neighbor binding logging
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 neighbor binding interface</td>
<td>Adds a static entry to the binding table database.</td>
</tr>
<tr>
<td>ipv6 neighbor binding vlan</td>
<td>Adds a static entry to the binding table database.</td>
</tr>
<tr>
<td>ipv6 neighbor tracking</td>
<td>Tracks entries in the binding table.</td>
</tr>
<tr>
<td>ipv6 snooping logging packet drop</td>
<td>Configures IPv6 snooping security logging.</td>
</tr>
</tbody>
</table>
**ipv6 neighbor binding max-entries**

To specify the maximum number of entries that are allowed to be inserted in the binding table cache, use the `ipv6 neighbor binding max-entries` command in global configuration mode. To return to the default, use the `no` form of this command.

```
ipv6 neighbor binding max-entries entries [vlan-limit number | interface-limit number | mac-limit number]
no ipv6 neighbor binding max-entries entries [vlan-limit | mac-limit]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>entries</th>
<th>Number of entries that can be inserted into the cache.</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-limit number</td>
<td>(Optional) Specifies a neighbor binding limit per number of VLANs.</td>
</tr>
<tr>
<td>interface-limit number</td>
<td>(Optional) Specifies a neighbor binding limit per interface.</td>
</tr>
<tr>
<td>mac-limit number</td>
<td>(Optional) Specifies a neighbor binding limit per number of Media Access Control (MAC) addresses.</td>
</tr>
</tbody>
</table>

**Command Default**

This command is disabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(2)SE</td>
<td>This command was integrated into Cisco IOS Release 15.0(2)SE.</td>
</tr>
<tr>
<td>15.3(1)S</td>
<td>This command was integrated into Cisco IOS Release 15.3(1)S.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 neighbor binding max-entries` command is used to control the content of the binding table. This command specifies the maximum number of entries that are allowed to be inserted in the binding table cache. Once this limit is reached, new entries are refused, and the Neighbor Discovery Protocol (NDP) traffic source with the new entry is dropped.

If the maximum number of entries specified is lower than the current number of entries in the database, no entries are cleared, and the new threshold is reached after normal cache attrition.

The maximum number of entries can be set globally per VLAN, interface, or MAC addresses.

**Examples**

The following example shows how to specify globally the maximum number of entries inserted into the cache:
Router(config)# ipv6 neighbor binding max-entries 100

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ipv6 neighbor binding interface</td>
<td>Adds a static entry to the binding table database.</td>
</tr>
<tr>
<td></td>
<td>ipv6 neighbor binding vlan</td>
<td>Adds a static entry to the binding table database.</td>
</tr>
<tr>
<td></td>
<td>ipv6 neighbor tracking</td>
<td>Tracks entries in the binding table.</td>
</tr>
</tbody>
</table>
ipv6 neighbor binding stale-lifetime

To set the length of time a stale entry is kept in the binding table, use the `ipv6 neighbor binding stale-lifetime` command in global configuration mode. To return to the default setting, use the `no` form of this command.

```
ipv6 neighbor binding stale-lifetime {value|infinite}
no ipv6 neighbor binding
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>The maximum time, in minutes, a stale entry is kept in the table before it is deleted or some proof of reachability is seen. The range is from 1 to 3600 minutes, and the default is 24 hours (or 1440 minutes).</td>
</tr>
<tr>
<td>infinite</td>
<td>Keeps an entry in the binding table for an infinite amount of time.</td>
</tr>
</tbody>
</table>

**Command Default**

Stale lifetime: 1440 minutes (24 hours)

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ipv6 neighbor binding stale-lifetime` command to configure the length of time a stale entry is kept in the binding table before it is removed.

**Examples**

The following example shows how to change the stale lifetime for a binding entry to 720 minutes (or 12 hours):

```
Router(config)# ipv6 neighbor binding stale lifetime 720
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 neighbor binding</td>
<td>Changes the defaults of neighbor binding entries in a binding table.</td>
</tr>
</tbody>
</table>
ipv6 neighbor binding vlan

To add a static entry to the binding table database, use the `ipv6 neighbor binding vlan` command in global configuration mode. To remove the static entry, use the `no` form of this command.

```
ipv6 neighbor binding vlan  vlan-id  [interface  type  number  ipv6-address  mac-address]  [{tracking  [{disable|enable|retry-interval  value}  ]  reachable-lifetime  value}]  
no  ipv6 neighbor binding  vlan  vlan-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan-id</code></td>
<td>ID of the specified VLAN.</td>
</tr>
<tr>
<td><code>interface  type  number</code></td>
<td>Adds static entries by the specified interface type and number.</td>
</tr>
<tr>
<td><code>ipv6-address</code></td>
<td>IPv6 address of the static entry.</td>
</tr>
<tr>
<td><code>mac-address</code></td>
<td>Media Access Control (MAC) address of the static entry.</td>
</tr>
<tr>
<td><code>tracking</code></td>
<td>(Optional) Verifies a static entry’s reachability directly.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>(Optional) Disables tracking for a particular static entry.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>(Optional) Enables tracking for a particular static entry.</td>
</tr>
<tr>
<td><code>retry-interval  value</code></td>
<td>(Optional) Verifies a static entry’s reachability, in seconds, at the configured interval. The range is from 1 to 3600, and the default is 300.</td>
</tr>
<tr>
<td><code>reachable-lifetime  value</code></td>
<td>(Optional) Specifies the maximum time, in seconds, an entry is considered reachable without getting a proof of reachability (direct reachability through tracking, or indirect reachability through Neighbor Discovery Protocol [NDP] inspection). After that, the entry is moved to stale. The range is from 1 to 3600 seconds, and the default is 300 seconds.</td>
</tr>
</tbody>
</table>

**Command Default**

- Retry interval: 300 seconds
- Reachable lifetime: 300 seconds

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(2)SE</td>
<td>This command was integrated into Cisco IOS Release 15.0(2)SE.</td>
</tr>
<tr>
<td>15.3(1)S</td>
<td>This command was integrated into Cisco IOS Release 15.3(1)S.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

The `ipv6 neighbor binding vlan` command is used to control the content of the binding table. Use this command to add a static entry in the binding table database. The binding table manager is responsible for aging out entries and verifying their reachability directly by probing them (if the `tracking` keyword is enabled). Use of the `tracking` keyword overrides any general behavior provided globally by the `ipv6 neighbor tracking` command for this static entry. The `disable` keyword disables tracking for this static entry. The `stale-lifetime` keyword defines the maximum time the entry will be kept once it is determined to be not reachable (or stale).

**Examples**

The following example shows how to change the reachable lifetime for binding entries to 100 seconds:

```
Router(config)# ipv6 neighbor binding vlan reachable-lifetime 100
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 neighbor binding max-entries</code></td>
<td>Specifies the maximum number of entries that are allowed to be inserted in the cache.</td>
</tr>
<tr>
<td><code>ipv6 neighbor tracking</code></td>
<td>Tracks entries in the binding table.</td>
</tr>
</tbody>
</table>
ipv6 neighbor tracking

To track entries in the binding table, use the `ipv6 neighbor tracking` command in global configuration mode. To disable entry tracking, use the `no` form of this command.

```bash
ipv6 neighbor tracking [retry-interval value]
no ipv6 neighbor tracking [retry-interval value]
```

**Syntax Description**

| retry-interval value | (Optional) Verifies a static entry’s reachability at the configured interval time, in seconds, between two probings. The range is from 1 to 3600, and the default is 300. |

**Command Default**

Entries in the binding table are not tracked.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.0(2)SE</td>
<td>This command was integrated into Cisco IOS Release 15.0(2)SE.</td>
</tr>
<tr>
<td>15.3(1)S</td>
<td>This command was integrated into Cisco IOS Release 15.3(1)S.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.2SE</td>
<td>This command was integrated into Cisco IOS XE Release 3.2SE.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.9S</td>
<td>This command was integrated into Cisco IOS XE Release 3.9S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 neighbor tracking` command enables the tracking of entries in the binding table. Entry reachability is tested at every interval configured by the optional `retry-interval` keyword (or every 300 seconds, which is the default retry interval) using the neighbor unreachable detection (NUD) mechanism used for directly tracking neighbor reachability.

Reachability can also be established indirectly by using Neighbor Discovery Protocol (NDP) inspection up to the VERIFY_MAX_RETRIES value (the default is 10 seconds). When there is no response, entries are considered stale and are deleted after the stale lifetime value is reached (the default is 1440 minutes).

When the `ipv6 neighbor tracking` command is disabled, entries are considered stale after the reachable lifetime value is met (the default is 300 seconds) and deleted after the stale lifetime value is met.

To change the default values of neighbor binding entries in a binding table, use the `ipv6 neighbor binding` command.

**Examples**

The following example shows how to track entries in a binding table:

```bash
Router(config)# ipv6 neighbor tracking
```
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 neighbor binding</td>
<td>Changes the defaults of neighbor binding entries in a binding table.</td>
</tr>
</tbody>
</table>
**ipv6 port-map**

To establish port-to-application mapping (PAM) for the system, use the `ipv6 port-map` command in global configuration mode. To delete user-defined PAM entries, use the `no` form of this command.

```
ipv6 port-map application port port-num [list acl-name]
no ipv6 port-map application port port-num [list acl-name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>application</code></td>
<td>Specifies the predefined application that requires port mapping.</td>
</tr>
<tr>
<td><code>port port-num</code></td>
<td>Specifies a port number. The range is from 1 to 65535.</td>
</tr>
<tr>
<td><code>list acl-name</code></td>
<td>(Optional) Specifies the name of the IPv6 access list (ACL) associated with the port mapping.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 port-map` command associates TCP or User Datagram Protocol (UDP) port numbers with applications or services, establishing a table of default port mapping information at the firewall. This information is used to support network environments that run services using ports that are different from the registered or well-known ports associated with a service or application.

The port mapping information in the PAM table is of one of three types:

- System-defined
- User-defined
- Host-specific

**System-Defined Port Mapping**

Initially, PAM creates a set of system-defined entries in the mapping table using well-known or registered port mapping information set up during the system start-up. The Cisco IOS Firewall Context-Based Access Control feature requires the system-defined mapping information to function properly. System-defined mapping information cannot be deleted or changed; that is, you cannot map HTTP services to port 21 (FTP) or FTP services to port 80 (HTTP).

The table below lists the default system-defined services and applications in the PAM table.
Table 16: System-Defined Port Mapping

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Well-Known or Registered Port Number</th>
<th>Protocol Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cuseeme</td>
<td>7648</td>
<td>CU-SeeMe Protocol</td>
</tr>
<tr>
<td>exec</td>
<td>512</td>
<td>Remote Process Execution</td>
</tr>
<tr>
<td>ftp</td>
<td>21</td>
<td>File Transfer Protocol (control port)</td>
</tr>
<tr>
<td>h323</td>
<td>1720</td>
<td>H.323 Protocol (for example, MS NetMeeting, Intel Video Phone)</td>
</tr>
<tr>
<td>http</td>
<td>80</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>login</td>
<td>513</td>
<td>Remote login</td>
</tr>
<tr>
<td>msrpc</td>
<td>135</td>
<td>Microsoft Remote Procedure Call</td>
</tr>
<tr>
<td>netshow</td>
<td>1755</td>
<td>Microsoft NetShow</td>
</tr>
<tr>
<td>real-audio-video</td>
<td>7070</td>
<td>RealAudio and RealVideo</td>
</tr>
<tr>
<td>scp</td>
<td>2000</td>
<td>Skinny Client Control Protocol (SCCP)</td>
</tr>
<tr>
<td>smtp</td>
<td>25</td>
<td>Simple Mail Transfer Protocol (SMTP)</td>
</tr>
<tr>
<td>sql-net</td>
<td>1521</td>
<td>SQL-NET</td>
</tr>
<tr>
<td>streamworks</td>
<td>1558</td>
<td>StreamWorks Protocol</td>
</tr>
<tr>
<td>sunrpc</td>
<td>111</td>
<td>SUN Remote Procedure Call</td>
</tr>
<tr>
<td>tftp</td>
<td>69</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>vdolive</td>
<td>7000</td>
<td>VDOLive Protocol</td>
</tr>
</tbody>
</table>

You can override the system-defined entries for a specific host or subnet using the `list` keyword in the `ipv6 port-map` command.

**User-Defined Port Mapping**

Network applications that use non-standard ports require user-defined entries in the mapping table. Use the `ipv6 port-map` command to create default user-defined entries in the PAM table.

To map a range of port numbers with a service or application, you must create a separate entry for each port number.

If you try to map an application to a system-defined port, a message appears warning you of a mapping conflict.
Use the **no** form of the `ipv6 port-map` command to delete user-defined entries from the PAM table.

To overwrite an existing user-defined port mapping, use the `ipv6 port-map` command to associate another service or application with the specific port.

**Host-Specific Port Mapping**

User-defined entries in the mapping table can include host-specific mapping information, which establishes port mapping information for specific hosts or subnets. In some environments, it might be necessary to override the default port mapping information for a specific host or subnet, including a system-defined default port mapping information. Use the **list** keyword for the `ipv6 port-map` command to specify an ACL for a host or subnet that uses PAM.

---

**Note**

If the host-specific port mapping information is the same as existing system-defined or user-defined default entries, host-specific port changes have no effect.

---

**Examples**

The following user-defined port-mapping configuration map port 8080 to the HTTP application:

```
ipv6 port-map http port 8080
```

Host-specific port-mapping configuration maps port 2121 to the FTP application from a particular set of host. First, the user needs to create a permit IPv6 access list for the allowed host(s). In the following example, packets from the hosts in the 2001:0DB8:1:7 subset destined for port 2121 will be mapped to the FTP application:

```
Router(config)# ipv6 access-list ftp-host
Router(config-ipv6-acl)# permit 2001:0DB8:1:7::/64 any
```

The port-map configuration is then configured as follows:

```
Router(config)# ipv6 port-map ftp port 2121 list ftp-host
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 port-map</code></td>
<td>Displays IPv6 port-mapping information.</td>
</tr>
</tbody>
</table>
ipv6 radius source-interface

To specify an interface to use for the source address in RADIUS packets, use the `ipv6 radius source-interface` command in global configuration mode. To remove the specified interface from the configuration, use the `no` form of this command.

```
ipv6 radius source-interface interface vrf vrf-name
no ipv6 radius source-interface interface
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Interface to be used for the source address in RADIUS packets.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>VPN routing/forwarding parameter name.</td>
</tr>
</tbody>
</table>

**Command Default**

No interface is specified.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.2S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>The <code>vrf vrf-name</code> keyword-argument pair was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 radius source-interface` command specifies an interface to use for the source address in RADIUS packets.

**Examples**

The following example shows how to configure the Gigabit Ethernet interface to be used as the source address in RADIUS packets:

```
Router(config)# ipv6 radius source-interface GigabitEthernet 0/0/0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius server</td>
<td>Configures the RADIUS server for IPv6 or IPv4 and enters RADIUS server configuration mode.</td>
</tr>
</tbody>
</table>
**ipv6 routing-enforcement-header loose**

To provide backward compatibility with legacy IPv6 inspection, use the `ipv6 routing-enforcement-header loose` command in parameter map type inspect configuration mode. To disable this feature, use the `no` form of this command.

```
ipv6 routing-enforcement-header loose
no ipv6 routing-enforcement-header loose
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Backward compatibility is not provided.

**Command Modes**

parameter map type inspect configuration mode (config-profile)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(2)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 routing-enforcement-header loose` command provides backward compatibility with legacy IPv6 inspection. Enabling this command ensures that the firewall will not drop IPv6 traffic with routing headers. The default firewall behavior is to drop all IPv6 traffic without a routing header.

**Examples**

The following example enables backward compatibility with legacy IPv6 inspection on an inspect type parameter map named `v6-param-map`:

```
Router(config)# parameter-map type inspect v6-param-map
Router (config-profile)# ipv6 routing-header-enforcement loose
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>parameter-map type inspect</td>
<td>Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the <code>inspect</code> action.</td>
</tr>
</tbody>
</table>
ipv6 snooping logging packet drop

To enable the logging of dropped packets by the IPv6 first-hop security feature, use the `ipv6 snooping logging packet drop` command in global configuration mode. To disable the logging of dropped packets by the IPv6 first-hop security feature, use the `no` form of this command.

```
ipv6 snooping logging packet drop
no ipv6 snooping logging packet drop
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Snooping security logging is not enabled.

**Command Modes**
Global configuration (config)#

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `ipv6 snooping logging packet drop` command to log packets that are dropped when they are received on an unauthorized port. For example, this command will log RA packets that are dropped because of the RA guard feature.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 neighbor binding logging</td>
<td>Enables the logging of binding table main events.</td>
</tr>
</tbody>
</table>
ipv6 tacacs source-interface

To specify an interface to use for the source address in TACACS packets, use the `ipv6 tacacs source-interface` command in global configuration mode. To remove the specified interface from the configuration, use the `no` form of this command.

```
ipv6 tacacs source-interface interface vrf vrf-name
no ipv6 tacacs source-interface interface
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>Interface to be used for the source address in TACACS packets.</td>
</tr>
<tr>
<td><code>vrf</code></td>
<td>VPN routing/forwarding parameter name.</td>
</tr>
<tr>
<td><code>vrf-name</code></td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

No interface is specified.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.2S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>The <code>vrf vrf-name</code> keyword-argument pair was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 tacacs source-interface` command specifies an interface to use for the source address in TACACS packets.

**Examples**

The following example shows how to configure the Gigabit Ethernet interface to be used as the source address in TACACS packets:

```
Router(config)# ipv6 tacacs source-interface GigabitEthernet 0/0/0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tacacs server</td>
<td>Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.</td>
</tr>
</tbody>
</table>
ipv6 virtual-reassembly

To enable Virtual Fragment Reassembly (VFR) on an interface, use the `ipv6 virtual-reassembly` command in global configuration mode. To remove VFR configuration, use the `no` form of this command.

```
ipv6 virtual-reassembly [ { in | out } ] [ max-reassemblies maxreassemblies ] [ max-fragments max-fragments ] [ timeout seconds ] [ drop-fragments ]
no ipv6 virtual-reassembly [ { in | out } ] [ max-reassemblies maxreassemblies ] [ max-fragments max-fragments ] [ timeout seconds ] [ drop-fragments ]
```

**Syntax Description**

- **in** (Optional) Enables VFR on the ingress direction of the interface.
- **out** (Optional) Enables VFR on the egress direction of the interface.
- **max-reassemblies** (Optional) Sets the maximum number of concurrent reassemblies (fragment sets) that the Cisco IOS software can handle at a time. The default value is 64.
- **max-fragments** (Optional) Sets the maximum number of fragments allowed per datagram (fragment set). The default is 16.
- **timeout** (Optional) Sets the timeout value of the fragment state. The default timeout value is 2 seconds. If a datagram does not receive all its fragments within 2 seconds, all of the fragments received previously will be dropped and the fragment state will be deleted.
- **drop-fragments** (Optional) Turns the drop fragments feature on or off.

**Command Default**

Max-reassembles = 64 Fragments = 16 If neither the `in` or `out` keyword is specified, VFR is enabled on the ingress direction of the interface only. `drop-fragments` keyword is not enabled.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.1(1)T</td>
<td>The <code>in</code> and <code>out</code> keywords were added.</td>
</tr>
<tr>
<td></td>
<td>• The <code>out</code> keyword must be used to configure or disable the egress direction</td>
</tr>
<tr>
<td></td>
<td>of the interface.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.4S</td>
<td>The <code>drop-fragments</code> keyword was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the `ipv6 virtual-reassembly` command is configured on an interface without using one of the command keywords, VFR is enabled on the ingress direction of the interface only. In Cisco IOS XE Release 3.4S, all VFR-related alert messages are suppressed by default.

**Maximum Number of Reassemblies**
Whenever the maximum number of 256 reassemblies (fragment sets) is crossed, all the fragments in the forthcoming fragment set will be dropped and an alert message VFR-4-FRAG_TABLE_OVERFLOW will be logged to the syslog server.

**Maximum Number of Fragments per Fragment Set**

If a datagram being reassembled receives more than eight fragments then, tall fragments will be dropped and an alert message VFR-4-TOO_MANY_FRAGMENTS will be logged to the syslog server.

**Explicit Removal of Egress Configuration**

As of the Cisco IOS 15.1(1)T release, the `no ipv6 virtual-reassembly` command, when used without keywords, removes ingress configuration only. To remove egress interface configuration, you must enter the `out` keyword.

**Examples**

The following example configures the ingress direction on the interface. It sets the maximum number of reassemblies to 32, maximum fragments to 4, and the timeout to 7 seconds:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ipv6 virtual-reassembly max-reassemblies 32 max-fragments 4 timeout 7
```

The following example enables the VFR on the ingress direction of the interface. Note that even if the `in` keyword is not used, the configuration default is to configure the ingress direction on the interface:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ipv6 virtual-reassembly
Router(config-if)# end
Router# show run interface Ethernet 0/0
interface Ethernet0/0
no ip address
ipv6 virtual-reassembly in
```

The following example enables egress configuration on the interface. Note that the `out` keyword must be used to enable and disable egress configuration on the interface:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ipv6 virtual-reassembly out
Router(config-if)# end
Router# show run interface Ethernet 0/0
interface Ethernet0/0
no ip address
ipv6 virtual-reassembly out
end
```

The following example disables egress configuration on the interface:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# no ipv6 virtual-reassembly out
Router(config-if)# end
```
ipv6 virtual-reassembly drop-fragments

To drop all fragments on an interface, use the ipv6 virtual-reassembly drop-fragments command in global configuration mode. Use the no form of this command to remove the packet-dropping behavior.

ipv6 virtual-reassembly drop-fragments
no ipv6 virtual-reassembly drop-fragments

Syntax Description

This command has no arguments or keywords.

Command Default

Fragments on an interface are not dropped.

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following example causes all fragments on an interface to be dropped:

ipv6 virtual-reassembly drop-fragments
ipv6 vrf forwarding

To configure the Virtual Private Network (VPN) routing and forwarding (VRF) parameters to use with the TACACS+ server group, use the `ipv6 vrf forwarding` command in TACACS+ server-group configuration mode. To enable server groups to use the global (default) routing table, use the `no` form of this command.

```
ipv6 vrf forwarding vrf-name
no ipv6 vrf forwarding vrf-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf-name</code></td>
<td>Name assigned to a VRF</td>
</tr>
</tbody>
</table>

**Command Default**

Server groups use the global routing table.

**Command Modes**

TACACS+ server-group configuration (config-sg-tacacs+)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ipv6 vrf forwarding` command to specify a VRF for a TACACS+ server group.

**Examples**

The following example shows how to configure the VRF user to reference the TACACS+ server in the server group tacacs1:

```
aaa group server tacacs+tacacs1
  server-private 10.1.1.1 port 19 key cisco
  ipv6 vrf forwarding cisco
  ip tacacs source-interface Loopback0
  ip vrf cisco
  rd 100:1
  interface Loopback0
  ip address 10.0.0.2 255.0.0.0
  ipv6 vrf forwarding cisco
```

The following example shows a scenario where the `ipv6 vrf forwarding` command is used to choose one of the global source interfaces configured if the source interface is not configured under the server group:

Example:

**Global configurations:**

```
ip radius source-interface Loopback0 vrf RED
ip radius source-interface Loopback1 vrf BLUE
ip radius source-interface Loopback2 vrf GREEN
```

**Server Group configuration: Case 1**

```
aaa group server radius radius-group1
ipv6 vrf forwarding RED
ipv6 radius source-interface Loopback0
>>> Here Loopback0 is considered as the source-interface.
```

**Server Group configuration: Case 2**

```
```
aaa group server radius radius-group1
ipv6 vrf forwarding BLUE

As the source interface is not mentioned under the server group, the command checks for the vrf forwarding configured with the group and checks for the global source interface configurations associated with vrf BLUE, which is Loopback1, so here Loopback1 is used as the source interface.

Server Group configuration: Case 3
aaa group server radius radius-group1
ipv6 vrf forwarding GREEN

Loopback2 is considered as the source-interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa group server radius</td>
<td>Groups different RADIUS server hosts into distinct lists and distinct methods.</td>
</tr>
<tr>
<td>ip tacacs source-interface</td>
<td>Uses the IP address of a specified interface for all outgoing TACACS+ packets.</td>
</tr>
<tr>
<td>ip vrf forwarding (server-group)</td>
<td>Configures the VRF reference of an AAA RADIUS or TACACS+ server group.</td>
</tr>
<tr>
<td>server-private</td>
<td>Configures the IP address of the private RADIUS server for the group server.</td>
</tr>
</tbody>
</table>
isakmp authorization list

To configure an Internet Key Exchange (IKE) shared secret using the authentication, authorization, and accounting (AAA) server in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the `isakmp authorization list` command in ISAKMP profile configuration mode. To disable the shared secret, use the `no` form of this command.

```
isakmp authorization list list-name
no isakmp authorization list list-name
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list-name</td>
<td>AAA authorization list used for configuration mode attributes or preshared keys for aggressive mode.</td>
</tr>
</tbody>
</table>

| Command Default       | No default behaviors or values                                             |

| Command Modes         | ISAKMP profile configuration (config-isa-prof)                             |

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.2(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.2(18)SXD</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXD.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 2.6</td>
<td>This command was integrated into Cisco IOS XE Release 2.6.</td>
</tr>
</tbody>
</table>

| Usage Guidelines   | This command allows you to retrieve a shared secret from an AAA server.     |

<table>
<thead>
<tr>
<th>Examples</th>
<th>The following example shows that an IKE shared secret is configured using an AAA server on a router:</th>
</tr>
</thead>
</table>
|                    | crypto isakmp profile vpnprofile
|                    | isakmp authorization list ikessaaalist                                                          |

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa authorization</td>
<td>Sets parameters that restrict user access to a network.</td>
</tr>
</tbody>
</table>
**issuer-name**

To specify the distinguished name (DN) as the certification authority (CA) issuer name for the certificate server, use the `issuer-name` command in certificate server configuration mode. To clear the issuer name and return to the default, use the `no` form of this command.

```
issuer-name  DN-string
no  issuer-name  DN-string
```

**Syntax Description**

| DN-string | Name of the DN string. |

**Command Default**

If the issuer name is not configured, the DN string is the certificate server name.

**Command Modes**

Certificate server configuration (cs-server)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must configure the `crypto pki server` command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

The DN-string value cannot be changed after the certificate server generates its signed certificate.

**Examples**

The following example shows how to define an issuer name for the certificate server “mycertserver”:

```
Router(config)#  ip http server
Router(config)#  crypto pki server mycertserver
Router(cs-server)#  database level minimal
Router(cs-server)#  database url nvram:
Router(cs-server)#  issuer-name CN = ipsec_cs,L = My Town,C = US
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-rollover</td>
<td>Enables the automated CA certificate rollover functionality.</td>
</tr>
<tr>
<td>cdp-url</td>
<td>Specifies a CDP to be used in certificates that are issued by the certificate server.</td>
</tr>
<tr>
<td>crl (cs-server)</td>
<td>Specifies the CRL PKI CS.</td>
</tr>
<tr>
<td>crypto pki server</td>
<td>Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>database archive</td>
<td>Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.</td>
</tr>
<tr>
<td>database level</td>
<td>Controls what type of data is stored in the certificate enrollment database.</td>
</tr>
<tr>
<td>database url</td>
<td>Specifies the location where database entries for the CS is stored or published.</td>
</tr>
<tr>
<td>database username</td>
<td>Specifies the requirement of a username or password to be issued when accessing the primary database location.</td>
</tr>
<tr>
<td>default (cs-server)</td>
<td>Resets the value of the CS configuration command to its default.</td>
</tr>
<tr>
<td>grant auto rollover</td>
<td>Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.</td>
</tr>
<tr>
<td>grant auto trustpoint</td>
<td>Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.</td>
</tr>
<tr>
<td>grant none</td>
<td>Specifies all certificate requests to be rejected.</td>
</tr>
<tr>
<td>grant ra-auto</td>
<td>Specifies that all enrollment requests from an RA be granted automatically.</td>
</tr>
<tr>
<td>hash (cs-server)</td>
<td>Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.</td>
</tr>
<tr>
<td>lifetime (cs-server)</td>
<td>Specifies the lifetime of the CA or a certificate.</td>
</tr>
<tr>
<td>mode ra</td>
<td>Enters the PKI server into RA certificate server mode.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>mode sub-cs</td>
<td>Enters the PKI server into sub-certificate server mode</td>
</tr>
<tr>
<td>redundancy (cs-server)</td>
<td>Specifies that the active CS is synchronized to the standby CS.</td>
</tr>
<tr>
<td>serial-number (cs-server)</td>
<td>Specifies whether the router serial number should be included in the certificate request.</td>
</tr>
<tr>
<td>show (cs-server)</td>
<td>Displays the PKI CS configuration.</td>
</tr>
<tr>
<td>shutdown (cs-server)</td>
<td>Allows a CS to be disabled without removing the configuration.</td>
</tr>
</tbody>
</table>
**ivrf**

To specify a user-defined VPN routing and forwarding (VRF) or use the global VRF, use the `ivrf` command in IKEv2 profile configuration mode. To delete the VRF specification, use the `no` form of this command.

`ivrf name`

`no ivrf`

**Syntax Description**

<table>
<thead>
<tr>
<th>name</th>
<th>VRF name</th>
</tr>
</thead>
</table>

**Command Default**

VRF is not specified.

**Command Modes**

IKEv2 profile configuration (config-ikev2-profile)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to specify a user-defined VRF or a global VRF, which should be attached to static and dynamic crypto maps. The inside VRF (IVRF) for a tunnel interface should be configured on the tunnel interface. IVRF specifies the VRF for cleartext packets. The default value for IVRF is Forward VRF (FVRF).

**Examples**

The following example shows how to specify IVRF:

```
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# ivrf vrf1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2 profile</td>
<td>Defines an IKEv2 profile.</td>
</tr>
<tr>
<td>show crypto ikev2 profile</td>
<td>Displays the IKEv2 profile.</td>
</tr>
</tbody>
</table>
K through L

- keepalive (isakmp profile), on page 803
- kerberos clients mandatory, on page 804
- kerberos credentials forward, on page 805
- kerberos instance map, on page 806
- kerberos local-realm, on page 807
- kerberos password, on page 808
- kerberos preauth, on page 809
- kerberos processes, on page 811
- kerberos realm, on page 812
- kerberos retry, on page 814
- kerberos server, on page 815
- kerberos srvtab entry, on page 817
- kerberos srvtab remote, on page 819
- kerberos timeout, on page 820
- key (config-radius-server), on page 821
- key (isakmp-group), on page 823
- key (TACACS+), on page 824
- key config-key, on page 825
- key config-key password-encryption, on page 826
- key-hash, on page 828
- keyring, on page 829
- keyring (IKEv2 profile), on page 830
- key-set, on page 832
- key-string (IKE), on page 834
- key-string (SSH), on page 836
- language, on page 837
- ldap attribute-map, on page 838
- ldap search, on page 839
- ldap server, on page 840
- length (RITE), on page 841
- license (parameter-map), on page 843
- lifetime (cs-server), on page 844
- lifetime (IKE policy), on page 847
• lifetime (IKEv2 profile), on page 849
• lifetime crl, on page 850
• lifetime enrollment-request, on page 851
• limit address-count, on page 852
• list (LSP Attributes), on page 853
• list (WebVPN), on page 854
• li-view, on page 855
• load-balance (server-group), on page 857
• load classification, on page 861
• local-address, on page 865
• local-port (WebVPN), on page 867
• local priority, on page 869
• lockdown (LSP Attributes), on page 871
• log (policy-map), on page 872
• log (parameter-map type), on page 873
• log (type access-control), on page 875
• logging (parameter-map), on page 877
• logging dmvpn, on page 878
• logging enabled, on page 880
• logging ip access-list cache (global configuration), on page 881
• logging ip access-list cache (interface configuration), on page 883
• login authentication, on page 885
• login-auth-bypass, on page 887
• login block-for, on page 888
• login delay, on page 891
• login-message, on page 893
• login quiet-mode access-class, on page 894
• login-photo, on page 896
• logo, on page 897
keepalive (isakmp profile)

To allow the gateway to send dead peer detection (DPD) messages to the peer, use the `keepalive` command in Internet Security Association Key Management Protocol (ISAKMP) profile configuration mode. To return to the default, use the `no` form of this command.

```
keepalive seconds retry retry-seconds
no keepalive seconds retry retry-seconds
```

**Syntax Description**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>Number of seconds between DPD messages. Range is from 10 to 3600 seconds.</td>
</tr>
<tr>
<td><code>retry</code></td>
<td>Number of seconds between retries if DPD message fails. Range is from 2 to 60 seconds.</td>
</tr>
</tbody>
</table>

**Command Default**

If this command is not configured, a DPD message is not sent to the client.

**Command Modes**

ISAKMP profile configuration (config-isa-prof)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.6</td>
<td>This command was integrated into Cisco IOS XE Release 2.6.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to enable the gateway (instead of the client) to send DPD messages to the client. Internet Key Exchange (IKE) DPD is a new keepalive scheme that sends messages to let the router know that the client is still connected.

**Examples**

The following example shows that DPD messages have been configured to be sent every 60 seconds and every 5 seconds between retries if the peer does not respond:

```
crypto isakmp profile vpnprofile
keepalive 60 retry 5
```
kerberos clients mandatory

To cause the `rsh`, `rcp`, `rlogin`, and `telnet` commands to fail if they cannot negotiate the Kerberos protocol with the remote server, use the `kerberos clients mandatory` command in global configuration mode. To make Kerberos optional, use the `no` form of this command.

```
kerberos clients mandatory
no kerberos clients mandatory
```

### Syntax Description

This command has no arguments or keywords.

### Command Default

Disabled

### Command Modes

Global configuration

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td></td>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If this command is not configured and the user has Kerberos credentials stored locally, the `rsh`, `rcp`, `rlogin`, and `telnet` commands attempt to negotiate the Kerberos protocol with the remote server and will use the non-Kerberized protocols if unsuccessful.

If this command is not configured and the user has no Kerberos credentials, the standard protocols for `rcp` and `rsh` are used to negotiate.

### Examples

The following example causes the `rsh`, `rcp`, `rlogin`, and `telnet` commands to fail if they cannot negotiate the Kerberos protocol with the remote server:

```
kerberos clients mandatory
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>connect</code></td>
<td>Logs in to a host that supports Telnet, rlogin, or LAT.</td>
</tr>
<tr>
<td><code>kerberos credentials forward</code></td>
<td>Forces all network application clients on the router to forward the Kerberos credentials of users upon successful Kerberos authentication.</td>
</tr>
<tr>
<td><code>rlogin</code></td>
<td>Logs in to a UNIX host using rlogin.</td>
</tr>
<tr>
<td><code>rsh</code></td>
<td>Executes a command remotely on a remote rsh host.</td>
</tr>
<tr>
<td><code>telnet</code></td>
<td>Logs in to a host that supports Telnet.</td>
</tr>
</tbody>
</table>
**kerberos credentials forward**

To force all network application clients on the router to forward users’ Kerberos credentials upon successful Kerberos authentication, use the `kerberos credentials forward` command in global configuration mode. To turn off forwarding of Kerberos credentials, use the `no` form of this command.

```
kerberos credentials forward
no kerberos credentials forward
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Disabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Enable credentials forwarding to have users’ ticket granting tickets (TGTs) forwarded to the host on which they authenticate. In this way, users can connect to multiple hosts in the Kerberos realm without running the KINIT program each time they need to get a TGT.

**Examples**

The following example forces all network application clients on the router to forward users’ Kerberos credentials upon successful Kerberos authentication:

```
kerberos credentials forward
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connect</td>
<td>Logs in to a host that supports Telnet, rlogin, or LAT.</td>
</tr>
<tr>
<td>rlogin</td>
<td>Logs in to a UNIX host using rlogin.</td>
</tr>
<tr>
<td>rsh</td>
<td>Executes a command remotely on a remote rsh host.</td>
</tr>
<tr>
<td>telnet</td>
<td>Logs in to a host that supports Telnet.</td>
</tr>
</tbody>
</table>
**kerberos instance map**

To map Kerberos instances to Cisco IOS privilege levels, use the `kerberos instance map` command in global configuration mode. To remove a Kerberos instance map, use the `no` form of this command.

```
kerberos instance map instance privilege-level
no kerberos instance map instance
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance</td>
<td>Name of a Kerberos instance.</td>
</tr>
<tr>
<td>privilege-level</td>
<td>The privilege level at which a user is set if the user’s Kerberos principal contains the matching Kerberos instance. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges.</td>
</tr>
</tbody>
</table>

**Command Default**

Privilege level 1

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to create user instances with access to administrative commands.

**Examples**

The following example sets the privilege level to 15 for authenticated Kerberos users with the `admin` instance in Kerberos realm:

```
kerberos instance map admin 15
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa authorization</code></td>
<td>Sets parameters that restrict user access to a network.</td>
</tr>
</tbody>
</table>
kerberos local-realm

To specify the Kerberos realm in which the router is located, use the **kerberos local-realm** command in global configuration mode. To remove the specified Kerberos realm from this router, use the **no** form of this command.

```
kerberos local-realm kerberos-realm
no kerberos local-realm
```

**Syntax Description**

```
kerberos-realm 
```

The name of the default Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters.

**Command Default**

Disabled

**Command Modes**

Global configuration

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

The router can be located in more than one realm at a time. However, there can only be one instance of Kerberos local-realm. The realm specified with this command is the default realm.

**Examples**

The following example specify the Kerberos realm in which the router is located as EXAMPLE.COM:

```
kerberos local-realm EXAMPLE.COM
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kerberos preauth</td>
<td>Specifies a preauthentication method to use to communicate with the KDC.</td>
</tr>
<tr>
<td>kerberos realm</td>
<td>Maps a host name or DNS domain to a Kerberos realm.</td>
</tr>
<tr>
<td>kerberos server</td>
<td>Specifies the location of the Kerberos server for a given Kerberos realm.</td>
</tr>
<tr>
<td>kerberos srvtab entry</td>
<td>Specifies a krb5 SRVTAB entry.</td>
</tr>
<tr>
<td>kerberos srvtab remote</td>
<td>Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.</td>
</tr>
</tbody>
</table>
To set the password shared with the key distribution center, use the **kerberos password** command in global configuration mode. To disable the configured password, use the **no** form of this command.

**Syntax**

```
kerberos password [text-string]
no kerberos password [text-string]
```

**Syntax Description**

- **text-string**: (Optional) The password string.

**Command Default**

The password is not set.

**Command Modes**

Global configuration (config)

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
<tr>
<td>2.1</td>
<td></td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

Kerberos is a network authentication protocol that allows a secured way of node communication in a nonsecure network.

**Examples**

The following example shows how to set the password:

```
Router# configure terminal
Router(config)# kerberos password treas123
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kerberos clients mandatory</td>
<td>Specifies the default direction of filters from RADIUS.</td>
</tr>
<tr>
<td>kerberos credentials forward</td>
<td>Forces all network application clients on the router to forward the Kerberos credentials of users upon successful Kerberos authentication.</td>
</tr>
</tbody>
</table>
**kerberos preauth**

To specify a preauthentication method to use to communicate with the key distribution center (KDC), use the `kerberos preauth` command in global configuration mode. To disable Kerberos preauthentication, use the `no` form of this command.

```
kerberos preauth [encrypted-unix-timestamp|encrypted-kerberos-timestamp|none]
```

**no kerberos preauth**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>encrypted-unix-timestamp</code></td>
<td>(Optional) Use an encrypted UNIX timestamp as a quick authentication method when communicating with the KDC.</td>
</tr>
<tr>
<td><code>encrypted-kerberos-timestamp</code></td>
<td>(Optional) Use the RFC1510 kerberos timestamp as a quick authentication method when communicating with the KDC.</td>
</tr>
<tr>
<td><code>none</code></td>
<td>(Optional) Do not use Kerberos preauthentication.</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

It is more secure to use a preauthentication for communications with the KDC. However, communication with the KDC will fail if the KDC does not support this particular version of `kerberos preauth`. If that happens, turn off the preauthentication with the `none` option.

The `no` form of this command is equivalent to using the `none` keyword.

**Examples**

The following example enables Kerberos preauthentication:

```
kerberos preauth encrypted-unix-timestamp
```

The following example disables Kerberos preauthentication:

```
kerberos preauth none
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>kerberos local-realm</code></td>
<td>Specifies the Kerberos realm in which the router is located.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>kerberos server</td>
<td>Specifies the location of the Kerberos server for a given Kerberos realm.</td>
</tr>
<tr>
<td>kerberos srvtab entry</td>
<td>Specifies a krb5 SRVTAB entry.</td>
</tr>
<tr>
<td>kerberos srvtab remote</td>
<td>Retrieves a SRVTAB file from a remote host and automatically generate a</td>
</tr>
<tr>
<td></td>
<td>Kerberos SRVTAB entry configuration.</td>
</tr>
</tbody>
</table>
kerberos processes

To set the number of kerberos processes to service requests, use the `kerberos processes` command in global configuration mode. To disable the configuration, use the `no` form of this command.

```
kerberos processes number
no kerberos processes
```

**Syntax Description**

`number` Number of processes. The range is from 1 to 10. The default is 1.

**Command Default**

The default process is 1.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the number of kerberos processes to 10:

```
Router# configure terminal
Router(config)# kerberos processes 10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug kerberos</code></td>
<td>Displays information associated with the Kerberos Authentication Subsystem.</td>
</tr>
</tbody>
</table>
**kerberos realm**

To map a host name or Domain Name System (DNS) domain to a Kerberos realm, use the `kerberos realm` command in global configuration mode. To remove a Kerberos realm map, use the `no` form of this command.

```
kerberos realm {dns-domain|host} kerberos-realm
no kerberos realm {dns-domain|host} kerberos-realm
```

**Syntax Description**

- `dns-domain`: Name of a DNS domain or host.
- `host`: Name of a DNS host.
- `kerberos-realm`: Name of the Kerberos realm to which the specified domain or host belongs.

**Command Default**

Disabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

DNS domains are specified with a leading dot (.) character; host names cannot begin with a dot (.) character. There can be multiple entries of this line.

A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters. The router can be located in more than one realm at a time. Kerberos realm names must be in all uppercase characters.

**Examples**

The following example maps the domain name “example.com” to the Kerberos realm, EXAMPLE.COM:

```
kerberos realm .example.com EXAMPLE.COM
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>kerberos local-realm</code></td>
<td>Specifies the Kerberos realm in which the router is located.</td>
</tr>
<tr>
<td><code>kerberos server</code></td>
<td>Specifies the location of the Kerberos server for a given Kerberos realm.</td>
</tr>
<tr>
<td><code>kerberos srvtab entry</code></td>
<td>Specifies a krb5 SRVTAB entry.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>kerberos srvtab remote</td>
<td>Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.</td>
</tr>
</tbody>
</table>
kerberos retry

To configure the number of retry attempts for the key distribution center (KDC) sessions, use the `kerberos retry` command in global configuration mode. To return to the default setting (4 retries), use the `no` form of this command.

```
kerberos retry number
no kerberos retry
```

**Syntax Description**

- `number`: Number of retry attempts. The range is from 1 to 5. The default value is 4.

**Command Default**

The default value is four retry attempts.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When multiple KDCs are configured, there is no way to control the timeout so that failover occurs. This causes common client applications to fail before the next KDC is contacted. Therefore, the `kerberos retry` command enables you to establish stable communication with the KDCs.

**Examples**

The following example shows how to configure the retry value for the KDC session:

```
Router> enable
Router# configure terminal
Router(config)# kerberos retry 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kerberos clients mandatory</td>
<td>Causes the <code>rsh</code>, <code>rcp</code>, <code>rlogin</code>, and <code>telnet</code> commands to fail if they cannot negotiate the Kerberos protocol with the remote server.</td>
</tr>
<tr>
<td>kerberos credentials forward</td>
<td>Forces all network application clients on the router to forward users’ Kerberos credentials upon successful Kerberos authentication.</td>
</tr>
</tbody>
</table>
kerberos server

To specify the location of the Kerberos server for a given Kerberos realm, use the `kerberos server` command in global configuration mode. To remove a Kerberos server for a specified Kerberos realm, use the `no` form of this command.

```
kerberos server kerberos-realm \{host-name\}ip-address \{port-number\}
no kerberos server kerberos-realm \{host-name\}ip-address
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kerberos-realm</td>
<td>Name of the Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase letters.</td>
</tr>
<tr>
<td>host-name</td>
<td>Name of the host functioning as a Kerberos server for the specified Kerberos realm (translated into an IP address at the time of entry).</td>
</tr>
<tr>
<td>ip-address</td>
<td>IP address of the host functioning as the Kerberos server for the specified Kerberos realm.</td>
</tr>
<tr>
<td>port-number</td>
<td>(Optional) Port that the key distribution center (KDC) monitors (defaults to 88).</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `kerberos server` command to specify the location of the Kerberos server for a given realm.

**Examples**

The following example specifies 192.168.47.66 as the Kerberos server for the Kerberos realm EXAMPLE.COM:

```
kerberos server EXAMPLE.COM 192.168.47.66
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kerberos local-realm</td>
<td>Specifies the Kerberos realm in which the router is located.</td>
</tr>
<tr>
<td>kerberos realm</td>
<td>Maps a host name or DNS domain to a Kerberos realm.</td>
</tr>
<tr>
<td>kerberos srvtab entry</td>
<td>Specifies a krb5 SRVTAB entry.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>kerberos srvtab remote</td>
<td>Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.</td>
</tr>
</tbody>
</table>
kerberos srvtab entry

To retrieve a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration, use the kerberos srvtab entry command in global configuration mode. To remove a SRVTAB entry from the router’s configuration, use the no form of this command.

**Syntax Description**

<table>
<thead>
<tr>
<th>kerberos-principal</th>
<th>A service on the router.</th>
</tr>
</thead>
<tbody>
<tr>
<td>principal-type</td>
<td>Version of the Kerberos SRVTAB.</td>
</tr>
<tr>
<td>timestamp</td>
<td>Number representing the date and time the SRVTAB entry was created.</td>
</tr>
<tr>
<td>key-version number</td>
<td>Version of the encryption key format.</td>
</tr>
<tr>
<td>key-type</td>
<td>Type of encryption used.</td>
</tr>
<tr>
<td>key-length</td>
<td>Length, in bytes, of the encryption key.</td>
</tr>
<tr>
<td>encrypted-keytab</td>
<td>Secret key the router shares with the key distribution center (KDC). It is encrypted with the private Data Encryption Standard (DES) key (if available) when you write out your configuration.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you use the kerberos srvtab remote command to copy the SRVTAB file from a remote host (generally the KDC), it parses the information in this file and stores it in the router’s running configuration in the kerberos srvtab entry format. The key for each SRVTAB entry is encrypted with a private DES key if one is defined on the router. To ensure that the SRVTAB is available (that is, that it does not need to be acquired from the KDC) when you reboot the router, use the write memory router configuration command to write the router’s running configuration to NVRAM.

If you reload a configuration, with a SRVTAB encrypted with a private DES key, on to a router that does not have a private DES key defined, the router displays a message informing you that the SRVTAB entry has been corrupted, and discards the entry.
If you change the private DES key and reload an old version of the router’s configuration that contains SRVTAB entries encrypted with the old private DES keys, the router will restore your Kerberos SRVTAB entries, but the SRVTAB keys will be corrupted. In this case, you must delete your old Kerberos SRVTAB entries and reload your Kerberos SRVTABs on the router using the `kerberos srvtab remote` command.

Although you can configure `kerberos srvtab entry` on the router manually, generally you would not do this because the keytab is encrypted automatically by the router when you copy the SRVTAB using the `kerberos srvtab remote` command.

**Examples**

In the following example, `host/new-router.example.com@EXAMPLE.COM` is the host, `0` is the type, `817680774` is the timestamp, `1` is the version of the key, `1` indicates the DES is the encryption type, `8` is the number of bytes, and `.cCN.YoU.okK` is the encrypted key:

```
kerberos srvtab entry host/new-router.example.com@EXAMPLE.COM 0 817680774 1 1 8 .cCN.YoU.okK
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>kerberos srvtab remote</code></td>
<td>Retrieves a krb5 SRVTAB file from the specified host.</td>
</tr>
<tr>
<td><code>key config-key</code></td>
<td>Defines a private DES key for the router.</td>
</tr>
</tbody>
</table>
kerberos srvtab remote

To retrieve a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration, use the kerberos srvtab remote command in global configuration mode.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Machine that has the Kerberos SRVTAB file.</td>
</tr>
<tr>
<td>ip-address</td>
<td>IP address of the machine that has the Kerberos SRVTAB file.</td>
</tr>
<tr>
<td>filename</td>
<td>Name of the SRVTAB file.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you use the `kerberos srvtab remote` command to copy the SRVTAB file from the remote host (generally the key distribution center [KDC]), it parses the information in this file and stores it in the router’s running configuration in the `kerberos srvtab entry` format. The key for each SRVTAB entry is encrypted with the private Data Encryption Standard (DES) key if one is defined on the router. To ensure that the SRVTAB is available (that is, that it does not need to be acquired from the KDC) when you reboot the router, use the `write memory` configuration command to write the router’s running configuration to NVRAM.

**Examples**

The following example copies the SRVTAB file residing on b1.example.com to a router named s1.example.com:

```
kerberos srvtab remote tftp://b1.example.com/s1.example.com-new-srvtab
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>kerberos srvtab entry</code></td>
<td>Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.</td>
</tr>
<tr>
<td><code>key config-key</code></td>
<td>Defines a private DES key for the router.</td>
</tr>
</tbody>
</table>
**kerberos timeout**

To configure the timeout for key distribution center (KDC) requests, use the `kerberos timeout` command in global configuration mode. To return to the default setting (5 seconds), use the `no` form of this command.

```
kerberos timeout seconds
no kerberos timeout
```

**Syntax Description**

| seconds | Timeout, in seconds, for KDC requests. The value range is from 1 to 10. The default value is 5 seconds. |

**Command Default**

The timeout for KDC requests is 5 seconds.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When multiple KDCs are configured, there is no way to control the timeout so that failover occurs. This causes common client applications to fail before the next KDC is contacted. Therefore, the `kerberos retry` command enables you to establish stable communication with the KDCs.

**Examples**

The following example shows how to configure the timeout value for KDC requests:

```
Router> enable
Router# configure terminal
Router(config)# kerberos timeout 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>kerberos clients mandatory</code></td>
<td>Causes the <code>rsh</code>, <code>rcp</code>, <code>rlogin</code>, and <code>telnet</code> commands to fail if they cannot negotiate the Kerberos protocol with the remote server.</td>
</tr>
<tr>
<td><code>kerberos credentials forward</code></td>
<td>Forces all network application clients on the router to forward users’ Kerberos credentials upon successful Kerberos authentication.</td>
</tr>
</tbody>
</table>
key (config-radius-server)

To specify the authentication and encryption key for all RADIUS communications between the device and the RADIUS server, use the key command in RADIUS server configuration mode. To remove the configured key, use the no form of this command.

```
key {0 string | 6 string | 7 string} string
no key
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| 0 string | Specifies that an unencrypted key follows.  
  - string — The unencrypted (clear text) shared key. |
| 6 string | Specifies that an advanced encryption scheme (AES) encrypted key follows.  
  - string — The advanced encryption scheme [AES] encrypted key. |
| 7 string | Specifies that a hidden key follows.  
  - string — The hidden shared key. |
| string | The unencrypted (cleartext) shared key. |

**Command Default**

The authentication and encryption key is disabled.

**Command Modes**

RADIUS server configuration (config-radius-server)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.4(1)T</td>
<td>This command was modified. The 6 keyword was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

After enabling authentication, authorization, and accounting (AAA) authentication with the aaa new-model command, you must set the authentication and encryption key using the radius server key command.

- **Note**
  
  Specify a RADIUS key after you issue the aaa new-model command.

  The key entered must match the key used on the RADIUS server. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

  Use the password encryption aes command to configure type 6 AES encrypted keys.

**Examples**

The following example shows how to specify the host with IP address 192.0.2.2 as the RADIUS server and set rad123 as the encryption key:
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2
Device(config-radius-server)# key rad123

The following example shows how to set the authentication and encryption key to anykey. The keyword 7 specifies that a hidden key follows.

Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2
Device(config-radius-server)# key 7 anykey

After you save your configuration and use the **show running-config** command, an encrypted key is displayed as follows:

Device> enable
Device# show running-config

radius server myserver
    address ipv4 192.0.2.2
    key 7 19283103834782sda
! The leading 7 indicates that the following text is encrypted.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>aaa new-model</strong></td>
<td>Enables the AAA access control model.</td>
</tr>
<tr>
<td><strong>address ipv4</strong></td>
<td>Configures the IPv4 address for the RADIUS server accounting and authentication parameters.</td>
</tr>
<tr>
<td><strong>password encryption aes</strong></td>
<td>Enables a type 6 encrypted preshared key.</td>
</tr>
<tr>
<td><strong>radius server</strong></td>
<td>Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode.</td>
</tr>
<tr>
<td><strong>show running-config</strong></td>
<td>Displays the current configuration of your routing device.</td>
</tr>
</tbody>
</table>
key (isakmp-group)

To specify the Internet Key Exchange (IKE) preshared key for group policy attribute definition, use the `key` command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove a preshared key, use the `no` form of this command.

```
key name
no key name
```

**Syntax Description**

<table>
<thead>
<tr>
<th><code>name</code></th>
<th>IKE preshared key that matches the password entered on the client.</th>
</tr>
</thead>
</table>

**Note** This value must match the "password" field that is defined in the Cisco VPN Client 3.x configuration GUI.

**Command Default**

No default behavior or values.

**Command Modes**

ISAKMP group configuration (config-isakmp-group)

<table>
<thead>
<tr>
<th><strong>Command History</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `key` command to specify the IKE preshared key when defining group policy information for Mode Configuration push. (It follows the `crypto isakmp client configuration group command`.) You must configure this command if the client identifies itself to the router with a preshared key. (You do not have to enable this command if the client uses a certificate for identification.)

**Examples**

The following example shows how to specify the preshared key “cisco”:

```
crypto isakmp client configuration group default
  key cisco
dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>acl</code></td>
<td>Configures split tunneling.</td>
</tr>
<tr>
<td><code>crypto isakmp client configuration group</code></td>
<td>Specifies the DNS domain to which a group belongs.</td>
</tr>
</tbody>
</table>
key (TACACS+)

To configure the per-server encryption key on the TACACS+ server, use the `key` command in TACACS+ server configuration mode. To remove the per-server encryption key, use the `no` form of this command.

```
key \[0|6|7]\] key-string
no key \[0|6|7]\] key-string
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(Optional) Specifies that an unencrypted key follows.</td>
</tr>
<tr>
<td>6</td>
<td>(Optional) Specifies that an advanced encryption scheme (AES) encrypted key follows.</td>
</tr>
<tr>
<td>7</td>
<td>(Optional) Specifies that a hidden key follows.</td>
</tr>
</tbody>
</table>

- `key-string` - The unencrypted shared key.

### Command Default
No TACACS+ encryption key is configured.

### Command Modes
TACACS+ server configuration (config-server-tacacs)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3.2S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.4(1)T</td>
<td>This command was integrated into Cisco IOS Release 15.4(1)T. The 6 keyword was added.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `key` command allows you to configure a per-server encryption key. Use the `password encryption aes` command to configure type 6 AES encrypted keys.

### Examples

The following example shows how to specify an unencrypted shared key named “key1”:

```
Device> enable
Device# configure terminal
Device(config)# tacacs server server1
Device(config)# tacacs server-tacacs# key 0 key1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>password encryption aes</code></td>
<td>Enables a type 6 encrypted preshared key.</td>
</tr>
<tr>
<td><code>tacacs server</code></td>
<td>Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.</td>
</tr>
</tbody>
</table>
key config-key

To define a private DES key for the router, use the **key config-key** command in global configuration mode. To delete a private Data Encryption Standard (DES) key from the router, use the **no** form of this command.

```
key config-key 1 string
no key config-key 1 string
```

### Syntax Description

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Key number. This number is always 1.</td>
</tr>
<tr>
<td><em>string</em></td>
<td>Private DES key (can be up to eight alphanumeric characters).</td>
</tr>
</tbody>
</table>

### Command Default

No DES-key defined.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2</td>
<td>This command was released.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command defines a private DES key for the router that will not show up in the router configuration. This private DES key can be used to DES-encrypt certain parts of the router’s configuration.

⚠️ **Caution**

The private DES key is unrecoverable. If you encrypt part of your configuration with the private DES key and lose or forget the key, you will not be able to recover the encrypted data.

### Examples

The following example sets `keyxx` as the private DES key on the router:

```
key config-key 1 keyxx
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kerberos srvtab entry</td>
<td>Specifies a krb5 SRVTAB entry.</td>
</tr>
<tr>
<td>kerberos srvtab remote</td>
<td>Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.</td>
</tr>
</tbody>
</table>
key config-key password-encryption

To store a type 6 encryption key in private NVRAM, use the `key config-key password-encryption` command in global configuration mode. To disable the encryption, use the `no` form of this command.

```
key config-key password-encryption [text]
no key config-key password-encryption [text]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>text</td>
<td>(Optional) Password or master key.</td>
</tr>
</tbody>
</table>

**Note**

It is recommended that you do not use the `text` argument but instead use interactive mode (using the enter key after you enter the `key config-key password-encryption` command) so that the preshared key will not be printed anywhere and, therefore, cannot be seen.

**Command Default**

No type 6 password encryption

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(2)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)SXD</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXD.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can securely store plain text passwords in type 6 format in NVRAM using a command-line interface (CLI). Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the `key config-key password-encryption` command with the `password encryption aes` command to configure and enable the password (symmetric cipher Advanced Encryption Standard [AES] is used to encrypt the keys). The password (key) configured using the `key config-key password-encryption` command is the master encryption key that is used to encrypt all other keys in the router.

If you configure the `password encryption aes` command without configuring the `key config-key password-encryption` command, the following message is printed at startup or during any nonvolatile generation (NVGEN) process, such as when the `show running-config` or `copy running-config startup-config` commands have been configured:

“Can not encrypt password. Please configure a configuration-key with ‘key config-key’”

**Changing a Password**

If the password (master key) is changed, or reencrypted, using the `key config-key password-encryption` command), the list registry passes the old key and the new key to the application modules that are using type 6 encryption.

**Deleting a Password**
If the master key that was configured using the `key config-key password-encryption` command is deleted from the system, a warning is printed (and a confirm prompt is issued) that states that all type 6 passwords will become useless. As a security measure, after the passwords have been encrypted, they will never be decrypted in the Cisco IOS software. However, passwords can be reencrypted as explained in the previous paragraph.

---

**Caution**

If the password configured using the `key config-key password-encryption` command is lost, it cannot be recovered. The password should be stored in a safe location.

---

**Unconfiguring Password Encryption**

If you later unconfigure password encryption using the `no password encryption aes` command, all existing type 6 passwords are left unchanged, and as long as the password (master key) that was configured using the `key config-key password-encryption` command exists, the type 6 passwords will be decrypted as and when required by the application.

**Storing Passwords**

Because no one can “read” the password (configured using the `key config-key password-encryption` command), there is no way that the password can be retrieved from the router. Existing management stations cannot “know” what it is unless the stations are enhanced to include this key somewhere, in which case the password needs to be stored securely within the management system. If configurations are stored using TFTP, the configurations are not standalone, meaning that they cannot be loaded onto a router. Before or after the configurations are loaded onto a router, the password must be manually added (using the `key config-key password-encryption` command). The password can be manually added to the stored configuration but is not recommended because adding the password manually allows anyone to decrypt all passwords in that configuration.

**Configuring New or Unknown Passwords**

If you enter or cut and paste cipher text that does not match the master key, or if there is no master key, the cipher text is accepted or saved, but an alert message is printed. The alert message is as follows:

```
“ciphertext>[for username bar]> is incompatible with the configured master key.”
```

If a new master key is configured, all the plain keys are encrypted and made type 6 keys. The existing type 6 keys are not encrypted. The existing type 6 keys are left as is.

If the old master key is lost or unknown, you have the option of deleting the master key using the `no key config-key password-encryption` command. Deleting the master key using the `no key config-key password-encryption` command causes the existing encrypted passwords to remain encrypted in the router configuration. The passwords will not be decrypted.

---

**Examples**

The following example shows that a type 6 encryption key is to be stored in NVRAM:

```
Router (config)# key config-key password-encryption
```

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password encryption aes</td>
<td>Enables a type 6 encrypted preshared key.</td>
</tr>
<tr>
<td>password logging</td>
<td>Provides a log of debugging output for a type 6 password operation.</td>
</tr>
</tbody>
</table>
key-hash

To specify the Secure Shell (SSH) Rivest, Shamir, and Adleman (RSA) key type and name, use the `key-hash` command in SSH public key configuration mode. To remove the SSH RSA Rivest, Shamir, and Adleman (RSA) public key, use the `no` form of this command.

```
key-hash  key-type  key-name
no  key-hash  [key-type  key-name]
```

**Syntax Description**
- `key-type  key-name` The SSH RSA public key type and name.

**Command Default**
SSH key type and name are not specified.

**Command Modes**
SSH public key configuration (conf-ssh-pubkey-user)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRA</td>
<td>This command was introduced in release earlier than Cisco IOS Release 12.(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The key type must be `ssh-rsa` for configuration of private-public key pairs. You can use a hashing software to compute the hash of the public key string or you can copy the hash value from another Cisco IOS router. Using the `key-string` command is the preferred method for entering the public key data for the first time.

**Examples**
The following example shows how to specify the SSH key type and name:

```
Router(config)# ip ssh pubkey-chain
Router(config)# username test
Router(config)# key-hash ssh-rsa key1
Router(config)# exit
Router(config)# exit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key-string</td>
<td>Specifies the SSH RSA public key of the remote peer.</td>
</tr>
</tbody>
</table>
keyring

To configure a keyring with an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the `keyring` command in ISAKMP profile configuration mode. To remove the keyring from the ISAKMP profile, use the `no` form of this command.

```
keyring keyring-name
no keyring keyring-name
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>keyring-name</th>
<th>The keyring name, which must match the keyring name that was defined in the global configuration.</th>
</tr>
</thead>
</table>

**Command Default**

If this command is not used, the ISAKMP profile uses the keys defined in the global configuration.

**Command Modes**

ISAKMP profile configuration (config-isa-prof)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(15)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.6</td>
<td>This command was integrated into Cisco IOS XE Release 2.6.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The ISAKMP profile successfully completes authentication of peers if the peer keys are defined in the keyring that is attached to this profile. If no keyring is defined in the profile, the global keys that were defined in the global configuration are used.

**Examples**

The following example shows that “vpnkeyring” is configured as the keyring name:

```
crypto isakmp profile vpnprofile
keyring vpnkeyring
```
keyring (IKEv2 profile)

To specify a locally defined or accounting, authentication and authorization (AAA)-based keyring, use the `keyring` command in IKEv2 profile configuration mode. To delete the keyring, use the `no` form of this command.

```
keyring [local] keyring-name|aaa list-name[ {name-mangler mangler-name|password password}]]
no keyring
```

### Syntax Description

<table>
<thead>
<tr>
<th>Documentation</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Specifies the local keyring.</td>
</tr>
<tr>
<td>keyring-name</td>
<td>The keyring name for a locally defined keyring.</td>
</tr>
<tr>
<td>aaa</td>
<td>Specifies the AAA-based preshared keys list name.</td>
</tr>
<tr>
<td>list-name</td>
<td>The AAA method list name.</td>
</tr>
<tr>
<td>name-mangler</td>
<td>Derives the username from the peer identity in the preshared key lookup on the AAA list.</td>
</tr>
<tr>
<td>mangler-name</td>
<td>(Optional) Globally defined name mangler.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies a password for the password. This argument defines the following values:</td>
</tr>
<tr>
<td>password</td>
<td>• 0—Specifies that the password is unencrypted.</td>
</tr>
<tr>
<td></td>
<td>• 6—Specifies that the password is encrypted.</td>
</tr>
<tr>
<td></td>
<td>• password—Specifies an unencrypted user password.</td>
</tr>
</tbody>
</table>

### Command Default

A keyring is not specified.

### Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
<tr>
<td>15.2(2)T</td>
<td>This command was modified. The keyword local and the keyword argument pair name-mangler mangler-name was added.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
<tr>
<td>15.3(3)M</td>
<td>This command was modified. The password password was added.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to specify a keyring for use with the local and remote preshared key authentication methods. Only one keyring can be configured either local or AAA based with or without the name mangler. If you configure an AAA based keyring with the name mangler, the name mangler cannot be deleted.

When using AAA, the default password for a Radius access request is "cisco". You can use the `password` keyword within the `keyring` command to change the password.
Local AAA is not supported for AAA-based preshared keys.

If the **name-mangler** keyword is not specified, the entire peer identity is used for key lookup.

### Examples

The following example shows how to configure an AAA-based keyring and assign the keyring to a profile:

```bash
Router(config)# aaa new-model
Router(config)# aaa authentication login aaa-psk-list default group radius
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# keyring aaa aaa-psk-list name-mangler mangler1
```

The following example shows how to configure a locally defined keyring:

```bash
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# keyring keyring1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2 keyring</td>
<td>Defines an IKEv2 keyring.</td>
</tr>
</tbody>
</table>
**key-set**

To associate a key set with a TIDP group, use the `key-set` command in TIDP group configuration mode. To remove the key set from the TIDP group configuration, use the `no` form of this command.

```
key-set name
no key-set
```

**Syntax Description**

- `name` Name of the key set.

**Command Default**

None.

**Command Modes**

TIDP group configuration (config-tidp-grp)

<table>
<thead>
<tr>
<th>Command History Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(15)XZ</td>
<td>This command was integrated into Cisco IOS Release 12.4(15)XZ.</td>
</tr>
</tbody>
</table>

**Note**

Effective with Cisco IOS Release 12.4(20)T, the `key-set` command is not available in Cisco IOS software.

**Usage Guidelines**

The `key-set` command is entered in TIDP group configuration mode to associate a global key set with a TIDP group. A key set must be configured before a TIDP group can be activated. The key set is first configured with the `tidp key-set` command in global configuration mode. This key set defines the authentication key for TIDP peer communication. This key set can be optionally configured with an encryption key to protect the contents of TIDP messages.

**Examples**

The following example configures TIDP group 10 to use the key set name KEY_1:

```
Router(config)# tidp key-set KEY_1
Router(config-tidp-ks)# authentication-key send key-string 0 Aa1Bb2Cc3
Router(config-tidp-ks)# authentication-key receive key-string 0 Dd4Ee5Ff6
Router(config-tidp-ks)# exit
Router(config)# tidp group 10
Router(config-tidp-grp)# key-set KEY_1
Router(config-tidp-grp)# registration retry-interval min 30 max 600
Router(config-tidp-grp)# peer 10.1.1.1
Router(config-tidp-grp)# peer 10.1.1.2
```
Router(config-tidp-grp)# peer 10.1.1.3
Router(config-tidp-grp)# active

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>Activates a TIDP group.</td>
</tr>
<tr>
<td>peer</td>
<td>Configures a consumer as a member of a TIDP group.</td>
</tr>
<tr>
<td>registration retry-interval (TIDP)</td>
<td>Configures the length of time and number of attempts for TIDP group registration.</td>
</tr>
<tr>
<td>tidp group</td>
<td>Configures a TIDP group.</td>
</tr>
<tr>
<td>tidp key-set</td>
<td>Configures a key-set for TIDP peer authentication and/or message encryption.</td>
</tr>
</tbody>
</table>
key-string (IKE)

To specify the Rivest, Shamir, and Adelman (RSA) public key of the remote peer, use the `key-string` command in public key configuration mode. To remove the RSA public key, use the `no` form of this command.

```
key-string key-string
no key-string key-string
```

### Syntax Description

| key-string | Enter the key in hexadecimal format. While entering the key data, you can press Return to continue entering data. |

### Command Default

No default behavior or values

### Command Modes

Public key configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.6</td>
<td>This command was integrated into Cisco IOS XE Release 2.6.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Before using this command, you must enter the `rsa-pubkey` command in the crypto keyring mode.

If possible, to avoid mistakes, you should cut and paste the key data (instead of attempting to type in the data).

To complete the command, you must return to the global configuration mode by typing `quit` at the config-pubkey prompt.

### Examples

The following example manually specifies the RSA public keys of an IP Security (IPSec) peer:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>crypto keyring</code></td>
<td>Defines a crypto keyring.</td>
</tr>
<tr>
<td></td>
<td><code>rsa-pubkey</code></td>
<td>Defines the RSA public key to be used for encryption or signatures during IKE authentication.</td>
</tr>
<tr>
<td></td>
<td><code>show crypto keyring</code></td>
<td>Displays keyrings on your router.</td>
</tr>
</tbody>
</table>
key-string (SSH)

To specify the Secure Shell (SSH) Rivest, Shamir, and Adleman (RSA) public key of the remote peer, use the **key-string** command in SSH public key configuration mode. To remove the SSH RSA public key, use the **no** form of this command.

**key-string**

**no key-string**

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

SSH RSA public key of the remote peer is not specified.

**Command Modes**

SSH public key configuration (conf-ssh-pubkey-user)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(33)SRA</td>
<td>This command was introduced in release earlier than Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **key-string** command specifies the SSH RSA public key of the remote peer and enters public-key data configuration mode. You can obtain the public key value from an open SSH client (.ssh/id_rsa.pub file).

You can return to global configuration mode by entering the **quit** command in public-key data configuration mode and then by entering the **exit** command in public key configuration mode.

**Examples**

The following example shows how to specify the SSH RSA public keys of the remote peer:

```console
Router(config)# ip ssh pubkey-chain
Router(conf-ssh-pubkey)# username test
Router(conf-ssh-pubkey-user)# key-string
Router(conf-ssh-pubkey-data)# quit
Router(config-pubkey)# exit
Router(config)# exit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key-hash</td>
<td>Specifies the SSH key type and name.</td>
</tr>
</tbody>
</table>
**language**

To specify the language to be used in a webvpn context, use the `language` command in webvpn context configuration mode. To remove the language, use the `no` form of this command.

```
language {Japanese|customize language-name device : file}
no language {Japanese|customize language-name device : file}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Japanese</code></td>
<td>Specifies that the language to be used is Japanese.</td>
</tr>
<tr>
<td><code>customize</code></td>
<td>Specifies that a language other than English or Japanese is to be used.</td>
</tr>
<tr>
<td><code>language-name</code></td>
<td>- <code>language-name</code> -- This language will be displayed in the selection box on the login and portal pages.</td>
</tr>
<tr>
<td><code>device</code></td>
<td>- <code>device : file</code> -- Storage device on the system and the file name. The file name should include the directory location.</td>
</tr>
<tr>
<td><code>device : file</code></td>
<td></td>
</tr>
</tbody>
</table>

### Command Default

English is the language.

### Command Modes

Webvpn context configuration (config-webvpn-context)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(22)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows that the language to be used is Japanese:

```
Router (config)# webvpn context
Router (config-webvpn-context)# language Japanese
```

The following example shows that the language (mylang) is to be customized from the file "lang.js," which is in flash:

```
Router (config)# webvpn context
Router (config-webvpn-context)# language customize mylang flash:lang.js
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>webvpn create template</code></td>
<td>Creates templates for multilanguage support for messages in an SSL VPN.</td>
</tr>
</tbody>
</table>
Idap attribute-map

To configure a dynamic Lightweight Directory Access Protocol (LDAP) attribute map, use the `ldap attribute-map` command in global configuration mode. To remove the attribute maps, use the `no` form of this command.

```
ldap attribute-map map-name
no ldap attribute-map map-name
```

**Syntax Description**

```
map-name  Name of the attribute map.
```

**Command Default**

Default mapping is applied.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can create LDAP attribute maps to map your existing user-defined LDAP attribute names and values to Cisco attribute names and values that are compatible. You can then bind these attribute maps to LDAP server configuration or remove them as required. The default map is displayed using the `show ldap attributes` command.

**Examples**

The following command shows how to create an unpopulated LDAP attribute map table named `att_map_1`:

```
Router(config)# ldap attribute-map att_map_1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attribute-map</td>
<td>Attaches an attribute map to a particular LDAP server.</td>
</tr>
<tr>
<td>map-type</td>
<td>Defines the mapping of a attribute in the LDAP server.</td>
</tr>
<tr>
<td>show ldap attribute</td>
<td>Displays information about default LDAP attribute mapping.</td>
</tr>
</tbody>
</table>
# ldap search

To search a Lightweight Directory Access Protocol (LDAP) server, use the `ldap search` command in privileged EXEC mode.

```
ldap search server-address port-number search-base scope-number search-filter ssl
```

## Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>server-address</code></td>
<td>The IP address of the server.</td>
</tr>
<tr>
<td><code>port-number</code></td>
<td>The remote TCP port. The range is from 0 to 65535.</td>
</tr>
<tr>
<td><code>search-base</code></td>
<td>The search base.</td>
</tr>
<tr>
<td><code>scope-number</code></td>
<td>The scope of the search. The range is from 0 to 2, which denotes to search from BASE, ONELEVEL, and SUBTREE.</td>
</tr>
<tr>
<td><code>search-filter</code></td>
<td>The filter for the search.</td>
</tr>
<tr>
<td><code>ssl</code></td>
<td>Specifies LDAP over Secure Socket Layer (SSL).</td>
</tr>
</tbody>
</table>

## Command Modes

Privileged EXEC (#)

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.0(1)M</td>
<td>This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

## Examples

The following example shows how to search an LDAP server:

```
Router# ldap search 10.0.0.1 265 c 2 sea ssl
```

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ldap server</code></td>
<td>Defines an LDAP server and enters LDAP server configuration mode.</td>
</tr>
</tbody>
</table>
ldap server

To define a Lightweight Directory Access Protocol (LDAP) server and enter LDAP server configuration mode, use the `ldap server` command in global configuration mode. To remove an LDAP server configuration, use the `no` form of this command.

`ldap server name`
`no ldap server name`

**Syntax Description**

| name          | Name of the LDAP server configuration. |

**Command Default**

No LDAP server is configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.3(2)T</td>
<td>This command was modified. IPv6 transport support for LDAP server was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can define the following parameters in LDAP server configuration mode:

- IP address of the LDAP server
- Transport protocol to connect to the server
- Security protocol for peer-to-peer communication
- LDAP timers

**Examples**

The following example shows how to define an LDAP server named server1:

```
Device(config)# ldap server server1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4 (ldap)</td>
<td>Creates an IPv4 address within an LDAP server address pool.</td>
</tr>
<tr>
<td>transport port (ldap)</td>
<td>Configures the transport protocol for establishing a connection with the LDAP server.</td>
</tr>
</tbody>
</table>
length (RITE)

To specify the length the captured portion of the packets being captured in IP traffic export capture mode, use the `length` command in RITE configuration mode. To return to the default condition of capturing entire packets, use the `no` form of this command.

```
length  bytes
no  length
```

**Syntax Description**

| bytes | The length in bytes of the packet captured in IP traffic export capture mode. Acceptable values are 128, 256, and 512. |

**Command Default**

When you do not use this command, the entire packet is captured.

**Command Modes**

RITE configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to limit the length of the portion of the packets being captured in IP traffic export capture mode. The captured portion of the packets are limited to 128, 256, or 512 bytes. If you do not use the `length` command, entire packets are captured.

**Examples**

The following example shows the use of the `length` command in the configuration of IP traffic export capture mode profile “corp2”:

```
Router(config)# ip traffic-export profile corp2 mode_capture
Router(config-rite)# bidirectional
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# length 512
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp2 size 10000000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bidirectional</strong></td>
<td>Enables incoming and outgoing IP traffic to be exported or captured across a monitored interface.</td>
</tr>
<tr>
<td><strong>incoming</strong></td>
<td>Configures filtering for incoming IP traffic export or IP traffic capture traffic.</td>
</tr>
<tr>
<td><strong>ip traffic-export apply profile</strong></td>
<td>Applies an IP traffic export or IP traffic capture profile to a specific interface.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>ip traffic-export profile</code></td>
<td>Creates an IP traffic export or IP traffic capture profile on an ingress interface.</td>
</tr>
<tr>
<td><code>outgoing</code></td>
<td>Configures filtering for outgoing IP traffic export or IP traffic capture traffic.</td>
</tr>
<tr>
<td><code>traffic-export interface</code></td>
<td>Controls the operation of IP traffic capture mode.</td>
</tr>
</tbody>
</table>
license (parameter-map)

To configure a license that is sent to Cloud Web Security for authentication, use the **license** command in parameter-map type inspect configuration mode. To remove the license, use the **no** form of this command.

```
license {0 key | 7 key}
no license {0 key | 7 key}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 key</td>
<td>Specifies an unencrypted 32-character hexadecimal license key.</td>
</tr>
<tr>
<td>7 key</td>
<td>Specifies an encrypted 66-character hexadecimal license key.</td>
</tr>
</tbody>
</table>

**Command Default**

The license is not configured.

**Command Modes**

Parameter-map type inspect configuration (config-profile)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(1)T1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must configure the **parameter-map type cws global** command before you configure the **license** command.

When the server license or the private key is not configured, content scan drops the traffic. When the server license or private key is wrong, content scan forwards the traffic to Cloud Web Security and Cloud Web Security sends a blocked warning page to the end user.

**Examples**

The following example shows how to configure an unencrypted license key:

```
Device(config)# parameter-map type cws global
Device(config-profile)# license 0 D7BF98AFEB0B4AFA5954CB0F81FFB620
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>parameter-map type cws global</td>
<td>Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode.</td>
</tr>
</tbody>
</table>
lifetime (cs-server)

To specify the lifetime of the certification authority (CA) or a certificate, use the `lifetime` command in certificate server configuration mode. To return to the default lifetime values, use the `no` form of this command.

```
lifetime {ca-certificate|certificate} days [hours [minutes]]
no lifetime {ca-certificate|certificate}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>ca-certificate</th>
<th>certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ca-certificate</code></td>
<td>Specifies that the lifetime applies to the CA certificate of the certificate server.</td>
<td></td>
</tr>
<tr>
<td><code>certificate</code></td>
<td>Specifies that the lifetime applies to the certificate of the certificate server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The maximum certificate lifetime is 1 month less than the expiration date of the CA certificate's lifetime.</td>
<td></td>
</tr>
<tr>
<td><code>days</code></td>
<td>An integer specifying the certificate lifetime in days. Valid values range from 0 to 7305.</td>
<td></td>
</tr>
<tr>
<td><code>hours</code></td>
<td>(Optional) An integer specifying the certificate lifetime in hours. Valid values range from 0 to 24.</td>
<td></td>
</tr>
<tr>
<td><code>minutes</code></td>
<td>(Optional) An integer specifying the certificate lifetime in minutes. Valid values range from 0 to 59. It is recommended that if you set the certificate lifetime in minutes, that the value be set to 3 minutes or greater. Setting the certificate lifetime to a value of less than 3 minutes will not allow certificate rollover to function.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

The default CA certificate lifetime is 1095 days, or 3 years.

The default certificate lifetime is 365 days, or 1 year.

**Command Modes**

Certificate server configuration (cs-server)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must configure the `crypto pki server` command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

Use the `lifetime` command if you want to specify lifetime values other than the default values for the CA certificate and the certificate of the certificate server.

After the certificate generates its signed certificate, the lifetime cannot be changed. All certificates are valid when they are issued.

**Examples**

The following example shows how to set the lifetime value for the CA to 30 days:

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# lifetime ca certificate 30
```
<table>
<thead>
<tr>
<th><strong>Related Commands</strong></th>
<th><strong>Command</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-rollover</td>
<td></td>
<td>Enables the automated CA certificate rollover functionality.</td>
</tr>
<tr>
<td>cdp-url</td>
<td></td>
<td>Specifies a CDP to be used in certificates that are issued by the certificate server.</td>
</tr>
<tr>
<td>crl (cs-server)</td>
<td></td>
<td>Specifies the CRL PKI CS.</td>
</tr>
<tr>
<td>crypto pki server</td>
<td></td>
<td>Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials</td>
</tr>
<tr>
<td>database archive</td>
<td></td>
<td>Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.</td>
</tr>
<tr>
<td>database level</td>
<td></td>
<td>Controls what type of data is stored in the certificate enrollment database.</td>
</tr>
<tr>
<td>database url</td>
<td></td>
<td>Specifies the location where database entries for the CS is stored or published.</td>
</tr>
<tr>
<td>database username</td>
<td></td>
<td>Specifies the requirement of a username or password to be issued when accessing the primary database location.</td>
</tr>
<tr>
<td>default (cs-server)</td>
<td></td>
<td>Resets the value of the CS configuration command to its default.</td>
</tr>
<tr>
<td>grant auto rollover</td>
<td></td>
<td>Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.</td>
</tr>
<tr>
<td>grant auto trustpoint</td>
<td></td>
<td>Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.</td>
</tr>
<tr>
<td>grant none</td>
<td></td>
<td>Specifies all certificate requests to be rejected.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>grant ra-auto</td>
<td>Specifies that all enrollment requests from an RA be granted automatically.</td>
<td></td>
</tr>
<tr>
<td>hash (cs-server)</td>
<td>Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.</td>
<td></td>
</tr>
<tr>
<td>issuer-name</td>
<td>Specifies the DN as the CA issuer name for the CS.</td>
<td></td>
</tr>
<tr>
<td>mode ra</td>
<td>Enters the PKI server into RA certificate server mode.</td>
<td></td>
</tr>
<tr>
<td>mode sub-cs</td>
<td>Enters the PKI server into sub-certificate server mode</td>
<td></td>
</tr>
<tr>
<td>redundancy (cs-server)</td>
<td>Specifies that the active CS is synchronized to the standby CS.</td>
<td></td>
</tr>
<tr>
<td>serial-number (cs-server)</td>
<td>Specifies whether the router serial number should be included in the certificate request.</td>
<td></td>
</tr>
<tr>
<td>show (cs-server)</td>
<td>Displays the PKI CS configuration.</td>
<td></td>
</tr>
<tr>
<td>shutdown (cs-server)</td>
<td>Allows a CS to be disabled without removing the configuration.</td>
<td></td>
</tr>
</tbody>
</table>
lifetime (IKE policy)

To specify the lifetime of an Internet Key Exchange (IKE) security association (SA), use the `lifetime` command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. To reset the SA lifetime to the default value, use the `no` form of this command.

Syntax Description

| seconds | Number of many seconds for each each SA should exist before expiring. Use an integer from 60 to 86,400 seconds, which is the default value. |

Command Default

The default is 86,400 seconds (one day).

Command Modes

ISAKMP policy configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was introduced on Cisco ASR 1000 Series Routers.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to specify how long an IKE SA exists before expiring.

When IKE begins negotiations, the first thing it does is agree upon the security parameters for its own session. The agreed-upon parameters are then referenced by an SA at each peer. The SA is retained by each peer until the SA's lifetime expires. Before an SA expires, it can be reused by subsequent IKE negotiations, which can save time when setting up new IPSec SAs. Before an SA expires, it can be reused by subsequent IKE negotiations, which can save time when setting up new IPSec SAs. New IPSec SAs are negotiated before current IPSec SAs expire.

So, to save setup time for IPSec, configure a longer IKE SA lifetime. However, shorter lifetimes limit the exposure to attackers of this SA. The longer an SA is used, the more encrypted traffic can be gathered by an attacker and possibly used in an attack.

Note that when your local peer initiates an IKE negotiation between itself and a remote peer, an IKE policy can be selected only if the lifetime of the remote peer’s policy is shorter than or equal to the lifetime of the local peer’s policy. Then, if the lifetimes are not equal, the shorter lifetime will be selected. To restate this behavior: If the two peer’s policies’ lifetimes are not the same, the initiating peer’s lifetime must be longer and the responding peer’s lifetime must be shorter, and the shorter lifetime will be used.

Examples

The following example configures an IKE policy with a security association lifetime of 600 seconds (10 minutes), and all other parameters are set to the defaults:
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>authentication (IKE policy)</code></td>
<td>Specifies the authentication method within an IKE policy.</td>
</tr>
<tr>
<td><code>crypto isakmp policy</code></td>
<td>Defines an IKE policy.</td>
</tr>
<tr>
<td><code>encryption (IKE policy)</code></td>
<td>Specifies the encryption algorithm within an IKE policy.</td>
</tr>
<tr>
<td><code>group (IKE policy)</code></td>
<td>Specifies the Diffie-Hellman group identifier within an IKE policy.</td>
</tr>
<tr>
<td><code>hash (IKE policy)</code></td>
<td>Specifies the hash algorithm within an IKE policy.</td>
</tr>
<tr>
<td><code>show crypto isakmp policy</code></td>
<td>Displays the parameters for each IKE policy.</td>
</tr>
</tbody>
</table>
lifetime (IKEv2 profile)

To specify the lifetime for an Internet Key Exchange Version 2 (IKEv2) security association (SA), use the `lifetime` command in IKEv2 profile configuration mode. To reset the SA lifetime to the default value, use the `no` form of this command.

```
lifetime  seconds
no  lifetime
```

**Syntax Description**

| seconds | The time that each IKE SA should exist before expiring. Use an integer from 60 to 86,400 seconds. |

**Command Default**

The default is 86,400 seconds (one day).

**Command Modes**

IKEv2 profile configuration (config-ikev2-profile)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 3.3S</td>
<td>This command was integrated into Cisco IOS XE Release 3.3S.</td>
</tr>
<tr>
<td>15.2(4)S</td>
<td>This command was integrated into Cisco IOS Release 15.2(4)S.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to specify the lifetime of an IKE SA. When IKE begins negotiations, IKE agrees on the security parameters for its session that are referenced by an SA at each peer. The SA is retained by each peer until the SA expires, and before an SA expires, it can be reused by subsequent IKE negotiations, which saves time when setting up new IKE SA. Although, SA with a shorter lifetime limits the exposure to attacks, to save time configure an IKE SA that has a longer lifetime. The longer an SA is used, the more encrypted traffic can be gathered by an attacker and possibly used in an attack.

**Examples**

The following example configures an IKEv2 profile with a security association lifetime of 600 seconds (10 minutes), and all other parameters are set to the defaults:

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# lifetime 600
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ikev2 profile</td>
<td>Defines an IKEv2 profile.</td>
</tr>
<tr>
<td>show crypto ikev2 profile</td>
<td>Displays the IKEv2 profile.</td>
</tr>
</tbody>
</table>
To define the lifetime of the certificate revocation list (CRL) that is used by the certificate server, use the `lifetime crl` command in certificate server configuration mode. To return to the default value of 1 week, use the no form of this command.

```
lifetime crl time
no lifetime crl time
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>time</code></td>
<td>Lifetime value, in hours, of the CRL. Maximum lifetime value is 336 hours (2 weeks). The default value is 168 hours (1 week).</td>
</tr>
</tbody>
</table>

**Command Default**

168 hours (1 week)

**Command Modes**

Certificate server configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

After you create a certificate server via the `crypto pki server` command, use the `lifetime crl` command if you want to specify a value other than the default value for the CRL. The lifetime value is added to the CRL when the CRL is created.

The CRL is written to the specified database location as `ca-label.crl`.

**Examples**

The following example shows how to set the lifetime value for the CRL to 24 hours:

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# lifetime crl 24
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdp-url</td>
<td>Specifies that CDP should be used in the certificates that are issued by the certificate server.</td>
</tr>
<tr>
<td>crypto pki server</td>
<td>Enables a Cisco IOS certificate server and enters PKI configuration mode.</td>
</tr>
</tbody>
</table>
lifetime enrollment-request

To specify how long an enrollment request should stay in the enrollment database, use the lifetime enrollment-request command in certificate server configuration mode. To return to the default value of 1 week, use the no form of this command.

```
lifetime enrollment-request time
no lifetime enrollment-request
```

**Syntax Description**

| `time` | Lifetime value, in hours, of an enrollment request. The maximum lifetime value is 1000 hours. The default value is 168 hours (1 week). |

**Command Default**

Lifetime value default is 168 hours.

**Command Modes**

Certificate server configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7T)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

After the certificate server receives an enrollment request, it can leave the request in pending, reject it, or grant it. The request is left in the Enrollment Request Database for the lifetime of the enrollment request until the client polls the certificate server for the result of the request.

**Examples**

The following example shows how to set the lifetime value for the enrollment request to 24 hours:

```
Router (config)# crypto pki server mycs
Router (cs-server)# lifetime enrollment-request 24
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto pki server</td>
<td>Enables a Cisco IOS certificate server.</td>
</tr>
<tr>
<td>crypto pki server grant</td>
<td>Grants all or certain SCEP requests.</td>
</tr>
<tr>
<td>crypto pki server remove</td>
<td>Removes enrollment requests that are in the certificate server Enrollment Request Database.</td>
</tr>
</tbody>
</table>
limit address-count

To limit the number of IPv6 addresses allowed to be used on the port, use the limit address-count command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode.

limit address-count maximum

Syntax Description

| maximum | Sets the role of the device to host. |

Command Default

The device role is host.

Command Modes

ND inspection policy configuration (config-nd-inspection)
RA guard policy configuration (config-ra-guard)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(50)SY</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The limit address-count command limits the number of IPv6 addresses allowed to be used on the port on which the policy is applied. Limiting the number of IPv6 addresses on a port helps limit the binding table size.

Use the limit address-count command after enabling NDP inspection policy configuration mode using the ipv6 nd inspection policy command.

Examples

The following example defines an NDP policy name as policy1, places the router in NDP inspection policy configuration mode, and limits the number of IPv6 addresses allowed on the port to 25:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# limit address-count 25
```
list (LSP Attributes)

To display the contents of a label switched path (LSP) attribute list, use the list command in LSP Attributes configuration mode.

```
list
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Contents of an LSP attribute list is not displayed.

**Command Modes**
LSP Attributes configuration (config-lsp-attr)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(26)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command displays the contents of the LSP attribute list. You can display each of the following configurable LSP attributes using the list command: affinity, auto-bw, bandwidth, lockdown, priority, protection, and record-route.

**Examples**

The following example shows how to display the contents of an LSP attribute list identified with the string priority:

```
!  Router(config)# mpls traffic-eng lsp attributes priority
Router(config-lsp-attr)# priority 0 0
Router(config-lsp-attr)# list
  priority 0 0
Router(config-lsp-attr)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls traffic-eng lsp attributes</td>
<td>Creates or modifies an LSP attribute list.</td>
</tr>
<tr>
<td>show mpls traffic-eng lsp attributes</td>
<td>Displays global LSP attribute lists.</td>
</tr>
</tbody>
</table>
list (WebVPN)

To list the currently configured access control list (ACL) entries sequentially, use the list command in webvpn acl configuration mode. This command has no no form.

list

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Currently configured ACL entries are not listed.

**Command Modes**

Webvpn acl configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(11)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before using this command, you must have configured the web context and the acl command.

**Examples**

The following example shows that currently configured ACL entries are to be listed:

```plaintext
webvpn context context1
  acl acl1
  list
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>webvpn context</td>
<td>Configures the WebVPN context and enters SSL VPN configuration mode.</td>
</tr>
<tr>
<td>acl</td>
<td>Defines an ACL using a SSL VPN gateway at the Application Layer level.</td>
</tr>
</tbody>
</table>
li-view

To initialize a lawful intercept view, use the li-view command in global configuration mode.

`li-view li-password user username password password`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>li-password</td>
<td>Password for the lawful intercept view. This password is used by the system administrator or a level 15 privilege user who initialized the lawful intercept view to access and configure it. The password can contain any number of alphanumeric characters.</td>
</tr>
<tr>
<td>Note</td>
<td>The password is case sensitive.</td>
</tr>
<tr>
<td>user</td>
<td>Specifies the user who can access the lawful intercept view.</td>
</tr>
<tr>
<td>password</td>
<td>Provides the password for the specified user. The user must provide this password to access the lawful intercept view.</td>
</tr>
</tbody>
</table>

**Command Default**

A lawful intercept view cannot be accessed.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(7)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRB</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRB.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.1</td>
<td>This command was integrated into Cisco IOS XE Release 2.1.</td>
</tr>
<tr>
<td>12.2(33)SXI</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXI.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Like a command-line interface (CLI) view, a lawful intercept view restricts access to specified commands and configuration information. Specifically, a lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of Network Management Protocol (SNMP) commands that stores information about calls and users.

Commands available in lawful intercept view belong to one of the following categories:

- Lawful intercept commands that should not be made available to any other view or privilege level.
- CLI commands that are useful for lawful intercept users but do not need to be excluded from other views or privilege levels.

**Note**

Only a system administrator or a level 15 privilege user can initialize a lawful intercept view.
The following example shows how to configure a lawful intercept view, add users to the view, and verify the users that were added to the view:

```
!Initialize the LI-View.
Router(config)# li-view lipass user li_admin password li_adminpass
00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config)# end

! Enter the LI-View; that is, check to see what commands are available within the view.
Router# enable view li-view
Password:
Router# 00:22:57:%PARSER-6-VIEW_SWITCH:successfully set to view 'li-view'.
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# parser view li-view

Router(config-view)# ?
View commands:
  commands Configure commands for a view
  default Set a command to its defaults
  exit Exit from view configuration mode
  name New LI-View name ===This option only resides in LI View.
  no Negate a command or set its defaults
  password Set a password associated with CLI views

Router(config-view)#
! NOTE:LI View configurations are never shown as part of ‘running-configuration’.
! Configure LI Users.
Router(config)# username lawful-intercept li-user1 password li-user1pass

Router(config)# username lawful-intercept li-user2 password li-user2pass

! Displaying LI User information.
Router# show users lawful-intercept
li_admin
li-user1
li-user2
Router#```
load-balance (server-group)

To enable RADIUS server load balancing for a named RADIUS server group, use the `load-balance` command in server group configuration mode. To disable named RADIUS server load balancing, use the `no` form of this command.

```
load-balance method least-outstanding [batch-size number] [ignore-preferred-server]
no load-balance
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>method least-outstanding</td>
<td>Enables least outstanding mode for load balancing.</td>
<td></td>
</tr>
<tr>
<td>batch-size</td>
<td>(Optional) The number of transactions to be assigned per batch.</td>
<td></td>
</tr>
<tr>
<td>number</td>
<td>(Optional) The number of transactions in a batch.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>Batch size may impact throughput and CPU load. It is recommended that the default batch size, 25, be used because it is optimal for high throughput, without adversely impacting CPU load.</td>
<td></td>
</tr>
<tr>
<td>ignore-preferred-server</td>
<td>(Optional) Indicates if a transaction associated with a single authentication, authorization, and accounting (AAA) session should attempt to use the same server or not.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If set, preferred server setting will not be used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default is to use the preferred server.</td>
<td></td>
</tr>
</tbody>
</table>

Command Default

If this command is not configured, named RADIUS server load balancing will not occur.

Command Modes

Server group configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(28)SB</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.4(11)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(11)T.</td>
</tr>
<tr>
<td>12.2(33)SRC</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRC.</td>
</tr>
</tbody>
</table>

Examples

The following example shows load balancing enabled for a named RADIUS server group. It is shown in three parts: the current configuration of RADIUS command output, debug output, and AAA server status information.
Server Configuration and Enabling Load Balancing for Named RADIUS Server Group Example

The following shows the relevant RADIUS configuration:

Router# show running-config
    
    aaa group server radius server-group1
        server 192.0.2.238 auth-port 2095 acct-port 2096
        server 192.0.2.238 auth-port 2015 acct-port 2016
        load-balance method least-outstanding batch-size 5
    !
    aaa authentication ppp default group server-group1
    aaa accounting network default start-stop group server-group1
    
    The lines in the current configuration of RADIUS command output above are defined as follows:
    
    • The **aaa group server radius** command shows the configuration of a server group with two member servers.
    
    • The **load-balance** command enables load balancing for the global RADIUS server groups with the batch size specified.
    
    • The **aaa authentication ppp** command authenticates all PPP users using RADIUS.
    
    • The **aaa accounting** command enables the sending of all accounting requests to the AAA server after the client is authenticated and after the disconnect using the start-stop keyword.

Debug Output for Named RADIUS Server Group Example

The debug output below shows the selection of a preferred server and the processing of requests for the configuration above.

Router#
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):Server (192.0.2.238:2095,2096) now being used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):Server (192.0.2.238:2095,2096) now being used as preferred server
server.

used as preferred server

server.

used as preferred server

server.

used as preferred server

server.

used as preferred server

server.


used as preferred server

server.

Server Status Information for Named RADIUS Server Group Example

The output below shows the AAA server status for the named RADIUS server group configuration example.

```
Router# show aaa servers
RADIUS:id 8, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
  State:current UP, duration 3781s, previous duration 0s
  Dead:total time 0s, count 0
  Quarantined:No
  Authen:request 0, timeouts 0
    Response:unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction:success 0, failure 0
  Author:request 0, timeouts 0
    Response:unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction:success 0, failure 0
  Account:request 0, timeouts 0
    Response:unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction:success 0, failure 0
  Elapsed time since counters last cleared:0m
RADIUS:id 9, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
  State:current UP, duration 3781s, previous duration 0s
  Dead:total time 0s, count 0
  Quarantined:No
  Authen:request 0, timeouts 0
    Response:unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction:success 0, failure 0
  Author:request 0, timeouts 0
    Response:unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction:success 0, failure 0
```

Cisco IOS Security Command Reference: Commands D to L
The output shows the status of two RADIUS servers. Both servers are alive, and no requests have been processed since the counters were cleared 0 minutes ago.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug aaa sg-server selection</td>
<td>Shows why the RADIUS and TACACS+ server group system in a router is selecting a particular server.</td>
</tr>
<tr>
<td>debug aaa test</td>
<td>Shows when the idle timer or dead timer has expired for RADIUS load balancing.</td>
</tr>
<tr>
<td>radius-server host</td>
<td>Enables RADIUS automated testing for load balancing.</td>
</tr>
<tr>
<td>radius-server load-balance</td>
<td>Enables RADIUS server load balancing for the global RADIUS server group.</td>
</tr>
<tr>
<td>test aaa group</td>
<td>Tests RADIUS load balancing server response manually.</td>
</tr>
</tbody>
</table>
load classification

Note
Effective with Cisco IOS Release 15.2(4)M, the load classification command is not available in Cisco IOS software.

To load a traffic classification definition file (TCDF) for a Flexible Packet Matching (FPM) configuration, use the load classification command in global configuration mode. To unload all TCDFs from a specified location or a single TCDF, use the no form of this command.

load classification location : filename
no load classification location : filename

Syntax Description

<table>
<thead>
<tr>
<th>location : filename</th>
<th>Location of the TCDF that is to be loaded onto the router.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>When used with the no form of this command, all TCDFs loaded from the specified filename will be unloaded.</td>
</tr>
<tr>
<td>Note</td>
<td>The location must be local to the routing device.</td>
</tr>
</tbody>
</table>

Command Default
No TCDF is loaded onto the router.

Command Modes
Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(4)M</td>
<td>This command was removed from the Cisco IOS software.</td>
</tr>
</tbody>
</table>

Usage Guidelines
A TCDF is an Extensible Markup Language (XML) file that you create in a text file or using an XML editor. FPM uses a TCDF to define classes of traffic and to specify actions to apply to the traffic classes for the purpose of blocking attacks on the network. Traffic classification behavior defined in a TCDF is identical to that configured using the command-line interface (CLI).

Use the load classification command to load the TCDF onto the routing device. The location to which you load the file must be local to the device. After the TCDF is loaded, you can use service policy CLI commands to attach the TCDF policies to a specific interface or interfaces. TCDF classes and policies, which are loaded, display as normal policies and classes when you issue a show command.

The TCDF requires that a relevant protocol header description file (PHDF) is already loaded onto the system through the use of the load protocol command. Standard PHDFs are provided with the FPM feature.

Examples
The following example shows how to create a TCDF for slammer packets (UDP 1434) for an FPM XML configuration. The match criteria defined within the class element is for slammer packets with an IP length not to exceed 404 (0x194) bytes, UDP port 1434 (0x59A), and pattern 0x4011010 at
224 bytes from start of the IP header. The policy “fpm-udp-policy” is defined with the action to drop slammer packets.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<tcdf>
  <class name="ip-udp" type="stack">
    <match>
      <eq field="ip.protocol" value="0x11" next="udp"></eq>
    </match>
  </class>
  <class name="slammer" type="access-control" match="all">
    <match>
      <eq field="udp.dest-port" value="0x59A"></eq>
      <eq field="ip.length" value="0x194"></eq>
      <eq start="l3-start" offset="224" size="4" value="0x00401010"></eq>
    </match>
  </class>
  <policy type="access-control" name="fpm-udp-policy">
    <class>
      ...
    </class>
  </policy>
</tcdf>
```
The following example shows how to load relevant PHDFs, load the TCDF file sql-slammer.tcdf, and attach the TCDF-defined policy to the interface Ethernet 0/1:

```
enable
cfg-term
load protocol localdisk1:ip.phdf
load protocol localdisk1:tcp.phdf
load protocol localdisk1:udp.phdf
load classification localdisk1:sql-slammer.tcdf
policy-map type access-control my-policy-1
  class ip-udp
  service-policy fpm-udp-policy
  interface Ethernet 0/1
  service-policy type access control input my-policy-1
end
```

The following CLI output is associated with the TCDF described in the example:

```
Router# show class-map type stack
  .
  .
class-map type stack match-all ip-udp
  match field IP protocol eq 0x11 next UDP
  .
  .
Router# show class-map type access-control
  .
  .
class-map type access-control match-all slammer
  match field UDP dest-port eq 0x59A
  match field IP length eq 0x194
  match start l3-start offset 224 size 4 eq 0x4011010
  .
  .
Router show policy-map my-policy-1
  .
  .
policy-map type access-control my-policy-1
  class slammer
    drop
    .
    .
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>load protocol</td>
<td>Loads a protocol header description file (PHDF) onto a router.</td>
</tr>
</tbody>
</table>
local-address

To limit the scope of an Internet Security Association and Key Management Protocol (ISAKMP) profile or an ISAKMP keyring configuration to a local termination address or interface, use the `local-address` command in ISAKMP profile configuration and keyring configuration modes. To remove the local address or interface, use the `no` form of this command.

```
local-address {interface-name|ip-address [vrf-tag]}
no local-address {interface-name|ip-address [vrf-tag]}
```

**Syntax Description**

- `interface-name`: Name of the local interface.
- `ip-address`: Local termination address.
- `vrf-tag`: (Optional) Scope of the IP address will be limited to the VRF instance.

**Command Default**

If this command is not configured, the ISAKMP profile or ISAKMP keyring is available to all local addresses.

**Command Modes**

ISAKMP profile configuration
Keyring configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(18)SXE</td>
<td>This command was integrated into Cisco IOS Release 12.2(18)SXE.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows that the scope of the ISAKMP profile is limited to interface serial2/0:

```
crypto isakmp profile profile1
    keyring keyring1
    match identity address 10.0.0.0 255.0.0.0
    local-address serial2/0
```

The following example shows that the scope of the ISAKMP keyring is limited only to interface serial2/0:

```
crypto keyring
    local-address serial2/0
    pre-shared-key address 10.0.0.1
```

The following example shows that the scope of the ISAKMP keyring is limited only to IP address 10.0.0.2:

```
crypto keyring keyring1
    local-address 10.0.0.2
    pre-shared-key address 10.0.0.2 key
```
The following example shows that the scope of an ISAKMP keyring is limited to IP address 10.34.35.36 and that the scope is limited to VRF examplevrf1:

```
ip vrf examplevrf1
  rd 12:3456
crypto keyring ring1
  local-address 10.34.35.36 examplevrf1
interface ethernet2/0
  ip vrf forwarding examplevrf1
  ip address 10.34.35.36 255.255.0.0
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>crypto isakmp profile</code></td>
<td>Defines an ISAKMP profile and audits IPSec user sessions.</td>
</tr>
<tr>
<td><code>crypto keyring</code></td>
<td>Defines a keyring and enters keyring configuration mode.</td>
</tr>
</tbody>
</table>
local-port (WebVPN)

To remap (forward) an application port number in a port forwarding list, use the `local-port` command in webvpn port-forward list configuration mode. To remove the application port mapping from the forwarding list, use the `no` form of this command.

```
local-port number remote-server name remote-port number description text-string
no local-port number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Configures the port number to which the local application is mapped. Valid values are 1 to 65535.</td>
</tr>
<tr>
<td><code>remote-server name</code></td>
<td>Identifies the remote server. An IPv4 address or fully qualified domain name is entered.</td>
</tr>
<tr>
<td><code>remote-port number</code></td>
<td>Specifies the well-known port number of the application, for which port-forwarding is to be configured. Valid values are 1 to 65535.</td>
</tr>
<tr>
<td><code>description text-string</code></td>
<td>Configures a description for this entry in the port-forwarding list. The text string is displayed on the end-user applet window. A text string up to 64 characters in length is entered.</td>
</tr>
</tbody>
</table>

**Command Default**

An application port number is not remapped.

**Command Modes**

Webvpn port-forward list configuration (config-webvpn-port-fwd)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `local-port` command is configured to add an entry to the port-forwarding list. The forward list is created with the `port-forward` command in webvpn context configuration mode. The remote port number is the well-known port to which the application listens. The local port number is the entry configured in the port forwarding list. A local port number can be configured only once in a given port-forwarding list.

**Examples**

The following example configures port forwarding for well-known e-mail application port numbers:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# port-forward EMAIL
Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail.company.com remote-port 110 description POP3
Router(config-webvpn-port-fwd)# local-port 30017 remote-server mail.company.com remote-port 25 description SMTP
Router(config-webvpn-port-fwd)# local-port 30018 remote-server mail.company.com remote-port
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>port-forward</strong></td>
<td>Enters webvpn port-forward list configuration mode to configure a port-forwarding list.</td>
</tr>
<tr>
<td><strong>webvpn context</strong></td>
<td>Enters webvpn context configuration mode to configure the SSL VPN context.</td>
</tr>
</tbody>
</table>
**local priority**

To set the local key server priority, use the `local priority` command in GDOI redundancy configuration mode. To remove the local key server priority that was set, use the `no` form of this command.

```
local priority number
no local priority number
```

**Syntax Description**

- `number`: Priority number of the local server. Value = 1 through 255.

**Command Default**

If the local priority is not set by this command, the local priority defaults to 1.

**Command Modes**

GDOI redundancy configuration (gdoi-coop-ks-config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(11)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.3</td>
<td>This command was implemented on the Cisco ASR 1000 Aggregation Services Series Routers.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Configure the priority to determine the order of preference of the key servers (the higher priority device becomes the primary key server). If the priority of two devices is the same, the IP address is used to set the priority. The higher the IP address, the higher the priority.

**Note**

If the `no local priority` option is configured, the default value of 1 is set for that key server.

**Examples**

The following example shows that the key server 10.1.1.1 has the highest priority and, therefore, becomes the primary key server:

```
address ipv4 10.1.1.1
redundancy
  local priority 10
  peer address ipv4 10.41.2.5
peer address ipv4 10.33.5.6

address ipv4 10.41.2.5
redundancy
  peer address ipv4 10.1.1.1
peer address ipv4 10.33.5.6

address ipv4 10.33.5.6
redundancy
  local priority 5
  peer address ipv4 10.41.2.5
```
peer address ipv4 10.1.1.1

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address ipv4</td>
<td>Sets the source address, which is used as the source for packets originated by the local key server.</td>
</tr>
<tr>
<td>peer address ipv4</td>
<td>Configures a GDOI redundant peer key server.</td>
</tr>
<tr>
<td>redundancy</td>
<td>Enters GDOI redundancy configuration mode and allows for peer key server redundancy.</td>
</tr>
<tr>
<td>server local</td>
<td>Designates a device as a GDOI key server and enters GDOI local server configuration mode.</td>
</tr>
</tbody>
</table>
lockdown (LSP Attributes)

To disable reoptimization of the label switched path (LSP), use the **lockdown** command in LSP Attributes configuration mode. To reenable reoptimization, use the **no** form of this command.

```
lockdown
no lockdown
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Reoptimization of the LSP is enabled.

**Command Modes**
LSP Attributes configuration (config-lsp-attr)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(26)S</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use this command to set up in an LSP attribute list the disabling of reoptimization of an LSP triggered by a timer, or the issuance of the **mpls traffic-eng reoptimize** command, or a configuration change that requires the resignalling of an LSP.

To associate the LSP lockdown attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes string** keyword and argument, where **string** is the identifier for the specific LSP attribute list.

**Examples**

The following example shows how to configure disabling of reoptimization in an LSP attribute list:

```
Configure terminal
!
mpls traffic-eng lsp attributes 4
  bandwidth 1000
  priority 1 1
  lockdown 1 1
end
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>mpls traffic-eng lsp attributes</strong></td>
<td>Creates or modifies an LSP attribute list.</td>
</tr>
<tr>
<td><strong>show mpls traffic-eng lsp attributes</strong></td>
<td>Displays global LSP attribute lists.</td>
</tr>
</tbody>
</table>
log (policy-map)

To generate a log of messages, use the log command in policy-map configuration mode. To disable the log, use the no form of this command.

```
log
no log
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

None

**Command Modes**

Policy-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(6)T</td>
<td>This command was introduced in Cisco IOS Release 12.4(6)T.</td>
</tr>
<tr>
<td>12.4(20)T</td>
<td>This command was modified in Cisco IOS Release 12.4(20)T. This command can now be used after entering the policy-map type inspect smtp.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can use this command only after entering the following commands:

- `policy-map type inspect http`
- `policy-map type inspect imap`
- `policy-map type inspect smtp`

**Examples**

The following example generates a log of messages:

```
policy-map type inspect http mypolicy
log
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>policy-map type inspect http</code></td>
<td>Creates a Layer 7 HTTP policy map.</td>
</tr>
<tr>
<td><code>policy-map type inspect imap</code></td>
<td>Creates a Layer 7 IMAP policy map.</td>
</tr>
<tr>
<td><code>policy-map type inspect smtp</code></td>
<td>Create a Layer 7 SMTP policy map</td>
</tr>
</tbody>
</table>
log (parameter-map type)

To log the firewall activity for an inspect parameter map, use the log command in parameter-map type inspect configuration mode.

```
log {dropped-packets {disable|enable}|summary [flows number] [time-interval seconds]}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dropped-packets</td>
<td>Logs the packets dropped by the firewall.</td>
</tr>
<tr>
<td>disable</td>
<td>enable</td>
</tr>
<tr>
<td>summary</td>
<td>Turns on the summary of the packets dropped during the firewall activity for</td>
</tr>
<tr>
<td></td>
<td>interzone and intrazone traffic.</td>
</tr>
<tr>
<td>flows number</td>
<td>(Optional) Specifies the number of flows for which the summary logs must be</td>
</tr>
<tr>
<td></td>
<td>printed. The default flow is 16.</td>
</tr>
<tr>
<td>time-interval seconds</td>
<td>(Optional) Specifies the time interval, in seconds, which the summary logs</td>
</tr>
<tr>
<td></td>
<td>must be printed. The default is 60.</td>
</tr>
</tbody>
</table>

**Command Default**

The firewall activity is not captured.

**Command Modes**

Parameter-map type inspect configuration (config-profile)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS-XE 2.4</td>
<td>This command was integrated into Cisco IOS-XE Release 2.4.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to log the firewall activity as follows:

- Time interval for the summary logs
- Display the protocol information in the summary logs
- Enable summary logs for the specified flows

If the flow is specified as zero as `log summary flow 0`, the log activity is turned off and summary logs are not printed until the flow count is greater than zero.

To display the summary logs, use the `show policy-firewall summary-log` and `clear policy-firewall summary-log` to clear the summary logs.

**Examples**

The following examples show how to configure the summary logs in two scenarios.

In the following example, the summary logs are printed for 40 flows every 2 minutes:

```
Router(config)# parameter-map type inspect global
```

Cisco IOS Security Command Reference: Commands D to L
Router(config-profile)# log summary flows 40 time-interval 120
In the following example, the summary logs are printed for 30 flows at the default time interval of 1 minute:
Router(config)# parameter-map type inspect global
Router(config-profile)# log summary flows 30
In the above example, the flow is not configured. Hence, the summary logs are printed by default for 16 flows every 30 seconds:
Router(config)# parameter-map type inspect global
Router(config-profile)# log summary time-interval 30

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear policy-firewall</td>
<td>Clears the information collected by the firewall.</td>
</tr>
<tr>
<td>parameter-map type inspect</td>
<td>Defines an inspect type parameter map.</td>
</tr>
<tr>
<td>pass</td>
<td>Allows packets to be sent to the router without being inspected.</td>
</tr>
<tr>
<td>show policy-firewall summary-log</td>
<td>Displays the summary log of the firewall.</td>
</tr>
</tbody>
</table>
log (type access-control)

Effective with Cisco IOS Release 15.2(4)M, the log command is not available in Cisco IOS software.

To generate log messages for a predefined traffic class, use the log command in policy-map class configuration mode. To disable the log, use the no form of this command.

```
log [all]
no log [all]
```

**Syntax Description**

- **all** (Optional) Logs the entire stream of discarded packets belonging to the traffic class.

**Command Default**

Log messages are disabled.

**Command Modes**

Policy-map class configuration (config-pmap-c)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1(3)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>15.2(4)M</td>
<td>This command was removed from the Cisco IOS software.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the log command is specified with the all keyword, then this command can only be used with a predefined session-based Flexible Packet Matching (FPM) traffic class that was created with the class-map type access-control command.

The log all command is used when configuring a policy map that can be attached to one or more interfaces to specify a service policy that is created with the policy-map type access-control command.

**Examples**

The following example shows how to configure a class map and policy map to specify the protocol stack class, the match criteria and action to take, and a combination of classes using session-based (flow-based) and nonsession-based actions. The log command all keyword is associated with the action taken on the policy.

```bash
Router(config)# class-map type access-control match-all my-HTTP
Router(config-cm)# match field tcp destport eq 8080
Router(config-cm)# match start tcp payload-start offset 20 size 10 regex “GET”
Router(config)# class-map type access-control match-all my-FTP
Router(config-cm)# match field tcp destport eq 21
Router(config)# class-map type access-control match all class1
Router(config-cm)# match class my-HTTP session
Router(config-cm)# match start tcp payload-start offset 40 size 20 regex “abc.*def”
Router(config)# policy-map type access-control my_http_policy
Router(config-pmap)# class class1
Router(config-pmap-c)# log all
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input my_http_policy
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class</td>
<td>Specifies the name of a predefined traffic class, which was configured with the <strong>class-map</strong> command. This command also classifies traffic to the traffic policy and enters policy-map class configuration mode.</td>
</tr>
<tr>
<td>class-map type access-control</td>
<td>Creates a class map to be used for matching packets to a specified class and enters class map configuration mode for determining the exact pattern to look for in the protocol stack of interest.</td>
</tr>
<tr>
<td>drop</td>
<td>Configures a traffic class to discard packets belonging to a specific class.</td>
</tr>
<tr>
<td>match class session</td>
<td>Configures match criteria for a class map used to identify a session (flow) containing packets of interest, which is then applied to all packets transmitted during the session.</td>
</tr>
<tr>
<td>policy-map type access-control</td>
<td>Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy, and enters policy-map configuration mode.</td>
</tr>
<tr>
<td>show class-map</td>
<td>Displays all class maps and their matching criteria.</td>
</tr>
<tr>
<td>show policy-map</td>
<td>Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.</td>
</tr>
<tr>
<td>show policy-map interface</td>
<td>Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.</td>
</tr>
</tbody>
</table>
logging (parameter-map)

To enable the logging of Cloud Web Security content scan events, use the `logging` command in privileged EXEC mode. To disable logging, use the `no` form of this command.

```
logging
no logging
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Logging of events is disabled.

**Command Modes**

Parameter-map type inspect configuration (config-profile)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.2(1)T1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must configure the `parameter-map type cws global` before you configure the `logging` command.

All Cloud Web Security-related syslog displays the username, group name, IP address, and port number of the source and destination.

**Examples**

The following example shows how to enable logging of Cloud Web Security content scan events:

```
Device(config)# parameter-map type cws global
Device(config-profile)# logging
Device(config-profile)# end
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>parameter-map type cws global</code></td>
<td>Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode.</td>
</tr>
</tbody>
</table>
logging dmvpn

To display Dynamic Multipoint VPN (DMVPN)-specific system logging information, use the `logging dmvpn` command in global configuration mode. To turn off logging, use the `no` form of this command.

```
logging dmvpn [rate-limit rate]
no logging dmvpn [rate-limit rate]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate-limit rate</td>
<td>(Optional) Specifies the number of DMVPN syslog messages generated per minute. The range is from 1 to 10000.</td>
</tr>
<tr>
<td></td>
<td>• The default rate is to generate 600 messages per minute.</td>
</tr>
</tbody>
</table>

**Command Default**

DMVPN system logging messages are not enabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(9)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 2.5</td>
<td>This command was integrated into Cisco IOS XE Release 2.5.</td>
</tr>
<tr>
<td>15.0(1)M</td>
<td>This command was modified. The <code>rate</code> argument was modified to specify the number of DMVPN syslog messages per minute.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `logging dmvpn rate-limit rate` command to specify the rate at which the DMVPN-specific syslog messages are displayed. In Cisco IOS Release 12.4(24)T and earlier releases, the `rate` argument specifies the minimum interval, in seconds, between two DMVPN syslog messages, with a range of 0 to 3600, and a default value of 60.

In Cisco IOS Release 15.0(1)M and later releases, the `rate` argument specifies the number of DMVPN syslog messages per minute. If you have upgraded to Release Cisco IOS 15.0(1)M or later releases, you must reconfigure the DMVPN rate limit settings.

**Examples**

The following example shows how to configure the router to display five DMVPN-specific syslog messages per minute:

```
Router> enable
Router# configure terminal
Router(config)# logging dmvpn rate-limit 5
```

The following example shows a sample system log with DMVPN messages:

```
%DMVPN-7-CRYPTO_SS: Tunnel101-192.0.2.1 socket is UP
%DMVPN-5-NHRP_NHS: Tunnel101 192.0.2.251 is UP
%DMVPN-5-NHRP_CACHE: Client 192.0.2.2 on Tunnel11 Registered.
%DMVPN-5-NHRP_CACHE: Client 192.0.2.2 on Tunnel11 came UP.
%DMVPN-3-NHRP_ERROR: Registration Request failed for 192.0.2.251 on Tunnel101
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug dmvpn</td>
<td>Debugs DMVPN sessions.</td>
</tr>
</tbody>
</table>
logging enabled

To enable syslog messages, use the `logging enabled` command in parameter-map-type consent configuration mode.

`logging enabled`

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Logging messages are not enabled.

**Command Modes**
Parameter-map-type consent (config-profile)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
After the `logging enabled` command is entered, a log entry (a syslog), including the client’s IP address and the time, is created every time a response is received for the consent web page.

**Examples**
The following example shows how to define the consent-specific parameter map “consent_parameter_map” and a default consent parameter map. In both parameter maps, logging is enabled.

```plaintext
parameter-map type consent consent_parameter_map
  authorize accept identity consent_identity_policy
  timeout file download 35791
  file flash:consent_page.html
  logging enabled
  exit
```

```plaintext
parameter-map type consent default
  authorize accept identity test_identity_policy
  timeout file download 35791
  file flash:consent_page.html
  logging enabled
  exit
```
logging ip access-list cache (global configuration)

To configure the Optimized ACL Logging (OAL) parameters, use the `logging ip access-list cache` command in global configuration mode. To return to the default settings, use the `no` form of this command.

```
logging ip access-list cache {entries entries|interval seconds|rate-limit pps|threshold packets}
no logging ip access-list cache [ {entries|interval|rate-limit|threshold} ]
```

**Syntax Description**

| entries entries | Specifies the maximum number of log entries that are cached in the software; valid values are from 0 to 1048576 entries. |
| interval seconds | Specifies the maximum time interval before an entry is sent to syslog; valid values are from 5 to 86400 seconds. |
| rate-limit pps   | Specifies the number of packets that are logged per second in the software; valid values are from 10 to 1000000 pps. |
| threshold packets| Specifies the number of packet matches before an entry is sent to syslog; valid values are from 1 to 1000000 packets. |

**Command Default**

The defaults are as follows:

- `entries` -- 8000 entries.
- `seconds` -- 300 seconds (5 minutes).
- `rate-limit` pps -- 0 (rate limiting is off) and all packets are logged.
- `threshold` packets -- 0 (rate limiting is off) and the system log is not triggered by the number of packet matches.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

OAL is supported on IPv4 unicast traffic only.

You cannot configure OAL and VACL capture on the same chassis. OAL and VACL capture are incompatible. With OAL configured, use SPAN to capture traffic.

If the entry is inactive for the duration that is specified in the `update-interval seconds` command, the entry is removed from the cache.

If you enter the `no logging ip access-list cache` command without keywords, all the parameters are returned to the default values.
You must set ICMP unreachable rate limiting to 0 if the OAL is configured to log denied packets.

When enabling the IP "too short" check using the mls verify ip length minimum command, valid IP packets with an IP protocol field of ICMP(1), IGMP(2), IP(4), TCP(6), UDP(17), IPv6(41), GRE(47), or SIPP-ESP(50) will be hardware switched. All other IP protocol fields are software switched.

---

**Caution**

Using optimized access-list logging (OAL) and the mls verify ip length minimum command together can cause routing protocol neighbor flapping as they are incompatible.

---

**Examples**

This example shows how to specify the maximum number of log entries that are cached in the software:

```
Router(config)#
logging ip access-list cache entries 200
```

This example shows how to specify the maximum time interval before an entry is sent to the system log:

```
Router(config)#
logging ip access-list cache interval 350
```

This example shows how to specify the number of packets that are logged per second in the software:

```
Router(config)#
logging ip access-list cache rate-limit 100
```

This example shows how to specify the number of packet matches before an entry is sent to the system log:

```
Router(config)#
logging ip access-list cache threshold 125
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear logging ip access-list cache</td>
<td>Clears all the entries from the OAL cache and sends them to the syslog.</td>
</tr>
<tr>
<td>logging ip access-list cache (interface configuration)</td>
<td>Enables an OAL-logging cache on an interface that is based on direction.</td>
</tr>
<tr>
<td>show logging ip access-list</td>
<td>Displays information about the logging IP access list.</td>
</tr>
<tr>
<td>update-interval seconds</td>
<td>Removes entries from the cache that are inactive for the duration that is specified in the command.</td>
</tr>
</tbody>
</table>
logging ip access-list cache (interface configuration)

To enable an Optimized ACL Logging (OAL)-logging cache on an interface that is based on direction, use the `logging ip access-list cache` command in interface configuration mode. To disable OAL, use the `no` form of this command.

```
logging ip access-list cache [in|out]
no logging ip access-list cache
```

**Syntax Description**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>in</strong></td>
<td>(Optional) Enables OAL on ingress packets.</td>
</tr>
<tr>
<td><strong>out</strong></td>
<td>(Optional) Enables OAL on egress packets.</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(17d)SXB</td>
<td>Support for this command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

This command is supported on traffic that matches the `log` keyword in the applied ACL. You must set ICMP unreachable rate limiting to 0 if the OAL is configured to log denied packets.

On systems that are configured with a PFC3A, support for the egress direction on tunnel interfaces is not supported.

OAL is supported on IPv4 unicast traffic only.

You cannot configure OAL and VACL capture on the same chassis. OAL and VACL capture are incompatible. With OAL configured, use SPAN to capture traffic.

If the entry is inactive for the duration that is specified in the `update-interval seconds` command, the entry is removed from the cache.

If you enter the `no logging ip access-list cache` command without keywords, all the parameters are returned to the default values.

When enabling the IP "too short" check using the `mls verify ip length minimum command`, valid IP packets with an IP protocol field of ICMP(1), IGMP(2), IP(4), TCP(6), UDP(17), IPv6(41), GRE(47), or SIPP-ESP(50) will be hardware switched. All other IP protocol fields are software switched.

**Caution**

Using optimized access-list logging (OAL) and the `mls verify ip length minimum command` together can cause routing protocol neighbor flapping as they are incompatible.
Examples

This example shows how to enable OAL on ingress packets:

Router(config-if)#
logging ip access-list cache in

This example shows how to enable OAL on egress packets:

Router(config-if)#
logging ip access-list cache out

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear logging ip access-list cache</td>
<td>Clears all the entries from the OAL cache and sends them to the syslog.</td>
</tr>
<tr>
<td>logging ip access-list cache (global configuration)</td>
<td>Configures the OAL parameters.</td>
</tr>
<tr>
<td>show logging ip access-list</td>
<td>Displays information about the logging IP access list.</td>
</tr>
<tr>
<td>update-interval seconds</td>
<td>Removes entries from the cache that are inactive for the duration that is specified in the command.</td>
</tr>
</tbody>
</table>
login authentication

To enable authentication, authorization, and accounting (AAA) authentication for logins, use the `login authentication` command inline configuration mode. To return to the default specified by the `aaa authentication login` command, use the `no` form of this command.

```
login authentication {default list-name}
no login authentication {default list-name}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default</code></td>
<td>Uses the default list created with the <code>aaa authentication login</code> command.</td>
</tr>
<tr>
<td><code>list-name</code></td>
<td>Uses the indicated list created with the <code>aaa authentication login</code> command.</td>
</tr>
</tbody>
</table>

**Command Default**

Uses the default set with `aaa authentication login`.

**Command Modes**

Line configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS release 12.(33)SRA.</td>
</tr>
<tr>
<td>12.2SX</td>
<td>This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is a per-line command used with AAA that specifies the name of a list of AAA authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line).

⚠️ **Caution**

If you use a `list-name` value that was not configured with the `aaa authentication login` command, you will disable login on this line.

Entering the `no` version of `login authentication` has the same effect as entering the command with the `default` keyword.

Before issuing this command, create a list of authentication processes by using the global configuration `aaa authentication login` command.

**Examples**

The following example specifies that the default AAA authentication is to be used on line 4:

```
line 4
login authentication default
```

The following example specifies that the AAA authentication list called `list1` is to be used on line 7:
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa authentication login</td>
<td>Sets AAA authentication at login.</td>
</tr>
</tbody>
</table>
login-auth-bypass

To configure the domain name and FQDN ACL that are to be bypassed for a parameter map, use the `login-auth-bypass fqdn` command in parameter map configuration mode.

```
login-auth-bypass ip-access-list  acl-name  domain-name-list  domain-name
```

**Syntax Description**

- `ip-access-list acl-name` Configures a FQDN standard, extended list to a named admission control rule. The value ranges from 1 through 199, or from 1300 through 2699 for expanded range.
- `domain-name-list  domain-name` Configures a domain.

**Command Default**

No domain name and FQDN ACL is defined for bypass.

**Command Modes**

Parameter map configuration mode (config-params-parameter-map)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 3E</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(2)S</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The FQDN ACL determines which IP addresses should redirect the BYOD to the ISE onboarding portal page. This ACL is same as the redirect ACL from ISE onboarding.

This example shows how to configure the domain name and FQDN ACL that are to be bypassed for a parameter map:

```
(config)# parameter-map type webauth Mymap
(config-params-parameter-map)# login auth-bypass ip-access-list byod domain-name-list abc
Device(config)# parameter-map type webauth Mymap
Device(config-params-parameter-map)# login auth-bypass ip-access-list byod domain-name-list abc
```
To configure your Cisco IOS device for login parameters that help provide denial-of-service (DoS) detection, use the `login block-for` command in global configuration mode. To disable the specified login parameters and return to the default functionality, use the `no` form of this command.

```bash
login block-for seconds attempts tries within seconds
no login block-for
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>Duration of time in which login attempts are denied (also known as a quiet period) by the Cisco IOS device. Valid values range from 1 to 65535 (18 hours) seconds.</td>
</tr>
<tr>
<td><code>attempts</code></td>
<td>Maximum number of failed login attempts that triggers the quiet period. Valid values range from 1 to 65535 tries.</td>
</tr>
<tr>
<td><code>tries</code></td>
<td>Duration of time in which the allowed number of failed login attempts must be made before the quiet period is triggered. Valid values range from 1 to 65535 (18 hours) seconds.</td>
</tr>
</tbody>
</table>

### Command Default

No login parameters are defined.

A quiet period is not enabled.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25).</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If the specified number of connection attempts (via the `attempts tries` option) fail within a specified time (via the `seconds` option), the Cisco IOS device will not accept any additional login attempts for a specified period of time (via the `seconds` argument).

All login parameters are disabled by default. You must issue the `login block-for` command, which enables default login functionality, before using any other login commands. After the `login block-for` command is enabled, the following defaults are enforced:

- A default login delay of 1 second
- All login attempts made via Telnet and secure shell (SSH) are denied during the quiet period; that is, no access control lists (ACLs) are exempt from the login period until the `login quiet-mode access-class` command is issued. If this command is not configured, then the default ACL `sl_def_acl` is created on
the router. This ACL is hidden in the running configuration. Use the `show access-list sl_def_acl` to view
the parameters for the default ACL.

For example:

```
Router# show access-lists sl_def_acl
Extended IP access list sl_def_acl
   10 deny tcp any any eq telnet
   20 deny tcp any any eq www
   30 deny tcp any any eq 22
   40 permit ip any any
```

**System Logging Messages**

The following logging message is generated after the router switches to quiet mode:

```
00:04:07:%SEC_LOGIN-1-QUIET_MODE_ON:Still time left for watching failures is 158 seconds, [user:sfd] [Source:10.4.2.11] [localport:23] [Reason:Invalid login], [ACL:22] at 16:17:23 UTC Wed Feb 26 2003
```

The following logging message is generated after the router switches from quiet mode back to normal mode:

```
00:09:07:%SEC_LOGIN-5-QUIET_MODE_OFF:Quiet Mode is OFF, because block period timed out at 16:22:23 UTC Wed Feb 26 2003
```

**Examples**

The following example shows how to configure your router to block all login requests for 100 seconds if 15 failed login attempts are exceeded within 100 seconds. Thereafter, the `show login` command is issued to verify the login settings.

```
Router(config)# login block-for 100 attempts 15 within 100
Router(config)# exit
Router# show login
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for 100 seconds.
Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5
```

The following example shows how to disable login parameters. Thereafter, the `show login` command is issued to verify that login parameters are no longer configured.

```
Router(config)# no login block-for
Router(config)# exit
Router# show login
No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps
Router NOT enabled to watch for login Attacks
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>login delay</td>
<td>Configures a uniform delay between successive login attempts.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>login quiet-mode access-class</td>
<td>Specifies an ACL that is to be applied to the router when it switches to quiet mode.</td>
</tr>
<tr>
<td>show login</td>
<td>Displays login parameters.</td>
</tr>
</tbody>
</table>
**login delay**

To configure a uniform delay between successive login attempts, use the `login delay` command in global configuration mode. To return to the default functionality (which is a 1 second delay), use the `no` form of this command.

```
login delay seconds
no login delay
```

**Syntax Description**

| seconds | Number of seconds between each login attempt. Valid values range from 1 to 10 seconds. |

**Command Default**

If this command is not enabled, a login delay of 1 second is automatically enforced.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A Cisco IOS device can accept connections (such as Telnet, secure shell (SSH), and HTTP) as fast as they can be processed. The `login delay` command introduces a uniform delay between successive login attempts. (The delay occurs for all login attempts--failed or successful attempts.) Thus, user users can better secure their Cisco IOS device from dictionary attacks, which are an attempt to gain username and password access to your device.

Although the `login delay` command allows users to configure a specific a delay, a uniform delay of 1 second is enabled if the `auto secure` command is issued. After the `auto secure` command is enabled, the autosecure dialog prompts users for login parameters; if login parameters have already been configured, the autosecure dialog will retain the specified values.

**Examples**

The following example shows how to configure your router to issue a delay of 10 seconds between each successive login attempt:

```
Router(config)# login delay 10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>auto secure</code></td>
<td>Secures the management and forwarding planes of the router.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>login block-for</td>
<td>Configures your Cisco IOS device for login parameters that help provide DoS detection.</td>
</tr>
<tr>
<td>show login</td>
<td>Displays login parameters.</td>
</tr>
</tbody>
</table>
login-message

To configure a login message for the text box on the user login page, use the `login-message` command in webvpn context configuration mode. To reconfigure the SSL VPN context configuration to display the default message, use the `no` form of this command.

```
login-message [message-string]
no login-message [message-string]
```

### Syntax Description

| message-string | (Optional) Login message string up to 255 characters in length. The string value may contain 7-bit ASCII values, HTML tags, and escape sequences. |

### Command Default

The following message is displayed if this command is not configured or if the `no` form is entered:

“Please enter your username and password”

### Command Modes

Webvpn context configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The optional form of this command is used to change or enter a login message. A text string up to 255 characters in length can be entered. The `no` form of this command is entered to configure the default message to be displayed. When the `login-message` command is entered without the optional text string, no login message is displayed.

### Examples

The following example changes the default login message to “Please enter your login credentials”:

```
Router(config)#
webvpn context context1

Router(config-webvpn-context)# login-message "Please enter your login credentials"
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>webvpn context</td>
<td>Enters webvpn context configuration mode to configure the SSL VPN context.</td>
</tr>
</tbody>
</table>
login quiet-mode access-class

To specify an access control list (ACL) that is to be applied to the router when the router switches to quiet mode, use the `login quiet-mode access-class` command in global configuration mode. To remove this ACL and allow the router to deny all login attempts, use the `no` form of this command.

```
login quiet-mode access-class {acl-name|acl-number}
no login quiet-mode access-class {acl-name|acl-number}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl-name</td>
<td>Named ACL that is to be enforced during quiet mode.</td>
</tr>
<tr>
<td>acl-number</td>
<td>Numbered (standard or extended) ACL that is to be enforced during quiet mode.</td>
</tr>
</tbody>
</table>

**Command Default**

All login attempts via Telnet, secure shell (SSH), and HTTP are denied.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This command was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This command was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
<tr>
<td>12.2(33)SRA</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SRA.</td>
</tr>
<tr>
<td>12.2(33)SXH</td>
<td>This command was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before using this command, you must issue the `login block-for` command, which allows you to specify the necessary parameters to enable a quiet period.

- Use the `login quiet-mode access-class` command to selectively allow hosts on the basis of a specified ACL. You may use this command to grant an active client or list of clients an infinite number of failed attempts that are not counted by the router; that is, the active clients are placed on a “safe list” that allows them access to the router despite a quiet period. If this command is not configured, then the default ACL `sl_def_acl` is created on the router. This ACL is hidden in the running configuration. Use the `show access-list sl_def_acl` to view the parameters for the default ACL.

For example:

```
Router#show access-lists sl_def_acl
Extended IP access list sl_def_acl
10 deny tcp any any eq telnet
20 deny tcp any any eq www
30 deny tcp any any eq 22
40 permit ip any any
```

**System Logging Messages**

The following logging message is generated after the router switches to quiet mode:

K through L
00:04:07:%SEC_LOGIN-1-QUIET_MODE_ON: Still time left for watching failures is 158 seconds, [user:sfd] [Source: 10.4.2.11] [localport: 23] [Reason: Invalid login], [ACL: 22] at 16:17:23 UTC Wed Feb 26 2003

The following logging message is generated after the router switches from quiet mode back to normal mode:

00:09:07:%SEC_LOGIN-5-QUIET_MODE_OFF: Quiet Mode is OFF, because block period timed out at 16:22:23 UTC Wed Feb 26 2003

Examples

The following example shows how to configure your router to accept hosts only from the ACL “myacl” during the next quiet period:

Router(config)# login quiet-mode access-class myacl

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>login block-for</td>
<td>Configures your Cisco IOS device for login parameters that help provide DoS detection.</td>
</tr>
<tr>
<td>show login</td>
<td>Displays login parameters.</td>
</tr>
</tbody>
</table>
login-photo

To set the photo parameters on a Secure Socket Layer Virtual Private Network (SSL VPN) login page, use the `login-photo` command in web vpn context configuration mode. To display the login page with no photo but with a message that spans the message and the photo columns, use the `no` form of this command.

```
login-photo [{file file-name|none}]
no login-photo
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>file file-name</code></td>
<td>Points to a file to be displayed on the login page. The <code>file-name</code> argument can be <code>jpeg</code>, <code>bitmap</code>, or <code>gif</code>. However, <code>gif</code> files are recommended.</td>
</tr>
<tr>
<td><code>none</code></td>
<td>No photo appears on the login page.</td>
</tr>
</tbody>
</table>

### Command Default

No photo appears, and the message spans the two columns (message and photo columns).

### Command Modes

Webvpn context configuration (config-webvpn-context)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(15)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To display no photo, use the `login-photo none` option. To display no photo and have the message span both columns (message column and photo column), use the `no login-photo` option.

The best resolution for login photos is 179 x 152 pixels.

### Examples

The following example shows that no photo is displayed:

```
Router (config)# webvpn context
Router (config-webvpn-context)# login-photo none
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>webvpn context</code></td>
<td>Enters webvpn context configuration mode to configure the SSL VPN context.</td>
</tr>
</tbody>
</table>
To configure a custom logo to be displayed on the login and portal pages of an SSL VPN, use the `logo` command in SSLVPN configuration mode. To configure the Cisco logo to be displayed, use the `no` form of this command.

```
logo [{file filename|none}]
no logo [{file filename|none}]  
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>filename</code></td>
<td>(Optional) Specifies the location of an image file. A gif, jpg, or png file can be specified. The file can be up to 100 KB in size. The name of the file can be up 255 characters in length.</td>
</tr>
<tr>
<td><code>none</code></td>
<td>(Optional) No logo is displayed.</td>
</tr>
</tbody>
</table>

### Command Default

The Cisco logo is displayed if the `no` form of this command is not configured or if the `no` form is entered.

### Command Modes

SSLVPN configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(14)T</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The source image file for the logo is a gif, jpg, or png file that is up to 255 characters in length (`filename`) and up to 100 kilobytes (KB) in size. The file is referenced from a local file system, such as flash memory. An error message will be displayed if the file is not referenced from a local file system. No logo will be displayed if the image file is removed from the local file system.

### Examples

The following example references `mylogo.gif` (from flash memory) to use as the SSL VPN logo:

```
Router(config)#
webvpn context SSLVPN

Router(config-webvpn-context)#
logo file flash:/mylogo.gif
```

In the following example, no logo is to be displayed on the login or portal pages:

```
Router(config)#
webvpn context SSLVPN

Router(config-webvpn-context)#
logo none
```

The following example configures the SSL VPN to display the default logo (Cisco) on the login and portal pages:

```
Router(config)#
webvpn context SSLVPN
```

```
Router(config-webvpn-context)#
logo
```
Router(config)#
webvpn context SSLVPN

Router(config-webvpn-context)#
logo none
Router(config-webvpn-context)#

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>webvpn context</td>
<td>Enters SSLVPN configuration mode to configure the WebVPN context.</td>
</tr>
</tbody>
</table>