C Commands

cipher suite

To configure a cipher suite for encrypting traffic with MACsec, use the **cipher suite** command. To reset the cipher suite to its default value, use the **no** form of this command.

cipher suite {**GCM-AES-128** | **GCM-AES-256** | **GCM-AES-XPN-128** | **GCM-AES-XPN-256**}

no cipher suite {**GCM-AES-128** | **GCM-AES-256** | **GCM-AES-XPN-128** | **GCM-AES-XPN-256**}

Syntax Description

GCM-AES-128	Specifies the Galois/Counter Mode (GCM) encryption method, Advanced Encryption Standard (AES) encryption algorithm, and 128-bit encryption.
GCM-AES-256	Specifies the GCM encryption method, AES encryption algorithm, and 256-bit encryption.
GCM-AES-XPN-128	Specifies the GCM encryption method, AES encryption algorithm that uses Extended Packet Numbering (XPN) of 64 bits, and 128-bit encryption.
GCM-AES-XPN-256	Specifies the GCM encryption method, AES encryption algorithm that uses Extended Packet Numbering (XPN) of 64 bits, and 256-bit encryption.

[1]

Command Default

The default cipher suite chosen for encryption is GCM-AES-XPN-256.

Command Modes

MACsec policy configuration (config-macsec-policy)

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

To use this command, you should enable the MACsec Key Agreement (MKA) feature first.

[1]
- GCM indicates the encryption method.
- AES and AES-XPN indicates the hash or integrity algorithm.
- The numeral indicates the length of the cipher.

Examples

This example shows how to configure a cipher suite:

```
switch# configure terminal
switch(config)# macsec policy p1
switch(config-macsec-policy)# cipher suite GCM-AES-XPN-128
```

Related Commands

Command	Description
feature mka	Enables the MKA feature.
key	Creates a key or enters the configuration mode of an existing key.
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.
macsec keychain policy	Configures a MACsec keychain policy.
macsec policy	Configures a MACsec policy.
show key chain	Displays the configuration of the specified keychain.
show macsec mka	Displays the details of MKA.
show macsec policy	Displays all the MACsec policies in the system.
show run mka	Displays the status of MKA.

clear access-list counters

To clear the counters for all IPv4, IPv6, and MAC access control lists (ACLs) or a single ACL, use the **clear access-list counters** command.

clear access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the ACL whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(2)	Added support for clearing IPv6 ACL counters.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear counters for all IPv4, IPv6, and MAC ACLs:

```
switch# clear access-list counters
switch#
```

This example shows how to clear counters for an IPv4 ACL named acl-ipv4-01:

```
switch# clear access-list counters acl-ipv4-01
switch#
```

Related Commands

Command	Description
clear ip access-list counters	Clears counters for IPv4 ACLs.
clear ipv6 access-list counters	Clears counters for IPv6 ACLs.
clear mac access-list counters	Clears counters for MAC ACLs.

Command	Description
clear vlan access-list counters	Clears counters for VACLs.
show access-lists	Displays information about one or all IPv4, IPv6, and MAC ACLs.

clear accounting log

To clear the accounting log, use the **clear accounting log** command.

clear accounting log [logflash]

Syntax Description

logflash	(Optional) Clears the accounting log stored in the logflash for the current VDC.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(2)	The **logflash** keyword was added.
4.0(1)	This command was introduced.

Usage Guidelines

The **clear accounting log** command operates only in the default virtual device context (VDC 1).

This command does not require a license.

Examples

This example shows how to clear the accounting log:

```
switch# clear accounting log
```

Related Commands

Command	Description
show accounting log	Displays the accounting log contents.

clear copp statistics

To clear control plane policing (CoPP) statistics, use the **clear copp statistics** command.

clear copp statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to specify a control plane class map and enter class map configuration mode:

```
switch# clear copp statistics
```

Related Commands

Command	Description
show policy-map interface control-plane	Displays the CoPP statistics for interfaces.

clear cts cache

To clear the Cisco TrustSec authentication and authorization information cache, use the **clear cts cache** command.

clear cts cache

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to clear the Cisco TrustSec authentication and authorization cache:

```
switch# clear cts cache
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

clear cts policy

To clear the Cisco TrustSec security group access control list (SGACL) policies, use the **clear cts policy** command.

clear cts policy {**all**| **peer** *device-id*| **sgt** *sgt-value*}

Syntax Description

all	Clears all the Cisco TrustSec SGACL policies on the local device.
peer *device-id*	Clears the Cisco TrustSec SGACL policies for a peer device on the local device.
sgt *sgt-value*	Clears the Cisco TrustSec SGACL policies for a security group tag (SGT) on the local device.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to clear all the Cisco TrustSec SGACL policies on the device:

```
switch# clear cts policy all
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based policy	Displays Cisco TrustSec SGACL policy information.

capture session

To enable a capture session for the access control list (ACL), use the capture session command.

capture session session

Syntax Description

session	Session ID. The range is from 1 to 48.

Command Default

None

Command Modes

ACL capture configuration mode (config-acl-capture)

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure an ACL capture session configuration:

```
switch# configure terminal
switch(config)# ip access-list abc1234
switch(config-acl)# capture session 7
switch(config-acl)#
```

Related Commands

Command	Description
ip access-list	Creates an access list.
monitor session session type acl-capture	Configures an ACL capture session.

cts dot1x

To enable Cisco TrustSec authentication on an interface and enter Cisco TrustSec 802.1X configuration mode, use the **cts dot1x** command. To revert to the default, use the **no** form of this command.

cts dot1x

no cts dot1x

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command is not supported for F1 Series modules and F2 Series modules.

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

After using this command, you must enable and disable the interface using the **shutdown**/**no shutdown** command sequence for the configuration to take effect.

This command requires the Advanced Services license.

Examples

This example shows how to enable Cisco TrustSec authentication on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to disable Cisco TrustSec authentication on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no cts dot1x
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

Command	Description
feature cts	Enables the Cisco TrustSec feature.

Command	Description
show cts interface	Displays Cisco TrustSec configuration information for interfaces.

Related Commands

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

You can use only IPv4 addressing with Cisco TrustSec.

This command requires the Advanced Services license.

Examples

This example shows how to configure Layer 3 Cisco TrustSec global mapping for an SPI and subnet:

```
switch# config t
switch(config)# cts l3 spi 3 10.10.1.1/23
```

This example shows how to remove Layer 3 global mapping for a subnet:

```
switch# config t
switch(config)# no cts l3 spi 10.10.1.1/23
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts l3 mapping	Displays the Layer 3 Cisco TrustSec mapping for SPI values to IPv4 subnets.

class (policy map)

To specify a control plane class map for a control plane policy map, use the **class** command. To delete a control plane class map from a control plane policy map, use the **no** form of this command.

class {*class-map-name* [**insert-before** *class-map-name2*]| **class-default**}

no class *class-map-name*

Syntax Description

class-map-name	Name of the class map.
insert-before *class-map-name2*	(Optional) Inserts the control plane class map ahead of another control plane class map for the control plane policy map.
class-default	Specifies the default class.

Command Default

None

Command Modes

Policy map configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to configure a class map for a control plane policy map:

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
swtich(config-pmap-c)
```

This example shows how to delete a class map from a control plane policy map:

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# no class ClassMapA
```

Related Commands

Command	Description
policy-map type control-plane	Specifies a control plane policy map and enters policy map configuration mode.
show policy-map type control-plane	Displays configuration information for control plane policy maps.

class-map type control-plane

To create or specify a control plane class map and enter class map configuration mode, use the **class-map type control-plane** command. To delete a control plane class map, use the **no** form of this command.

class-map type control-plane [**match-all| match-any**] *class-map-name*

no class-map type control-plane [**match-all| match-any**] *class-map-name*

Syntax Description

match-all	(Optional) Specifies to match all match conditions in the class map.
match-any	(Optional) Specifies to match any match conditions in the class map.
class-map-name	Name of the class map. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.

Command Default

match-any

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You cannot use match-all, match-any, or class-default as names for control plane class maps.

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to specify a control plane class map and enter class map configuration mode:

```
switch# configure terminal
switch(config)# class-map type control-plane ClassMapA
switch(config-cmap)#
```

This example shows how to delete a control plane class map:

```
switch# configure terminal
switch(config)# no class-map type control-plane ClassMapA
```

Related Commands

Command	Description
show class-map type control-plane	Displays control plane policy map configuration information.

clear aaa local user blocked

To clear the blocked local user, use the **clear local user blocked** command.

clear local user blocked username {**all**| **username**}

Syntax Description

all	Clears all the blocked users.
username	Clears the specified user.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to clear all the blocked users.

```
switch# clear aaa local user blocked all
```

Related Commands

Command	Description
aaa authentication rejected	Configures the login block per user.
show aaa authentication	Displays the AAA authentication configuration.
show aaa local user blocked	Displays the blocked local users.

clear ldap-server statistics

To clear the Lightweight Directory Access Protocol (LDAP) server statistics, use the **clear ldap-server statistics** command.

clear ldap-server statistics {**ipv4-address| ipv6-address| host-name**}

Syntax Description

ipv4-address	Server IPv4 address in the *A.B.C.D* format.
ipv6-address	Server IPv6 address in the *X:X:X:X* format.
host-name	Server name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear the statistics for an LDAP server:

```
switch# clear ldap-server statistics 10.10.1.1
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap-server host	Specifies the IPv4 or IPv6 address or hostname for an LDAP server.
show ldap-server **statistics**	Displays the LDAP server statistics.

clear mac access-list counters

To clear the counters for all MAC access control lists (ACLs) or a single MAC ACL, use the **clear mac access-list counters** command.

clear mac access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the MAC ACL whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear counters for all MAC ACLs:

```
switch# clear mac access-list counters
switch#
```

This example shows how to clear counters for a MAC ACL named acl-mac-0060:

```
switch# clear mac access-list counters acl-ipv4-0060
switch#
```

Related Commands

Command	Description
clear access-list counters	Clears counters for IPv4, IPv6, and MAC ACLs.
clear ip access-list counters	Clears counters for IPv4 ACLs.
clear ipv6 access-list counters	Clears counters for IPv6 ACLs.
clear vlan access-list counters	Clears counters for VACLs.

Command	Description
show access-lists	Displays information about one or all IPv4, IPv6, and MAC ACLs.
show mac access-lists	Displays information about one or all MAC ACLs.

clear port-security

To clear a single, dynamically learned, secure MAC address or to clear all dynamically learned, secure MAC addresses for a specific interface, use the **clear port-security** command.

clear port-security dynamic interface ethernet slot / **port** [**vlan vlan-id**]

clear port-security dynamic interface port-channel *channel-number* [**vlan** *vlan-id*]

clear port-security dynamic address *address* [**vlan** *vlan-id*]

Syntax Description

dynamic	Specifies that you want to clear dynamically learned, secure MAC addresses.
interface	Specifies the interface of the dynamically learned, secure MAC addresses that you want to clear.
ethernet *slot*/*port*	Specifies the Ethernet interface of the dynamically learned, secure MAC addresses that you want to clear.
vlan *vlan-id*	(Optional) Specifies the VLAN of the secure MAC addresses to be cleared. Valid VLAN IDs are from 1 to 4096.
port-channel *channel-number*	Specifies the port-channel interface of the dynamically learned, secure MAC addresses that you want to clear.
address *address*	Specifies a single MAC address to be cleared, where *address* is the MAC address, in dotted hexadecimal format.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	Support was added for port-security on port-channel interfaces.
4.0(1)	This command was introduced.

Usage Guidelines

You must enable port security by using the **feature port-security** command before you can use the **clear port-security** command.

This command does not require a license.

Examples

This example shows how to remove dynamically learned, secure MAC addresses from the Ethernet 2/1 interface:

```
switch# configure terminal
switch(config)# clear port-security dynamic interface ethernet 2/1
```

This example shows how to remove the dynamically learned, secure MAC address 0019.D2D0.00AE:

```
switch# configure terminal
switch(config)# clear port-security dynamic address 0019.D2D0.00AE
```

Related Commands

Command	Description
debug port-security	Provides debugging information for port security.
feature port-security	Enables port security globally.
show port-security	Shows information about port security.
switchport port-security	Enables port security on a Layer 2 interface.

clear cts role-based counters

To clear the role-based access control list (RBACL) statistics so that all counters are reset to 0, use the **clear cts role-based counters** command.

clear cts role-based counters

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command requires the Advanced Services license.

Examples

This example shows how to clear the RBACL statistics:

```
switch# clear cts role-based counters
```

Related Commands

Command	Description
cts role-based counters enable	Enables the RBACL statistics.
show cts role-based counters	Displays the configuration status of RBACL statistics and lists statistics for all RBACL policies.

clear dot1x

To clear 802.1X authenticator instances, use the **clear dot1x** command.

cleardot1x{**all**| **interface** | *slot/port*}

Syntax Description

all	Specifies all 802.1X authenticator instances.
interface ethernet *slot*/*port*	Specifies the 802.1X authenticator instances for a specified interface.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to clear all 802.1X authenticator instances:

```
switch# clear dot1x all
```

This example shows how to clear the 802.1X authenticator instances for an interface:

```
switch# clear dot1x interface ethernet 1/1
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

clear eou

To clear Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) sessions, use the **clear eou** command.

clear eou {**all**| **authentication** {**clientless**| **eap**| **static**}| **interface ethernet slot / port**| **ip-address ipv4-address**| **mac-address mac-address**| **posturetoken type**}

Syntax Description

all	Specifies all EAPoUDP sessions.
authentication	Specifies EAPoUDP authentication.
clientless	Specifies sessions authenticated using clientless posture validation.
eap	Specifies sessions authenticated using EAPoUDP.
static	Specifies sessions authenticated using statically configured exception lists.
interface ethernet *slot/port*	Specifies an interface.
ip-address *ipv4-address*	Specifies an IPv4 address. in the A.B.C.D format.
mac-address *mac-address*	Specifies a MAC address.
posturetoken *type*	Specifies a posture token name.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable EAPoUDP by using the **feature eou** command before using the **clear eou** command.

This command does not require a license.

Examples

This example shows how to clear all the EAPoUDP sessions:

```
switch# clear eou all
```

This example shows how to clear the statically authenticated EAPoUDP sessions:

```
switch# clear eou authentication static
```

This example shows how to clear the EAPoUDP sessions for an interface:

```
switch# clear eou interface ethernet 1/1
```

This example shows how to clear the EAPoUDP sessions for an IP address:

```
switch# clear eou ip-address 10.10.1.1
```

This example shows how to clear the EAPoUDP sessions for a MAC address:

```
switch# clear eou mac-address 0019.076c.dac4
```

This example shows how to the EAPoUDP sessions with a posture token type of checkup:

```
switch# clear eou posturetoken healthy
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
show eou	Displays EAPoUDP information.

clear hardware rate-limiter

To clear rate-limit statistics, use the **clear hardware rate-limiter** command.

clear hardware rate-limiter {**access-list-log**| **all**| **copy**| **layer-2** {**l2pt**| **mcast-snooping**| **port-security**| **storm-control**| **vpc-low**}| **layer-3** {**control**| **glean**| **glean-fast**| **mtu**| **multicast** {**directly-connected**| **local-groups**| **rpf-leak**}| **ttl**}| **receive**}

Syntax Description

access-list-log	Clears rate-limit statistics for access-list log packets.
all	Clears all rate-limit statistics.
copy	Clears rate-limit statistics for copy packets.
layer-2	Specifies Layer 2 packet rate limits.
l2pt	Clears rate-limit statistics for Layer 2 Tunnel Protocol (L2TP) packets.
mcast-snooping	Clears rate-limit statistics for Layer 2 multicast-snooping packets.
port-security	Clears rate-limit statistics for Layer 2 port-security packets.
storm-control	Clears rate-limit statistics for Layer 2 storm-control packets.
vpc-low	Clears rate-limit statistics for Layer 2 control packets over the VPC low queue.
layer-3	Specifies Layer 3 packet rate limits.
control	Clears rate-limit statistics for Layer 3 control packets.
glean	Clears rate-limit statistics for Layer 3 glean packets.
glean-fast	Clears rate-limit statistics for Layer 3 glean fast-path packets.
mtu	Clears rate-limit statistics for Layer 3 maximum transmission unit (MTU) packets.
multicast	Specifies Layer 3 multicast rate limits.
directly-connected	Clears rate-limit statistics for Layer 3 directly connected multicast packets.

local-groups	Clears rate-limit statistics for Layer 3 local group multicast packets.
rpf-leak	Clears rate-limit statistics for Layer 3 reverse path forwarding (RPF) leak multicast packets.
ttl	Clears rate-limit statistics for Layer 3 time-to-live (TTL) packets.
receive	Clears rate-limit statistics for receive packets.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.2(2)	Added the glean-fast keyword.
5.0(2)	Added the **l2pt** keyword.
4.0(3)	Added the **port-security** keyword.
4.0(1)	This command was introduced.

Usage Guidelines

You can use the command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to clear all the rate-limit statistics:

```
switch# clear hardware rate-limiter all
```

This example shows how to clear the rate-limit statistics for access-list log packets:

```
switch# clear hardware rate-limiter access-list-log
```

This example shows how to clear the rate-limit statistics for Layer 2 storm-control packets:

```
switch# clear hardware rate-limiter layer-2 storm-control
```

This example shows how to clear the rate-limit statistics for Layer 3 glean packets:

```
switch# clear hardware rate-limiter layer-3 glean
```

This example shows how to clear the rate-limit statistics for Layer 3 directly connected multicast packets:

```
switch# clear hardware rate-limiter layer-3 multicast directly-connected
```

This example shows how to clear the rate-limit statistics for received packets:

```
switch# clear hardware rate-limiter receive
```

Related Commands

Command	Description
hardware rate-limiter	Configures rate limits.
show hardware rate-limiter	Displays rate-limit information.

clear ip arp inspection log

To clear the Dynamic ARP Inspection (DAI) logging buffer, use the **clear ip arp inspection log** command.

clear ip arp inspection log

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear the DAI logging buffer:

```
switch# clear ip arp inspection log
switch#
```

Related Commands

Command	Description
ip arp inspection log-buffer	Configures the DAI logging buffer size.
show ip arp inspection	Displays the DAI configuration status.
show ip arp inspection log	Displays the DAI log configuration.
show ip arp inspection statistics	Displays the DAI statistics.

clear ip access-list counters

To clear the counters for all IPv4 access control lists (ACLs) or a single IPv4 ACL, use the **clear ip access-list counters** command.

clear ip access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the IPv4 ACL whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear counters for all IPv4 ACLs:

```
switch# clear ip access-list counters
switch#
```

This example shows how to clear counters for an IP ACL named acl-ipv4-101:

```
switch# clear ip access-list counters acl-ipv4-101
switch#
```

Related Commands

Command	Description
clear access-list counters	Clears counters for IPv4, IPv6, and MAC ACLs.
clear ipv6 access-list counters	Clears counters for IPv6 ACLs.
clear mac access-list counters	Clears counters for MAC ACLs.
clear vlan access-list counters	Clears counters for VACLs.

Command	Description
show access-lists	Displays information about one or all IPv4, IPv6, and MAC ACLs.
show ip access-lists	Displays information about one or all IPv4 ACLs.

clear ip arp inspection statistics vlan

To clear the Dynamic ARP Inspection (DAI) statistics for a specified VLAN, use the **clear ip arp inspection statistics vlan** command.

clear ip arp inspection statistics vlan *vlan-list*

Syntax Description

vlan *vlan-list*	Specifies the VLANs whose DAI statistics this command clears. The *vlan-list* argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges (see the "Examples" section). Valid VLAN IDs are from 1 to 4094.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear the DAI statistics for VLAN 2:

```
switch# clear ip arp inspection statistics vlan 2
switch#
```

This example shows how to clear the DAI statistics for VLANs 5 through 12:

```
switch# clear ip arp inspection statistics vlan 5-12
switch#
```

This example shows how to clear the DAI statistics for VLAN 2 and VLANs 5 through 12:

```
switch# clear ip arp inspection statistics vlan 2,5-12
switch#
```

Related Commands

Command	Description
clear ip arp inspection log	Clears the DAI logging buffer.

Command	Description
ip arp inspection log-buffer	Configures the DAI logging buffer size.
show ip arp inspection	Displays the DAI configuration status.
show ip arp inspection vlan	Displays DAI status for a specified list of VLANs.

clear ip device tracking

To clear IP device tracking information, use the **clear ip device tracking** command.

clear ip device tracking {**all**| **interface ethernet slot / port**| **ip-address ipv4-address**| **mac-address mac-address**}

Syntax Description

all	Clears all IP device tracking information.
interface ethernet *slot/port*	Clears IP device tracking information for an interface.
ip-address *ipv4-address*	Clears IP device tracking information for an IPv4 address in the A.B.C.D format.
mac-address *mac-address*	Clears IP tracking information for a MAC address in the XXXX.XXXX.XXXX format.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear all the IP device tracking information:

```
switch# clear ip device tracking all
```

This example shows how to clear the IP device tracking information for an interface:

```
switch# clear ip device tracking interface ethernet 1/1
```

This example shows how to clear the IP device tracking information for an IP address:

```
switch# clear ip device tracking ip-address 10.10.1.1
```

This example shows how to clear the IP device tracking information for a MAC address:

```
switch# clear ip device tracking mac-address 000c.30da.86f4
```

Related Commands

Command	Description
ip device tracking	Enables IP device tracking.
show ip device tracking	Displays IP device tracking information.

clear ip dhcp relay statistics

To clear the DHCP relay statistics, use the **clear ip dhcp relay statistics** command.

clear ip dhcp relay statistics [**interface interface**]

Syntax Description

interface *interface*	(Optional) Clears the DHCP relay statistics for a specific interface. The supported interface types are ethernet, port-channel, and VLAN.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear the global DHCP relay statistics:

```
switch# clear ip dhcp relay statistics
```

Related Commands

Command	Description
ip dhcp relay	Enables the DHCP relay agent.
show ip dhcp relay statistics	Displays the DHCP relay statistics.

clear ip dhcp snooping binding

To clear the DHCP snooping binding database, use the **clear ip dhcp snooping binding** command.

clear ip dhcp snooping binding

clear ip dhcp snooping binding [**vlan vlan-id mac mac-address ip ip-address interface ethernet slot** / **port** [. **subinterface-number**]]

clear ip dhcp snooping binding [**vlan** *vlan-id* **mac** *mac-address* **ip** *ip-address* **interface port-channel** *channel-number* [. *subchannel-number*]]

Syntax Description

vlan *vlan-id*	(Optional) Clears the DHCP snooping binding database for an entry identified with the VLAN ID specified by the *vlan-id* argument and the additional keywords and arguments that follow.
mac-address *mac-address*	Specifies the MAC address of the binding database entry to be cleared. Enter the *mac-address* argument in dotted hexadecimal format.
ip *ip-address*	Specifies the IPv4 address of the binding database entry to be cleared. Enter the *ip-address* argument in dotted decimal format.
interface ethernet *slot*/*port*	(Optional) Specifies the Ethernet interface of the binding database entry to be cleared.
.*subinterface-number*	(Optional) Number of the Ethernet-interface subinterface. **Note** The dot separator is required between the *port* and *subinterface-number* arguments.
interface port-channel *channel-number*	(Optional) Specifies the Ethernet port-channel of the binding database entry to be cleared.
.*subchannel-number*	(Optional) Number of the Ethernet port-channel subchannel. **Note** The dot separator is required between the *channel-number* and *subchannel-number* arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(3)	This command was modified to support clearing a specific binding database entry. The optional **vlan** keyword and the arguments and keywords that follow it were added.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear the DHCP snooping binding database:

```
switch# clear ip dhcp snooping binding
switch#
```

This example shows how to clear a specific entry from the DHCP snooping binding database:

```
switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9 interface
ethernet 2/11
switch#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping on the device.
show ip dhcp snooping	Displays general information about DHCP snooping.
show ip dhcp snooping binding	Displays IP-MAC address bindings, including the static IP source entries.
show ip dhcp snooping statistics	Displays DHCP snooping statistics.
show running-config dhcp	Displays DHCP snooping configuration, including the IP Source Guard configuration.

clear ipv6 access-list counters

To clear the counters for all IPv6 access control lists (ACLs) or a single IPv6 ACL, use the **clear ipv6 access-list counters** command.

clear ipv6 access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the IPv6 ACL whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear counters for all IPv6 ACLs:

```
switch# clear ipv6 access-list counters
switch#
```

This example shows how to clear counters for an IPv6 ACL named acl-ipv6-3A:

```
switch# clear ipv6 access-list counters acl-ipv6-3A
switch#
```

Related Commands

Command	Description
clear access-list counters	Clears counters for IPv4, IPv6, and MAC ACLs.
clear ip access-list counters	Clears counters for IPv4 ACLs.
clear mac access-list counters	Clears counters for MAC ACLs.
clear vlan access-list counters	Clears counters for VACLs.

Command	Description
show access-lists	Displays information about one or all IPv4, IPv6, and MAC ACLs.
show ipv6 access-lists	Displays information about one or all IPv6 ACLs.

clear ipv6 dhcp relay statistics

To clear the DHCPv6 relay statistics, use the **clear ipv6 dhcp relay statistics** command.

clear ipv6 dhcp relay statistics [**interface interface**]

Syntax Description

interface *interface*	(Optional) Clears the DHCPv6 relay statistics for a specific interface. The supported interface types are ethernet, port-channel, and VLAN.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear the global DHCPv6 relay statistics:

```
switch# clear ipv6 dhcp relay statistics
```

Related Commands

Command	Description
ipv6 dhcp relay	Enables the DHCPv6 relay agent.
show ipv6 dhcp relay statistics	Displays the DHCPv6 relay statistics.

clear ipv6 dhcp-ldra statistics

To clear Lightweight DHCPv6 Relay Agent (LDRA) related statistics, use the clear ipv6 dhcp-ldra statistics command.

clear ipv6 dhcp-ldra statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the DHCP feature and LDRA feature.

Examples

This example shows how to clear the LDRA related statistics:

```
switch# clear ipv6 dhcp-ldra statistics
```

Related Commands

Command	Description
show ipv6 dhcp-ldra	Displays the configuration details of LDRA.

clear vlan access-list counters

To clear the counters for all VLAN access control lists (VACLs) or a single VACL, use the **clear vlan access-list counters** command.

clear vlan access-list counters [*access-map-name*]

Syntax Description

access-map-name	(Optional) Name of the VLAN access map whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear counters for all VACLs:

```
switch# clear vlan access-list counters
switch#
```

This example shows how to clear counters for a VACL named vlan-map-101:

```
switch# clear vlan access-list counters vlan-map-101
switch#
```

Related Commands

Command	Description
clear access-list counters	Clears counters for IPv4, IPv6, and MAC ACLs.
clear ip access-list counters	Clears counters for IPv4 ACLs.
clear ipv6 access-list counters	Clears counters for IPv6 ACLs.
clear mac access-list counters	Clears counters for MAC ACLs.

Command	Description
show access-lists	Displays information about one or all IPv4, IPv6, and MAC ACLs.
show vlan access-map	Displays information about one or all VACLs.

conf-offset

To configure the confidentiality offset for MACsec Key Agreement (MKA) encryption, use the **conf-offset** command. To disable the confidentiality offset, use the **no** form of this command.

conf-offset {**CONF-OFFSET-0** | **CONF-OFFSET-30** | **CONF-OFFSET-50**}

no conf-offset {**CONF-OFFSET-0** | **CONF-OFFSET-30** | **CONF-OFFSET-50**}

Syntax Description

CONF-OFFSET-0	Does not offset the encryption.
CONF-OFFSET-30	Offsets the encryption by 30 characters.
CONF-OFFSET-50	Offsets the encryption by 50 characters.

Command Default

No confidentiality offset is configured for MKA encryption.

Command Modes

MACsec policy configuration (config-macsec-policy)

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

To use this command, you should enable the MKA feature first.

Examples

This example shows how to set the confidentiality offset:

```
switch# configure terminal
switch(config)# macsec policy p1
switch(config-macsec-policy)# conf-offset CONF-OFFSET-0
```

Related Commands

Command	Description
feature mka	Enables the MKA feature.
key	Creates a key or enters the configuration mode of an existing key.
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.

Command	Description
macsec keychain policy	Configures a MACsec keychain policy.
macsec policy	Configures a MACsec policy.
show key chain	Displays the configuration of the specified keychain.
show macsec mka	Displays the details of MKA.
show macsec policy	Displays all the MACSec policies in the system.
show run mka	Displays the status of MKA.

copp copy profile

To create a copy of the Control Plane Policing (CoPP) best practice policy, use the copp clone profile command.

copp copy profile {**lenient**| **moderate**| **strict**} {**prefix**| **suffix**} **string**

Syntax Description

lenient	Specifies the lenient profile.
moderate	Specifies the moderate profile.
strict	Specifies the strict profile.
prefix	Specifies a prefix for the cloned policy.
suffix	Specifies a suffix for the cloned policy.
string	Prefix or suffix string. The suffix or prefix can be any alphanumeric string up to 20 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

When you use the copp copy profile command, CoPP renames all class maps and policy maps with the specified prefix or suffix.

This command does not require a license.

Examples

This example shows how to create a clone of the CoPP best practice policy:

```
switch # copp copy profile moderate abc
```

Related Commands

Command	Description
copp profile	Applies the default CoPP best practice policy on the Cisco NX-OS device.
show copp status	Displays the CoPP status, including the last configuration operation and its status.
show running-config copp	Displays the CoPP configuration in the running configuration.

copp profile

To apply the default Control Plane Policing (CoPP) best practice policy on the Cisco NX-OS device without rerunning the setup utility, use the copp profile command. To remove the default CoPP policy from the Cisco NX-OS device, use the no form of this command.

copp profile {**dense**| **lenient**| **moderate**| **strict**}

no copp profile {**dense**| **lenient**| **moderate**| **strict**}

Syntax Description

dense	Specifies the dense profile.
lenient	Specifies the lenient profile.
moderate	Specifies the moderate profile.
strict	Specifies the strict profile.

Command Default

strict

Command Modes

Global configuration (config)

Command History

Release	Modification
5.2(1)	This command was introduced.
6.0(1)	Added the dense keyword.

Usage Guidelines

In Cisco NX-OS releases prior to 5.2(1), you must use the setup utility to change or reapply the default CoPP policy. You can access the setup utility using the setup command.

Beginning with Cisco NX-OS Release 5.2, the CoPP best practice policy is read-only. If you want to modify its configuration, you must clone it using the copp clone profile command. Cloned policies are treated as user configurations.

When you use in-service software downgrade (ISSU) to upgrade to Cisco NX-OS Release 5.2, the policy attached to the control plane is treated as a user-configured policy. Check the CoPP profile using the show copp profile command and make any required changes.

If you use ISSU to downgrade from Cisco NX-OS Release 5.2, CoPP reports the incompatible configuration and instructs you to clone the CoPP profile. In the lower version, all configurations are restored in user-configuration mode.

This command does not require a license.

Examples

This example shows how to apply the default CoPP best practice policy on the Cisco NX-OS device:

```
switch# configure terminal
switch(config)# copp profile moderate
switch(config)#
```

This example shows how remove the default CoPP best practice policy from the Cisco NX-OS device:

```
switch(config)# no copp profile moderate
switch(config)#
```

Related Commands

Command	Description
copp copy profile	Creates a copy of the CoPP best practice policy.
show copp profile	Displays the details of the CoPP best practice policy.
show copp status	Displays the CoPP status, including the last configuration operation and its status.
show running-config copp	Displays the CoPP configuration in the running configuration.

CRLLookup

To configure the attribute name, search filter, and base-DN for the certificate revocation list (CRL) search operation in order to send a search query to the Lightweight Directory Access Protocol (LDAP) server, use the **CRLLookup** command. To disable this configuration, use the **no** form of this command.

CRLLookup attribute-name attribute-name search-filter filter base-DN *base-DN-name*

no CRLLookup

Syntax Description

attribute-name *attribute-name*	Specifies the attribute name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
search-filter *filter*	Specifies the filter for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
base-DN *base-DN-name*	Specifies the base-designated name for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Command Default

None

Command Modes

Lightweight Directory Access Protocol (LDAP) search map configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the attribute name, search filter, and base-DN for the CRL search operation in order to send a search query to the LDAP server:

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# CRLLookup attribute-name certificateRevocationList
search-filter (&(objectClass=cRLDistributionPoint)) base-DN CN=CDP,CN=Public Key
Services,CN=Services,CN=Configuration,DC=mdsldaptestlab,DC=com
switch(config-ldap-search-map)#
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap search-map	Configures an LDAP search map.
show ldap-search-map	Displays the configured LDAP search maps.

crypto ca authenticate

To associate and authenticate a certificate of the certificate authority (CA) and configure its CA certificate (or certificate chain), use the **crypto ca authenticate** command. To remove the association and authentication, use the **no** form of this command.

crypto ca authenticate *trustpoint-label*

no crypto ca authenticate *trustpoint-label*

Syntax Description

trustpoint-label	Name of the trustpoint. The name The name is alphanumeric, case sensitive, and has a maximum length of 64 characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

You can use this command to authenticate the CA to the Cisco NX-OS device by obtaining the self-signed certificate of the CA that contains the public key of the CA. Because the CA signs its own certificate, you should manually authenticate the public key of the CA by contacting the CA administrator when you execute this command. The CA certificate or certificate chain must be available in Privacy Enhanced Mail (PEM) (base-64) encoded format.

Use this command when you initially configure certificate authority support for the device. First create the trustpoint using the **crypto ca trustpoint** command using the CA certificate fingerprint published by the CA. You must compare the certificate fingerprint displayed during authentication with the one published by the CA and accept the CA certificate only if it matches.

If the CA to authenticate is a subordinate CA (it is not self-signed), then another CA certifies it, which in turn may be certified by yet another CA, and so on, until there is a self-signed CA. In this case, the subordinate CA has a CA certificate chain. You must enter the entire chain during CA authentication. The maximum length that the CA certificate chain supports is ten.

The trustpoint CA is the certificate authority that you configure on the device as the trusted CA. The device accepts any peer certificate if it is signed by a locally trusted CA or its subordinates.

The trustpoint configuration that you create with the **crypto ca trustpoint** command persists across device reboots only if you save it explicitly using the **copy running-config startup-config** command. The certificates and CRL associated to a trustpoint are automatically persistent when you save the trustpoint configuration in the startup configuration. Otherwise, if you do not saved the trustpoint in the startup configuration, the associated certificates and CRL are not automatically persistent because they cannot exist without the corresponding trustpoint after the device reboots.

To ensure that the configured certificates, CRLs, and key pairs are persistent, always save the running configuration in the startup configuration.

This command does not require a license.

Examples

This example shows how to authenticate a CA certificate called admin-ca:

```
switch# configure terminal
switch(config)# crypto ca authenticate myCA
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO
MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
 END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
Do you accept this certificate? [yes/no]: y
```

Related Commands

Command	Description
crypto ca trustpoint	Configures the trustpoint.
show crypto ca certificates	Displays configured trustpoint certificates.
show crypto ca trustpoints	Displays trustpoint configurations.

crypto ca crl request

To configure a new certificate revocation list (CRL) downloaded from the certificate authority (CA), use the **crypto ca crl request** command.

crypto ca crl request *trustpoint-label source-file*

Syntax Description

trustpoint-label	Name of the trustpoint. The maximum size is 64 characters.
source-file	Location of the CRL in the form **bootflash**:*filename* . The maximum size is 512.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

The crypto ca crl request command allows you to pre-download CRLs for the trustpoints and cache the CRLs in the certificate (cert) store. The CRL file specified should contain the latest CRL in either the Privacy Enhanced Mail (PEM) format or Distinguished Encoding Rules (DER) format.

The trustpoint configuration that you create with the **crypto ca trustpoint** command persists across device reboots only if you save it explicitly using the **copy running-config startup-config** command. The certificates and CRL associated to a trustpoint are automatically persistent when you save the trustpoint configuration in the startup configuration. Otherwise, if you do not save the trustpoint in the startup configuration, the associated certificates and CRL are not automatically persistent because they cannot exist without the corresponding trustpoint after the device reboots.

To ensure that the configured certificates, CRLs and key pairs are persistent, always save the running configuration in the startup configuration.

This command does not require a license.

Examples

This example shows how to configure a CRL for the trustpoint or replaces the current CRL:

```
switch# configure teminal
switch(config)# crypto ca crl request admin-ca bootflash:admin-ca.crl
```

Related Commands

Command	Description
revocation-check	Configures trustpoint revocation check methods.
show crypto ca crl	Displays configured certificate revocation lists (CRL).

clear ldap-server statistics

To clear the Lightweight Directory Access Protocol (LDAP) server statistics, use the **clear ldap-server statistics** command.

clear ldap-server statistics {**ipv4-address| ipv6-address| host-name**}

Syntax Description

ipv4-address	Server IPv4 address in the *A.B.C.D* format.
ipv6-address	Server IPv6 address in the *X:X:X:X* format.
host-name	Server name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear the statistics for an LDAP server:

```
switch# clear ldap-server statistics 10.10.1.1
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap-server host	Specifies the IPv4 or IPv6 address or hostname for an LDAP server.
show ldap-server **statistics**	Displays the LDAP server statistics.

clear mac access-list counters

To clear the counters for all MAC access control lists (ACLs) or a single MAC ACL, use the **clear mac access-list counters** command.

clear mac access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the MAC ACL whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear counters for all MAC ACLs:

```
switch# clear mac access-list counters
switch#
```

This example shows how to clear counters for a MAC ACL named acl-mac-0060:

```
switch# clear mac access-list counters acl-ipv4-0060
switch#
```

Related Commands

Command	Description
clear access-list counters	Clears counters for IPv4, IPv6, and MAC ACLs.
clear ip access-list counters	Clears counters for IPv4 ACLs.
clear ipv6 access-list counters	Clears counters for IPv6 ACLs.
clear vlan access-list counters	Clears counters for VACLs.

Command	Description
show access-lists	Displays information about one or all IPv4, IPv6, and MAC ACLs.
show mac access-lists	Displays information about one or all MAC ACLs.

clear port-security

To clear a single, dynamically learned, secure MAC address or to clear all dynamically learned, secure MAC addresses for a specific interface, use the **clear port-security** command.

clear port-security dynamic interface ethernet slot / port [**vlan vlan-id**]

clear port-security dynamic interface port-channel *channel-number* [**vlan** *vlan-id*]

clear port-security dynamic address *address* [**vlan** *vlan-id*]

Syntax Description

dynamic	Specifies that you want to clear dynamically learned, secure MAC addresses.
interface	Specifies the interface of the dynamically learned, secure MAC addresses that you want to clear.
ethernet *slot/port*	Specifies the Ethernet interface of the dynamically learned, secure MAC addresses that you want to clear.
vlan *vlan-id*	(Optional) Specifies the VLAN of the secure MAC addresses to be cleared. Valid VLAN IDs are from 1 to 4096.
port-channel *channel-number*	Specifies the port-channel interface of the dynamically learned, secure MAC addresses that you want to clear.
address *address*	Specifies a single MAC address to be cleared, where *address* is the MAC address, in dotted hexadecimal format.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	Support was added for port-security on port-channel interfaces.
4.0(1)	This command was introduced.

Usage Guidelines

You must enable port security by using the **feature port-security** command before you can use the **clear port-security** command.

This command does not require a license.

Examples

This example shows how to remove dynamically learned, secure MAC addresses from the Ethernet 2/1 interface:

```
switch# configure terminal
switch(config)# clear port-security dynamic interface ethernet 2/1
```

This example shows how to remove the dynamically learned, secure MAC address 0019.D2D0.00AE:

```
switch# configure terminal
switch(config)# clear port-security dynamic address 0019.D2D0.00AE
```

Related Commands

Command	Description
debug port-security	Provides debugging information for port security.
feature port-security	Enables port security globally.
show port-security	Shows information about port security.
switchport port-security	Enables port security on a Layer 2 interface.

clear radius-server statistics

To clear the statistics for a RADIUS server host, use the **clear radius-server statistics** command.

clear radius-server statistics {*ipv4-address*| *ipv6-address*| *server-name*}

Syntax Description

ipv4-address	IPv4 address of a RADIUS server host in *A.B.C.D* format.
ipv6-address	IPv6 address of a RADIUS server host in *A:B::C:D* format.
server-name	Name of a RADIUS server host. The name is case sensitive.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear statistics for a RADIUS server:

```
switch# clear radius-server statistics 10.10.1.1
```

Related Commands

Command	Description
show radius-server statistics	Displays RADIUS server host statistics.

clear ssh hosts

To clear the Secure Shell (SSH) host sessions and the known host file for a virtual device context (VDC), use the **clear ssh hosts** command.

clear ssh hosts

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear all SSH host sessions and the known host file:

```
switch# clear ssh hosts
```

Related Commands

Command	Description
ssh server enable	Enables the SSH server.

clear tacacs-server statistics

To clear the statistics for a TACACS+ server host, use the **clear tacacs-server statistics** command.

clear tacacs-server statistics {*ipv4-address*| *ipv6-address*| *server-name*}

Syntax Description

ipv4-address	IPv4 address of a TACACS+ server host in *A.B.C.D* format.
ipv6-address	IPv6 address of a TACACS+ server host in *A:B::C:D* format.
server-name	Name of a TACACS+ server host. The name is case sensitive.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear statistics for a TACACS+ server:

```
switch# clear tacacs-server statistics 10.10.1.1
```

Related Commands

Command	Description
show tacacs-server statistics	Displays TACACS+ server host statistics.

clear user

To clear a user session for a virtual device context (VDC), use the **clear user** command.

clear user *user-id*

Syntax Description

user-id	User identifier.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **show users** command to display the current user sessions on the device.

This command does not require a license.

Examples

This example shows how to clear all SSH host sessions:

```
switch# clear user user1
```

Related Commands

Command	Description
show users	Displays the user session information.

cts l3 spi (global)

To enable Layer 3 Cisco TrustSec and map a security parameter index (SPI) and subnet for the device, use the **cts l3 spi** command. To remove the mapping to an IPv4 subnet, use the **no** form of this command.

ctsl3 **spi A.B.C.D** / *length*

no ctsl3 **spi A.B.C.D** / *length*

Syntax Description

spi-number	SPI for the device. The range is from 0 to 429496729.
A.B.C.D/length	IPv4 subnet.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

You can use only IPv4 addressing with Cisco TrustSec.

This command requires the Advanced Services license.

Examples

This example shows how to configure Layer 3 Cisco TrustSec global mapping for an SPI and subnet:

```
switch# config t
switch(config)# cts l3 spi 3 10.10.1.1/23
```

This example shows how to remove Layer 3 global mapping for a subnet:

```
switch# config t
switch(config)# no cts l3 spi 10.10.1.1/23
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

Command	Description
show cts l3 mapping	Displays the Layer 3 Cisco TrustSec mapping for SPI values to IPv4 subnets.

cts l3 spi (interface)

To enable Layer 3 Cisco TrustSec and configure a security parameter index (SPI) on an interface, use the **cts l3 spi** command. To revert to the default, use the **no** form of this command.

cts l3 spi *spi-number*

no cts l3

Syntax Description

spi-number	SPI for the interface. The range is from 0 to 429496729.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to enable Layer 3 Cisco TrustSec for an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts l3 spi 3 10.10.1.1/23
```

This example shows how to disable Layer 3 Cisco TrustSec for an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# no cts l3
```

Related Commands

Command	Description
cts l3 spi (global)	Enables the Layer 3 Cisco TrustSec for the device.
feature cts	Enables the Cisco TrustSec feature.

Command	Description
show cts l3 interface	Displays the Layer 3 Cisco TrustSec configuration on the interfaces.

crypto ca enroll

To request a certificate for the device RSA key pair created for this trustpoint CA, use the **crypto ca enroll** command.

crypto ca enroll *trustpoint-label*

Syntax Description

trustpoint-label	Name of the trustpoint. The maximum size is 64 characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

A Cisco NX-OS device enrolls with the trustpoint CA to obtain an identity certificate. You can enroll your device with multiple trustpoints and obtain a separate identity certificate from each trustpoint.

When enrolling with a trustpoint, you must specify an RSA key pair to certify. You must generate the key pair and associate it to the trustpoint before generating the enrollment request.

Use the crypto ca enroll command to generate a request to obtain an identity certificate from each of your trustpoints that correspond to authenticated CAs. The certificate signing request (CSR) generated is per the Public-Key Cryptography Standards (PKCS) #10 standard and is displayed in the PEM format. You then cut and paste the certificate and submit it to the corresponding CA through an e-mail or on the CA website. The CA administrator issues the certificate and makes it available to you either through the website or by sending it in an e-mail. You need to import the obtained identity certificate that corresponds to the trustpoint using the **crypto ca import** *trustpoint-label* **certificate** command.

Note The device does not save the challenge password with the configuration. Record this password so that you can provide it if you need to revoke your certificate.

This command does not require a license.

Examples

This example shows how to generate a certificate request for an authenticated CA:

```
switch# configure terminal
switch(config)# crypto ca enroll myCA
```

```
 Create the certificate request ..
 Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
  Password:nbv123
 The subject name in the certificate will be: Vegas-1.cisco.com
 Include the switch serial number in the subject name? [yes/no]:no
 Include an IP address in the subject name [yes/no]:yes
ip address:209.165.200.226
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
```

Related Commands

Command	Description
crypto ca import trustpoint-label certificate	Imports the identity certificate obtained from the CA to the trustpoint.
crypto key generate rsa	Generates an RSA key pair.
rsakeypair	Configures and associates the RSA key pair details to a trustpoint.
show crypto key mypubkey rsa	Displays all RSA public key configurations.

crypto ca export

To export the RSA key pair and the associated certificates (identity and CA) of a trustpoint within a Public-Key Cryptography Standards (PKCS) #12 format file to a specified location, use the **crypto ca export** command.

crypto ca export *trustpoint-label* **pkcs12** *destination-file-url pkcs12-password*

Syntax Description

trustpoint-label	Name of the trustpoint. The maximum size is 64 characters.
pkcs12 *destination-file-url*	Specifies a destination file in **bootflash**:*filename* format. The filename is alphanumeric, case sensitive, and has maximum of 512 characters.
*pkcs 12***-***password*	Password to be used to protect the RSA private key in the exported file. The passwords is alphanumeric, case sensitive, and has maximum of 64 characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

You can export the identity certificate with the associated RSA key pair and CA certificate (or certificate chain) to a PKCS #12 format file for backup purposes. You can later import the certificate and RSA key pair to recover from a system crash on your device.

This command does not require a license.

Examples

This example shows how to export a certificate and key pair in the PKCS #12 format:

```
switch# configure terminal
switch(config)# crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123
```

Related Commands

Command	Description
crypto ca import trustpoint-label certificate	Imports the identity certificate obtained from the CA to the trustpoint.
crypto ca import trustpoint-label pkcs12	Imports the identity certificate and associated RSA key pair and CA certificate (chain) to a trustpoint.
crypto key generate rsa	Generates an RSA key pair.
rsakeypair	Configures and associates the RSA key pair details to a trustpoint.
show crypto key mypubkey rsa	Displays any RSA public key configurations.

crypto ca import

To import the identity certificate in the Privacy Enhanced Mail (PEM) format or the identity certificate and associated RSA key pair and CA certificate (or certificate chain) in the Public-Key Cryptography Standards (PKCS) #12 format, use the **crypto ca import** command.

crypto ca import *trustpoint-label* {**certificate**| **pkcs12** *source-file-url pkcs12- password* }

Syntax Description

trustpoint-label	Name of the trustpoint. The maximum size is 64 characters.
certificate	Specifies that you will paste the trustpoint certificate at the command-line interface (CLI) prompt.
pkcs12 *source-file-url pkcs12-*	Specifies a source file containing the trustpoint certificate in **bootflash**:*filename* format. The filename is case sensitive.
password	Password that was used to protect the RSA private key in the imported PKCS#12 file. The password is case sensitive.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **certificate** keyword to import (by cut and paste means) the identity certificate obtained from the CA, corresponding to the enrollment request generated earlier in the trustpoint and submitted to the CA.

Use the **pkcs12** *source-file-url pkcs12-password* keyword and argumen t to import the complete identity information, which includes the identity certificate and associated RSA key pair and CA certificate or certificate chain, into an empty trustpoint. This method allows you to restore the configuration after a system crash.

The trustpoint configuration that you create with the **crypto ca trustpoint** command persists across device reboots only if you save it explicitly using the **copy running-config startup-config** command. The certificates and CRL associated to a trustpoint are automatically persistent when you save the trustpoint configuration in the startup configuration. Otherwise, if you do not saved the trustpoint in the startup configuration, the associated certificates and CRL are not automatically persistent because they cannot exist without the corresponding trustpoint after the device reboots.

To ensure that the configured certificates, CRLs and key pairs are persistent, always save the running configuration in the startup configuration.

This command does not require a license.

Examples

This example shows how to install an identity certificate obtained from a CA corresponding to an enrollment request made and submitted earlier:

```
switch# configure terminal
switch(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz
Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu
Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRFbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
```

This example shows how to import a certificate and key pair in a Public-Key Cryptography Standards (PKCS) #12 format file:

```
switch# configure terminal
witch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123
```

Related Commands

Command	Description
crypto ca export trustpoint-label pkcs12	Exports the RSA key pair and associated certificates of a trustpoint.
crypto ca enroll	Generates a certificate signing request for a trustpoint.
crypto key generate rsa	Generates the RSA key pair.
rsakeypair	Configures trustpoint RSA key pair details.
show crypto ca certificates	Displays the identity and CA certificate details.
show crypto key mypubkey rsa	Displays any RSA public key configurations.

crypto ca lookup

To specify the cert-store to be used for certificate authentication, use the **crypto ca lookup** command.

crypto ca lookup {**local**| **remote**| **both**}

Syntax Description

local	Specifies the local cert-store for certificate authentication.
remote	Specifies the remote cert-store for certificate authentication.
both	Specifies the local cert-store for certificate authentication, but if the authentication fails or the CA certificate is not found, the remote cert-store is used.

Command Default

Local

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

If you plan to configure a remote cert-store, you must set up an LDAP server in a remote device and make sure that the CA certificates that are used for authentication are loaded to the Active Directory.

This command does not require a license.

Examples

This example shows how to specify the remote cert-store for certificate authentication:

```
switch(config)# crypto ca lookup remote
```

Related Commands

Command	Description
crypto ca remote ldap crl-refresh-time	Configures the refresh time to update the certificate revocation list from the remote cert-store.

Command	Description
crypto ca remote ldap server-group	Configures the LDAP server group to be used while communicating with LDAP.
show crypto ca certstore	Displays the configured cert-store.
show crypto ca remote-certstore	Displays the remote cert-store configuration.

crypto ca remote ldap crl-refresh-time

To configure the refresh time to update the certificate revocation list (CRL) from the remote cert-store, use the **crypto ca remote ldap crl-refresh-time** command.

crypto ca remote ldap crl-refresh-time hours

Syntax Description

hours	Refresh time value in hours. The range is from 0 to 744 hours. If you enter 0, the refresh routine runs once.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must configure a remote cert-store and the LDAP server group.

This command does not require a license.

Examples

This example shows how to configure the refresh time to update the CRL from the remote cert-store:

```
switch(config)# crypto ca remote ldap crl-refresh-time 10
```

Related Commands

Command	Description
crypto ca lookup	Specifies the cert-store to be used for certificate authentication.
crypto ca remote ldap server-group	Configures the LDAP server group to be used while communicating with LDAP.

crypto ca remote ldap server-group

To configure the Lightweight Directory Access Protocol (LDAP) server group to be used while communicating with LDAP, use the **crypto ca remote ldap server-group** command.

crypto ca remote ldap server-group group-name

Syntax Description

group-name	Server group name. You can enter up to 64 alphanumeric characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must configure a remote cert-store.

This command does not require a license.

Examples

This example shows how to configure the LDAP server group to be used while communicating with LDAP:

```
switch(config)# crypto ca remote ldap server-group group1
```

Related Commands

Command	Description
crypto ca lookup	Specifies the cert-store to be used for certificate authentication.
crypto ca remote ldap crl-refresh-time	Configures the refresh time to update the certificate revocation list from the remote cert-store.

crypto ca test verify

To verify a certificate file, use the **crypto ca test verify** command.

crypto ca test verify *certificate-file*

Syntax Description

certificate-file	Certificate filename in the form **bootflash**:*filename* . The filename is case sensitive.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use this command to verify the specified certificate in the PEM format by using the trusted CAs configured and by consulting the certificate revocation list (CRL), if needed, as indicated by the revocation checking configuration.

This command does not require a license.

Examples

This example shows how to verify a certificate file:

```
switch(config)# crypto ca test verify bootflash:id1.pem
verify status oode:0
verify error msg:
```

Note The verify status code value of 0 indicates that the verification is successful.

Related Commands

Command	Description
show crypto ca certificates	Displays configured trustpoint certificates.

crypto ca trustpoint

To create a trustpoint certificate authority (CA) that the device should trust and enter trustpoint configuration mode, use the **crypto ca trustpoint** command. To remove the trustpoint, use the **no** form of this command.

crypto ca trustpoint *trustpoint-label*

no crypto ca trustpoint *trustpoint-label*

Syntax Description

trustpoint-label	Name of the trustpoint. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Trustpoints have the following characteristics:

- A trustpoint corresponds to a single CA, which a Cisco NX-OS device trusts for peer certificate verification for any application.
- A CA must be explicitly associated to a trustpoint using the **crypto ca authenticate** command.
- A Cisco NX-OS device can have many trustpoints and all applications on the device can trust a peer certificate issued by any of the trustpoint CAs.
- A trustpoint is not restricted to a specific application.
- The Cisco NX-OS device can optionally enroll with a trustpoint CA to get an indemnity certificate for itself.

You do not need to designate one or more trustpoints to an application. Any application should be able to use any certificate issued by any trustpoint as long as the certificate satisfies the application requirement.

You do not need more than one identity certificate from a trustpoint or more than one key pair associated to a trustpoint. A CA certifies a given identity (name) only once and does not issue multiple certificates with the same subject name. If you need more than one identity certificate for a CA, define another trustpoint for the same CA, associate another key pair to it, and have it certified if the CA allows multiple certificates with the same subject name.

Note Before using the **no crypto ca trustpoint** command to remove the trustpoint, you must first delete the identity certificate and CA certificate (or certificate chain) and then disassociate the RSA key pair from the trustpoint. The device enforces this sequence of actions to prevent the accidental removal of the trustpoint with the certificates.

This command does not require a license.

Examples

This example shows how to declare a trustpoint CA that the device should trust and enter trustpoint configuration mode:

```
switch#
configure terminal

switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)#
```

This example shows how to remove the trustpoint CA:

```
switch#
configure terminal

switch(config)# no crypto ca trustpoint admin-ca
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the certificate of the certificate authority.
crypto ca enroll	Generates a certificate signing request for a trustpoint.
show crypto ca certificates	Displays the identity and CA certificate details.
show crypto ca trustpoints	Displays trustpoint configurations.

crypto cert ssh-authorize

To configure a certificate mapping filter for the SSH protocol, use the **crypto cert ssh-authorize** command.

crypto cert ssh-authorize [**default**| **issuer-CAname**] [**map map-name1 [map-name2]**]

Syntax Description

default	Specifies the default filter map for SSH authorization.
issuer-CAname	Issuer of the CA certificate. You can enter up to 64 alphanumeric characters. You can enter up to 64 alphanumeric characters.
map	Specifies the mapping filter to be applied.
map-name1, map-name2	Name of the default mapping filter, which is already configured. You can enter up to 64 alphanumeric characters. If you do not use the default map, you can specify one or two filter maps for authorization.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must create a filter map.

This command does not require a license.

Examples

This example shows how to configure a certificate mapping filter for the SSH protocol:

```
switch(config)# crypto cert ssh-authorize default map
 filtermap1
```

Related Commands

Command	Description
crypto certificatemap mapname	Creates a filter map.
filter	Configures one or more certificate mapping filters within the filter map.
show crypto ssh-auth-map	Displays the mapping filters configured for SSH authentication.

crypto certificatemap mapname

To create a filter map, use the **crypto certificatemap mapname** command.

crypto certificatemap mapname *map-name*

Syntax Description

map-name	Name of the filter map. You can enter up to 64 alphanumeric characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must configure a cert-store for certificate authentication.

This command does not require a license.

Examples

This example shows how to create a new filter map:

```
switch(config)# crypto certificatemap mapname
 filtermap1
```

Related Commands

Command	Description
filter	Configures one or more certificate mapping filters within the filter map.
show crypto certificatemap	Displays the certificate mapping filters.

cts cache enable

To enable Cisco TrustSec authentication and authorization information caching, use the **cts cache enable** command. To revert to the default, use the **no** form of this command.

cts cache enable

no cts cache enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to enable Cisco TrustSec authentication and authorization caching:

```
switch# config t
switch(config)# cts cache enable
```

This example shows how to disable Cisco TrustSec authentication and authorization caching:

```
switch# config t
switch(config)# no cts cache enable
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts	Displays Cisco TrustSec configuration information.

cts device-id

To configure a Cisco TrustSec device identifier, use the **cts device-id** command.

cts device-id *device-id* **password [7]** *password*

Syntax Description

device-id	Cisco TrustSec device identifier name. The name is alphanumeric and case-sensitive. The maximum length is 32 characters.
7	(Optional) Encrypts the password.
password *password*	Specifies the password to use during EAP-FAST processing. The name is alphanumeric and case-sensitive. The maximum length is 32 characters.

Command Default

No Cisco TrustSec device identifier

Clear text password

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

The Cisco TrustSec device identifier name must be unique in your Cisco TrustSec network cloud.

This command requires the Advanced Services license.

Examples

This example shows how to configure a Cisco TrustSec device identifier:

```
switch# configure terminal
swtich(config)# cts device-id DeviceA password Cisco321
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

Command	Description
show cts credentials	Displays the Cisco TrustSec credentials information.

cts role-based sgt-map

To manually configure the Cisco TrustSec security group tag (SGT) mapping to IP addresses, use the **cts role-based sgt-map** command. To remove an SGT, use the **no** form of this command.

cts role-based sgt-map *ipv4-address sgt-value*

no cts role-based sgt-map *ipv4-address*

Syntax Description

ipv4-address	IPv4 address. The format is *A.B.C.D*
sgt-value	SGT value. The range is 0 to 65533.

Command Default

None

Command Modes

Global configuration VLAN configuration VRF configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

You can use only IPv4 addressing with Cisco TrustSec.

This command requires the Advanced Services license.

Examples

This example shows how to configure mapping for a Cisco TrustSec SGT:

```
switch# configure terminal
switch(config)# cts role-based sgt-map 10.10.1.1 3
switch(config-rbacl)#
```

This example shows how to remove a Cisco TrustSec SGT mapping:

```
switch# configure terminal
switch(config)# no ccts role-based sgt-map 10.10.1.1
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based sgt-map	Displays the Cisco TrustSec SGT mapping.

cts sgt

To configure the security group tag (SGT) for Cisco TrustSec, use the **cts sgt** command.

cts sgt *tag*

Syntax Description

tag	Local SGT for the device that is a decimal value or a hexadecimal value with the format **0x***hhhh* . The decimal range is from 2 to 65519, and the hexadecimal range is from 0x0 to 0xffff.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
6.2(2)	Modified the tag argument to accept decimal values.
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to configure the Cisco TrustSec SGT for the device:

```
switch# configure terminal
switch(config)# cts sgt 0x3
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts environment-data	Displays the Cisco TrustSec environment data.

cts l3 spi (global)

To enable Layer 3 Cisco TrustSec and map a security parameter index (SPI) and subnet for the device, use the **cts l3 spi** command. To remove the mapping to an IPv4 subnet, use the **no** form of this command.

ctsl3 **spi A.B.C.D** / *length*

no ctsl3 **spi A.B.C.D** / *length*

Syntax Description

spi-number	SPI for the device. The range is from 0 to 429496729.
A.B.C.D/length	IPv4 subnet.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

You can use only IPv4 addressing with Cisco TrustSec.

This command requires the Advanced Services license.

Examples

This example shows how to configure Layer 3 Cisco TrustSec global mapping for an SPI and subnet:

```
switch# config t
switch(config)# cts l3 spi 3 10.10.1.1/23
```

This example shows how to remove Layer 3 global mapping for a subnet:

```
switch# config t
switch(config)# no cts l3 spi 10.10.1.1/23
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

Command	Description
show cts l3 mapping	Displays the Layer 3 Cisco TrustSec mapping for SPI values to IPv4 subnets.

cts l3 spi (interface)

To enable Layer 3 Cisco TrustSec and configure a security parameter index (SPI) on an interface, use the **cts l3 spi** command. To revert to the default, use the **no** form of this command.

cts l3 spi *spi-number*

no cts l3

Syntax Description

spi-number	SPI for the interface. The range is from 0 to 429496729.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to enable Layer 3 Cisco TrustSec for an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts l3 spi 3 10.10.1.1/23
```

This example shows how to disable Layer 3 Cisco TrustSec for an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# no cts l3
```

Related Commands

Command	Description
cts l3 spi (global)	Enables the Layer 3 Cisco TrustSec for the device.
feature cts	Enables the Cisco TrustSec feature.

Command	Description
show cts l3 interface	Displays the Layer 3 Cisco TrustSec configuration on the interfaces.

cts l3 spi (interface)

To enable Layer 3 Cisco TrustSec and configure a security parameter index (SPI) on an interface, use the **cts l3 spi** command. To revert to the default, use the **no** form of this command.

cts l3 spi *spi-number*

no cts l3

Syntax Description

spi-number	SPI for the interface. The range is from 0 to 429496729.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to enable Layer 3 Cisco TrustSec for an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts l3 spi 3 10.10.1.1/23
```

This example shows how to disable Layer 3 Cisco TrustSec for an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# no cts l3
```

Related Commands

Command	Description
cts l3 spi (global)	Enables the Layer 3 Cisco TrustSec for the device.
feature cts	Enables the Cisco TrustSec feature.

Command	Description
show cts l3 interface	Displays the Layer 3 Cisco TrustSec configuration on the interfaces.

cts manual

To enter Cisco TrustSec manual configuration for an interface, use the **cts manual** command. To remove the manual configuration, use the **no** form of this command.

cts manual

no cts manual

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

After using this command, you must enable and disable the interface using the **shutdown**/**no shutdown** command sequence for the configuration to take effect.

This command requires the Advanced Services license.

Examples

This example shows how to enter Cisco TrustSec manual configuration mode for an interface:

```
switch# configure terminal
switch(config)# interface etherent 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)#
```

This example shows how to remove the Cisco TrustSec manual configuration from an interface:

```
switch# configure terminal
switch(config)# interface etherent 2/4
switch(config-if)# no cts manual
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

Command	Description
show cts interface	Displays Cisco TrustSec configuration information for interfaces.

cts refresh environment-data

To refresh the Cisco TrustSec environment data downloaded from the AAA server, use the **cts refresh environment-data** command.

cts refresh environment-data

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

Ensure that you are using the Cisco Identity Services Engine (ISE) Release 1.0 or later releases.

Examples

This example shows how to refresh the Cisco TrustSec environment data downloaded from the AAA server:

```
switch# cts refresh environment-data
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts environment-data	Displays the Cisco TrustSec environment data.

cts refresh role-based-policy

To refresh the Cisco TrustSec security group access control list (SGACL) policies downloaded from the Cisco Secure ACS, use the **cts refresh role-based-policy** command.

cts refresh role-based-policy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to enter Cisco TrustSec manual configuration mode for an interface:

```
switch# cts refresh role-based-policy
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based policy	Displays Cisco TrustSec SGACL policy configuration.

cts rekey

To rekey an interface for Cisco TrustSec policies, use the **cts rekey** command.

cts rekey ethernet *slot/port*

Syntax Description

ethernet *slot*/*port*	Specifies an Ethernet interface.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to rekey an interface for Cisco TrustSec:

```
switch# cts rekey ethernet 2/3
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts interface	Displays Cisco TrustSec configuration information for interfaces.

cts role-based access-list

To create or specify a Cisco TrustSec security group access control list (SGACL) and enter role-based access control list configuration mode, use the **cts role-based access-list** command. To remove an SGACL, use the **no** form of this command.

cts role-based access-list *list-name*

no cts role-based access-list *list-name*

Syntax Description

list-name	Name for the SGACL. The name is alphanumeric and case-sensitive. The maximum length is 32 characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to create a Cisco TrustSec SGACL and enter role-based access list configuration mode :

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)#
```

This example shows how to remove a Cisco TrustSec SGACL:

```
switch# configure terminal
switch(config)# no cts role-based access-list MySGACL
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based access-list	Displays the Cisco TrustSec SGACL configuration.

cts role-based counters enable

To enable role-based access control list (RBACL) statistics, use the **cts role-based counters enable** command. To disabled RBACL statistics, use the **no** form of this command.

cts role-based counters enable

no cts role-based counters enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

To use this command, you must enable RBACL policy enforcement on the VLAN and VRF.

When you enable RBACL statistics, each policy requires one entry in the . If you do not have enough space remaining in the , an error message appears, and you cannot enable the statistics.

When you modify an RBACL policy, statistics for the previously assigned access control entry (ACE) are displayed, and the newly assigned ACE statistics are initialized to 0.

RBACL statistics are lost only when the Cisco NX-OS device reloads or you deliberately clear the statistics.

This command requires the Advanced Services license.

Examples

This example shows how to enable RBACL statistics:

```
switch# configure terminal
switch(config)# cts role-based counters enable
```

This example shows how to disable RBACL statistics:

```
switch# configure terminal
switch(config)# no cts role-based counters enable
```

Related Commands

Command	Description
clear cts role-based counters	Clears the RBACL statistics so that all counters are reset to 0.
show cts role-based counters	Displays the configuration status of RBACL statistics and lists statistics for all RBACL policies.

cts role-based detailed-logging

To enable the displaying of ACE-Action details for the RBACL policies, use the **cts role-based detailed-logging** command. To revert to the default, use the **no** form of this command.

cts role-based detailed-logging

no cts role-based detailed-logging

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configurationVRF configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

Note To view the detailed ACLLOGS, you need to enable logging ip access-list detailed after enabling **cts role-based detailed logging**.

Examples

This example shows how to configure RBACL ace level permission and monitor logging:

```
switch# configure terminal
switch(config)# cts role-based detailed-logging
```

This example shows how to disable RBACL ace level permission and monitor logging:

```
switch# configure terminal
switch(config)# no
cts role-based detailed-logging
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based enable	Displays the Cisco TrustSec SGACL policy enforcement configuration.

cts role-based enforcement

To enable Cisco TrustSec security group access control list (SGACL) enforcement in a VLAN or Virtual Routing and Forwarding instance (VRF), use the **cts role-based enforcement** command. To revert to the default, use the **no** form of this command.

To disable Cisco TrustSec SGACL enforcement in an L3 interface or L3 port-channel, use the **no cts role-based enforcement** command. To revert to the default, use the **cts role-based enforcement** command.

cts role-based enforcement

no cts role-based enforcement

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled for VLAN, and Virtual Routing and Forwarding instance (VRF).

Enabled for L3 interfaces and L3 port-channels.

Command Modes

Global configuration VLAN configuration VRF configuration Interface configuration

Command History

Release	Modification
8.0(1)	Added the support for disabling SGACL policy enforcement on L3 interfaces and L3 port-channels.
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to enable Cisco TrustSec SGACL enforcement in the default VRF:

```
switch# configure terminal
switch(config)# cts role-based enforcement
```

This example shows how to enable Cisco TrustSec SGACL enforcement in a VLAN:

```
switch# configure terminal
switch(config)# vlan 1
switch(config-vlan)# cts role-based enforcement
```

This example shows how to enable Cisco TrustSec SGACL enforcement in a nondefault VRF:

```
switch# configure terminal
switch(config)# vrf context MyVRF
switch(config-vrf)# cts role-based enforcement
```

This example shows how to disable Cisco TrustSec SGACL enforcement in an interface and L3 port-channel:

```
switch# configure terminal
switch(config)# interface ethernet 6/2
switch(config-if)# no cts role-based enforcement
switch(config-if)# exit


switch(config)# interface port-channel 100
switch(config-if)# no cts role-based enforcement
switch(config-if)# exit
```

This example shows how to disable Cisco TrustSec SGACL enforcement:

```
switch# configure terminal
switch(config)# no cts role-based enforcement
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based enable	Displays the Cisco TrustSec SGACL policy enforcement configuration.

cts role-based monitor

To configure RBACL monitor, use the **cts role-based monitor** command. To revert to the default, use the **no** form of this command.

cts role-based monitor {**all**| **enable**| **permissions from**| {**sgt**| **unknown** }| **to** | {**dgt**| **unknown**}}[*ipv4* | *ipv6*]

no cts role-based monitor {**all**| **enable**| **permissions from**| {**sgt**| **unknown** }| **to** | {**dgt**| **unknown**}}[*ipv4* | *ipv6*]

Syntax Description

all	Enables monitoring permissions for all source groups to all destination groups.
enable	Enables RBACL monitor mode.
permission	Specifies the range for the SGT and DGT that needs to be monitored.
sgt	Specifies any SGT.
dgt	Specifies the Specifies the destination SGT.
unknown	Specifies an unknown SGT.
ipv4	Specifies the IPv4 protocol version.
ipv6	Specifies the IPv6 protocol version.

Command Default

Disabled

Command Modes

Global configurationVRF configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

Examples

This example shows how to enable monitoring permissions for all source groups to all destination groups:

```
switch# configure terminal
switch(config)# cts role-based monitor all
```

This example shows how to disable monitoring permissions for all source groups to all destination groups:

```
switch# configure terminal
switch(config)# no cts role-based monitor all
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based enable	Displays the Cisco TrustSec SGACL policy enforcement configuration.

cts role-based policy priority-static

To set a higher install priority for the SGACLs configured by using CLI, use the **cts role-based policy priority-static** command. Use the **no** form of this command to revert, that is, set the install priority for the SGACLs downloaded by ISE.

cts role-based policy priority-static

no cts role-based policy priority-static

Command Default

Install priority is set for the SGACLs configured by using CLI.

Command Modes

Global configuration

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

Examples

This example shows how to set higher install priority for ISE configured SGACLs:

```
switch# configure terminal
switch(config)# no cts role-based policy priority-static
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
cts refresh role-based-policy	Refreshes the Cisco TrustSec security group access control list (SGACL) policies.
show cts role-based policy	Displays the Cisco TrustSec SGACL policies and their details.

cts role-based sgt

To manually configure mapping of Cisco TrustSec security group tags (SGTs) to a security group access control list (SGACL), use the **cts role-based sgt** command. To remove the SGT mapping to an SGACL, use the **no** form of this command.

cts role-based sgt {**sgt-value**| **any**| **unknown**} **dgt** {**dgt-value**| **unknown**} **access-list list-name**

no cts role-based sgt {*sgt-value*| **any**| **unknown**} **dgt** {*dgt-value*| **unknown**}

Syntax Description

sgt-value	Source SGT value. The range is 0 to 65533.
any	Specifies any SGT.
unknown	Specifies an unknown SGT.
dgt	Specifies the destination SGT.
dgt-value	Destination SGT value. The range is 0 to 65533.
access-list *list-name*	Specifies the name for the SGACL.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

You must configure the SGACL before you can configure SGT mapping.

This command requires the Advanced Services license.

Examples

This example shows how to configure SGT mapping for an SGACL:

```
switch# configure terminal
switch(config)# cts role-based sgt 3 dgt 10 access-list MySGACL
```

This example shows how to remove SGT mapping for an SGACL

```
switch# configure terminal
switch(config)# no cts role-based sgt 3 sgt 10
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based policy	Displays the Cisco TrustSec SGT mapping for an SGACL.

cts sxp allow default-route-sgt

To enable the default route for SGT bindings, use the **cts sxp allow default-route-sgt** command. To disable, use the **no** form of this command.

cts sxp allow default-route-sgt

no cts sxp allow default-route-sgt

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec SXP feature using the **cts sxp enable** command.

Examples

This example shows how to expand the network limit:

```
switch# configure terminal
switch(config)# cts sxp allow default-route-sgt
```

This example shows how to disable the network limit:

```
switch# configure terminal
switch(config)# no cts sxp allow default-route-sgt
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts sxp	Displays the Cisco TrustSec SXP configuration information.

cts sxp connection peer

To configure a Security Group Tag (SGT) Exchange Protocol (SXP) peer connection for Cisco TrustSec, use the **cts sxp connection peer** command. To remove the SXP connection, use the **no** form of this command.

cts sxp connection peer *ipv4-address* **[source***source-ip-address* **password** {**default**| **none**| **required**} **mode** {**local**| **peer**} [[[**listener**| **speaker**] [**hold-time** *minimum-time maximum-time*]]| **both** [**vrf** *vrf-name*]]

no cts sxp connection peer *ipv4-address* {**source**| **password**} {**default**| **none**} **mode** {**local**| **peer**} [[[**listener**| **speaker**] [**hold-time** *minimum-time maximum-time*| **vrf** *vrf-name*]]| **both** [**vrf** *vrf-name*]]

Syntax Description

peer-ipv4-addr	IPv4 address of the peer device.
source *src-ipv4-addr*	(Optional) Specifies the IPv4 address of the source device.
password	Specifies the password option to use for the SXP authentication.
default	Specifies that SXP should use the default SXP password for the peer connection.
none	Specifies that SXP should not use a password.
required	Specifies the password that SXP should use for this peer connection.
password	Clear text password. The password is alphanumeric and case-sensitive. The maximum length is 32 characters.
7 *encrypted password*	Specifies an encrypted password. The maximum length is 32 characters.
mode	Specifies the mode of the peer device.
speaker	Specifies that the peer is the speaker.
listener	Specifies that the peer is the listener.
vrf *vrf-name*	(Optional) Specifies the VRF for the peer.

hold-time *minimum-time maximum-time*	(Optional) Specifies the hold-time period, in seconds, for the device. The range for minimum and maximum time is from 0 to 65535. A *maximum-time* value is required only when you use the following keywords: **peer speaker** and **local listener**. In other instances, only a *minimum-time* value is required. **Note** If both minimum and maximum times are required, the *maximum-time* value must be greater than or equal to the *minimum-time* value.

Command Default

The CTS-SXP peer IP address is not configured and no CTS-SXP peer password is used for the peer connection.

The default setting for a CTS-SXP connection password is **none**.

Command Modes

Global configuration

Command History

Release	Modification
8.0(1)	This command was modified. The **hold-time** keyword and *minimum-time* and *maximum-time* arguments were added.
4.1(3)	Added the **7** option to allow encrypted passwords.
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

You can use only IPv4 addressing with Cisco TrustSec.

If you do not specify a source IPv4 address, you must configure a default SXP source IPv4 address using the **cts sxp default source-ip** command.

If you specify default as the password mode, you must configure a default SXP password using the **cts sxp default password** command.

This command requires the Advanced Services license.

Examples

This example shows how to configure an SXP peer connection:

```
switch# configure terminal
switch(config)# cts sxp connection peer 10.10.1.1 source 10.10.2.2 password default mode
listener
```

This example shows how to remove an SXP peer connection:

```
switch# configure terminal
switch(config)# no cts sxp connection peer 10.10.1.1
```

This example shows how to configure the hold-time for the SXPv4 protocol for each connection.

```
switch# configure terminal
switch(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
hold-time 500
```

Related Commands

Command	Description
cts sxp default password	Configures the default SXP password for the device.
cts sxp default source-ip	Configures the default SXP source IPv4 address for the device.
feature cts	Enables the Cisco TrustSec feature.
show cts sxp connection	Displays the Cisco TrustSec SXP peer connection information.

cts sxp default password

To configure the default Security Group Tag (SGT) Exchange Protocol (SXP) password for the device, use the **cts sxp default password** command. To remove the default, use the **no** form of this command.

cts sxp default password {*password*| **7** *encrypted-password*}

no cts sxp default password

Syntax Description

password	Clear text password. The password is alphanumeric and case-sensitive. The maximum length is 32 characters.
7 *encrypted password*	Specifies an encrypted password. The maximum length is 32 characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(3)	Added the **7** option to allow encrypted passwords.
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to configure the default SXP password for the device:

```
switch# configure terminal
switch(config)# cts sxp default password Cisco654
```

This example shows how to remove the default SXP password:

```
switch# configure terminal
switch(config)# no cts sxp default password
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts sxp	Displays the Cisco TrustSec SXP configuration information.

cts sxp default source-ip

To configure the default Security Group Tag (SGT) Exchange Protocol (SXP) source IPv4 address for the device, use the **cts sxp default source-ip** command. To revert to the default, use the **no** form of this command.

cts sxp default source-ip *ipv4-address*

no cts sxp default source-ip *ipv4-address*

Syntax Description

ipv4-address	Default SXP IPv4 address for the device.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

You can use only IPv4 addressing with Cisco TrustSec.

This command requires the Advanced Services license.

Examples

This example shows how to configure the default SXP source IP address for the device:

```
switch# configure terminal
switch(config)# cts sxp default source-ip 10.10.3.3
```

This example shows how to remove the default SXP source IP address:

```
switch# configure terminal
switch(config)# no cts sxp default source-ip
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts sxp	Displays the Cisco TrustSec SXP configuration information.

cts sxp enable

To enable the Security Group Tag (SGT) Exchange Protocol (SXP) peer on a device, use the **cts sxp enable** command. To revert to the default, use the **no** form of this command.

cts sxp enable

no cts sxp enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to enable SXP:

```
switch# configure terminal
switch(config)# cts sxp enable
```

This example shows how to disable SXP:

```
switch# configure terminal
switch(config)# no cts sxp enable
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts sxp	Displays the Cisco TrustSec SXP configuration information.

cts sxp listener hold-time

To configure the global hold-time period of a listener network device in a Cisco TrustSec Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4) network, use the **cts sxp listener hold-time** command in global configuration mode. To remove the hold time from the listener device, use the **no** form of this command.

cts sxp listener hold-time *minimum-period maximum-period*

no cts sxp listener hold-time

Syntax Description

minimum-period	Minimum allowed hold time in seconds. The range is from 1 to 65534.
maximum-period	Specifies the maximum allowed hold-time in seconds. The range is from 1 to 65534 seconds. **Note** The *maximum-period* specified must be greater than or equal to the *minimum-period*.

Command Default

The default hold time range for a listener device is 90 seconds to 180 seconds.

Command Modes

Global configuration

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

SXP uses a TCP-based, keepalive mechanism to determine if a connection is live. SXPv4 adds an optional negotiated keepalive mechanism, the hold-time period, in order to provide more predictable and timely detection of connection loss.

Hold time can be configured globally on a network device. This global configuration will apply the configuration to all SXP connections configured on the device.

You may configure a hold-time period locally on a listener device or a default of 90 seconds to 180 seconds is used. A value of “0xFFFF..0xFFFF” indicates that the keepalive mechanism is not used.

The hold-time negotiation between the speaker device and the listener device succeeds when the speaker’s minimum acceptable hold-time falls below or within the desirable hold-time range of the listener. (Use the **cts sxp speaker hold-time** command to configure the hold-time of the speaker device.) If one end turns off the keepalive mechanism, the other end should also turn it off to make the negotiation successful.

The negotiation fails when the speaker's minimum acceptable hold-time is greater than the upper bound of the listener's hold-time range.

The selected hold-time period of a successful negotiation is the maximum of the speaker’s minimum acceptable hold-time and the lower bound of the listener’s hold-time range.

The speaker calculates the keepalive time to one-third of the selected hold time by default, unless a different keepalive time is locally configured.

Examples

The following example shows how to configure the hold time period of a listener device for a minimum of 300 seconds and a maximum of 500 seconds:

```
switch# configure terminal
switch(config)# cts sxp listener hold-time 300 500
```

Related Commands

Command	Description
cts sxp enable	Enables Cisco TrustSec SXP on a device.
cts sxp speaker hold-time	Configures the hold time of a speaker device in an SXPv4 network.
show cts sxp	Displays the status of all Cisco TrustSec SXP configurations.

cts sxp mapping network-map

To expand the network limit, use the **cts sxp mapping network-map** command. To revert to the default, use the **no** form of this command.

cts sxp mapping network-map *num_bindings*

no cts sxp mapping network-map *num_bindings*

Syntax Description

num_bindings	Number of bindings to be expanded. The range is from 0 to 65535.

Command Default

Zero (0)

Command Modes

Global configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature by using the **feature cts** command.

Examples

This example shows how to expand the network limit:

```
switch# configure terminal
switch(config)# cts sxp mapping network-map 64
```

This example shows how to disable the network limit:

```
switch# configure terminal
switch(config)# no cts sxp mapping network-map 64
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts sxp	Displays the Cisco TrustSec SXP configuration information.

cts sxp node-id

To configure the node ID of a network device for Cisco TrustSec (CTS) Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4), use the **cts sxp node-id** command in global configuration mode. To remove the node ID, use the **no** form of this command.

cts sxp node-id {*node-id* | **interface** *interface-type* | *ipv4-address*}

no cts sxp node-id

Syntax Description

node-id	Specifies the node ID of the device. Enter the node ID in hexadecimal format.
interface *interface-type*	Specifies the type of interface.
ipv4-address	Specifies the SXP peer IPv4 address.

Command Default

A node ID is not configured.

Command Modes

Global configuration

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The **cts sxp node-id** command configures the node ID of a network device.

An SXP node ID is used to identify the individual devices within the network. The node ID is a four-octet integer that can be configured by the user. If it is not configured by the user, SXP picks a node ID itself using the highest IPv4 address in the default VRF domain, in the same manner that EIGRP generates its node ID.

The node ID has to be unique in the network that SXP connections traverse to enable SXP loop prevention.

The SXP loop detection mechanism drops the binding propagation packets based on finding its own node ID in the peer sequence attribute. Changing a node ID in a loop detection running SXP network could break SXP loop detection functionality and therefore needs to be handled carefully.

Wait until the SXP bindings that are propagated with the particular node ID in the path attribute are deleted, before you change the node ID.

Note A syslog is generated when you change the node ID.

Examples

```
switch(config)# cts sxp node-id 172.16.1.3
```

Related Commands

Command	Description
cts sxp enable	Enables CTS-SXP on a device.
show cts sxp	Displays the status of all CTS-SXP configurations.

cts sxp reconcile-period

To configure a Security Group Tag (SGT) Exchange Protocol (SXP) reconcile period timer, use the **cts sxp reconcile-period** command. To revert to the default, use the **no** form of this command.

cts sxp reconcile-period *seconds*

no cts sxp reconcile-period

Syntax Description

seconds	Number of seconds. The range is from 0 to 64000.

Command Default

60 seconds (1 minute)

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

After a peer terminates an SXP connection, an internal hold down timer starts. If the peer reconnects before the internal hold down timer expires, the SXP reconcile period timer starts. While the SXP reconcile period timer is active, the Cisco NX-OS software retains the SGT mapping entries learned from the previous connection and removes invalid entries.

Note Setting the SXP reconcile period to 0 seconds disables the timer and causes all entries from the previous connection to be removed.

This command requires the Advanced Services license.

Examples

This example shows how to configure the SXP reconcile period:

```
switch# configure terminal
switch(config)# cts sxp reconcile-period 120
```

This example shows how to revert to the default SXP reconcile period value:

```
switch# configure terminal
switch(config)# no cts sxp reconcile-period
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts sxp connection	Displays the Cisco TrustSec SXP configuration information.

cts sxp retry-period

To configure a Security Group Tag (SGT) Exchange Protocol (SXP) retry period timer, use the **cts sxp retry-period** command. To revert to the default, use the **no** form of this command.

cts sxp retry-period *seconds*

no cts sxp retry-period

Syntax Description

seconds	Number of seconds. The range is from 0 to 64000.

Command Default

120 seconds (2 minutes)

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

The SXP retry period determines how often the Cisco NX-OS software retries an SXP connection. When an SXP connection is not successfully set up, the Cisco NX-OS software makes a new attempt to set up the connection after the SXP retry period timer expires.

Note Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted.

This command requires the Advanced Services license.

Examples

This example shows how to configure the SXP retry period:

```
switch# configure terminal
switch(config)# cts sxp retry-period 120
```

This example shows how to revert to the default SXP retry period value:

```
switch# configure terminal
switch(config)# no cts sxp retry-period
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts sxp connection	Displays the Cisco TrustSec SXP peer connection information.

cts sxp speaker hold-time

To configure the global hold-time period of a speaker network device in a Cisco TrustSec Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4) network, use the **cts sxp speaker hold-time** command in global configuration mode. To remove the hold time from the speaker device, use the **no** form of this command.

cts sxp speaker hold-time *minimum-period*

no cts sxp speaker hold-time

Syntax Description

minimum-period	Minimum allowed hold time in seconds. The range is from 1 to 65534.

Command Default

The default hold time for a speaker device is 120 seconds.

Command Modes

Global configuration

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The Security Group Tag Exchange Protocol (SXP) uses a TCP-based, keepalive mechanism to determine if a connection is live. SXPv4 adds an optional negotiated keepalive mechanism, the hold-time period, in order to provide more predictable and timely detection of connection loss.

Hold time can be configured globally on a network device. This global configuration will apply the configuration to all SXP connections configured on the device.

You may configure a hold-time period locally on a speaker device or a default of 120 seconds is used. This is the shortest period of time a speaker is willing to send keepalive messages for keeping the connection active. Any shorter hold-time period would require a faster keepalive rate than the rate the speaker is ready to support. A value of 0xFFFF indicates that the keepalive mechanism is not used.

The hold-time negotiation between the speaker device and the listener device succeeds when the speaker's minimum acceptable hold time falls below or within the desirable hold-time range of the listener. (Use the **cts sxp listener hold-time** command to configure the hold time of the listener device.) If one end turns off the keepalive mechanism, the other end should also turn it off to make the negotiation successful.

The negotiation fails when the speaker's minimum acceptable hold-time is greater than the upper bound of the listener's hold-time range.

The selected hold-time period of a successful negotiation is the maximum of the speaker's minimum acceptable hold time and the lower bound of the listener's hold-time range.

The speaker calculates the keepalive time to one-third of the selected hold time by default, unless a different keepalive time is locally configured.

Examples

The following example shows how to configure the minimum hold time period of a speaker device for 300 seconds:

```
switch(config)# cts sxp speaker hold-time 300
```

Related Commands

Command	Description
cts sxp enable	Enables Cisco TrustSec SXP on a device.
cts sxp listener hold-time	Configures the hold time of a listener device in an SXPv4 network.
show cts sxp	Displays the status of all Cisco TrustSec SXP configurations.