E Commands

This chapter describes the Cisco NX-OS Security commands that begin with E.

enable Cert-DN-match

To enable LDAP users to login only if the user profile lists the subject-DN of the user certificate as authorized for login, use the **enable Cert-DN-match** command. To disable this configuration, use the **no** form of this command.

enable Cert-DN-match

no enable Cert-DN-match

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

LDAP server group configuration

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 enable LDAP users to login only if the user profile lists the subject-DN of the user certificate as authorized for login:

```
switch# configure terminal
switch(config)# aaa group server ldap LDAPServer1
switch(config-ldap)# server 10.10.2.2
switch(config-ldap)# enable Cert-DN-match
switch(config-ldap)
```

Related Commands

Command	Description
aaa group server ldap	Creates an LDAP server group and enters the LDAP server group configuration mode for that group.
enable user-server-group	Enables group validation for an LDAP server group.
server	Configures the LDAP server as a member of the LDAP server group.
show ldap-server groups	Displays the LDAP server group configuration.

enable

To enable a user to move to a higher privilege level after being prompted for a secret password, use the **enable** command.

enable *level*

Syntax Description

level	Privilege level to which the user must log in. The only available level is 15.

Defaults

Privilege level 15

Command Modes

EXEC configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the cumulative privilege of roles for command authorization on TACACS+ servers using the **feature privilege** command.

This command does not require a license.

Examples

This example shows how to enable the user to move to a higher privilege level after being prompted for a secret password:

```
switch# enable 15
```

Related Commands

Command	Description
enable secret priv-lvl	Enables a secret password for a specific privilege level.
feature privilege	Enables the cumulative privilege of roles for command authorization on TACACS+ servers.
show privilege	Displays the current privilege level, username, and status of cumulative privilege support.
username *user-id* priv-lvl	Enables a user to use privilege levels for authorization.

enable secret

To enable a secret password for a specific privilege level, use the **enable secret** command. To disable the password, use the **no** form of this command.

enable secret [0 | 5] *password* **[priv-lvl** *priv-lvl* **| all]**

no enable secret [0 | 5] *password* **[priv-lvl** *priv-lvl* **| all]**

Syntax Description

0	(Optional) Specifies that the password is in clear text.
5	(Optional) Specifies that the password is in encrypted format.
password	Password for user privilege escalation. It contains up to 64 alphanumeric, case-sensitive characters.
priv-lvl *priv-lvl*	(Optional) Specifies the privilege level to which the secret belongs. The range is from 1 to 15.
all	Adds or removes all privilege level secrets.

Defaults

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 cumulative privilege of roles for command authorization on TACACS+ servers using the **feature privilege** command.

This command does not require a license.

Examples

This example shows how to enable a secret password for a specific privilege level:

```
switch# configure terminal
switch(config)# feature privilege
switch(config)# enable secret 5 def456 priv-lvl 15
switch(config)# username user2 priv-lvl 15
switch(config)#
```

Related Commands

Command	Description
enable *level*	Enables the user to move to a higher privilege level after being prompted for a secret password.
feature privilege	Enables the cumulative privilege of roles for command authorization on TACACS+ servers.

Command	Description
show privilege	Displays the current privilege level, username, and status of cumulative privilege support.
username *user-id* priv-lvl	Enables a user to use privilege levels for authorization.

enable user-server-group

To enable group validation for an LDAP server group, use the **enable user-server-group** command. To disable group validation, use the **no** form of this command.

enable user-server-group

no enable user-server-group

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

LDAP server group configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must configure the LDAP server group name in the LDAP server.

Users can login through public-key authentication only if the username is listed as a member of this configured group in the LDAP server.

This command does not require a license.

Examples

This example shows how to enable group validation for an LDAP server group:

```
switch# configure terminal
switch(config)# aaa group server ldap LDAPServer1
switch(config-ldap)# server 10.10.2.2
switch(config-ldap)# enable user-server-group
switch(config-ldap)
```

Related Commands

Command	Description
aaa group server ldap	Creates an LDAP server group and enters the LDAP server group configuration mode for that group.
enable Cert-DN-match	Enables LDAP users to login only if the user profile lists the subject-DN of the user certificate as authorized for login.
server	Configures the LDAP server as a member of the LDAP server group.
show ldap-server groups	Displays the LDAP server group configuration.

encryption decrypt type6

To convert type-6 encrypted passwords back to their original state, use the **encryption decrypt type6** command.

encryption decrypt type6

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

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 convert type6 encrypted passwords back to their original state:

```
switch # encryption decrypt type6
Please enter current Master Key:
```

Related Commands

Command	Description
encryption re-encrypt obfuscated	Converts the existing obfuscated passwords to type6 encrypted passwords.
key config-key	Configures the master key for the type-6 encryption.

encrypt pause-frame

To configure pause frame encryption for Cisco Trusted Security (Cisco TrustSec) on an M1 module interface, use the **encrypt pause-frame** command. To remove the pause frame encryption, use the **no** form of this command.

encrypt pause-frame

no encrypt pause-frame

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled on the line cards that support the encryption of pause frames

Command Modes

Cisco TrustSec 802.1X configuration mode (config-if-cts-manual)
Cisco TrustSec manual configuration mode (config-if-cts-dotx1)

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

You must enable flow control on the interface by using the **flowcontrol** {**send** | **receive**} command.

When you enter the **no encrypt pause-frame** command, the pause frames are sent as unencypted. When you enter the e**ncrypt pause-frame** command, pause frames are sent encrypted over the Cisco TrustSec link.

You cannot enable Cisco TrustSec on interfaces in half-duplex mode. Use the **show interface** command to determine if an interface is configured for half-duplex mode.

This command is only needed in the unlikely event global pause has been enable. While pause is used in FCoE environments, it is not needed in typical Ethernet deployments.

This command does not apply to the M132XP-12L module.

Note F1 Series modules, F2 Series modules, F2e Series modules, and the N7K-M132XP-12(L) module support only clear pause frames. All other M1 Series modules support both secure (encrypted and decrypted) and clear pause frames.

Caution For the pause frame encryption or decryption configuration to take effect, you must enable and disable the interface, which disrupts traffic on the interface.

This command does not require a license.

Examples

This example shows how to decrypt an interface:

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

Related Commands

Command	Description
cts dot1x	Enables Cisco TrustSec authentication on an interface and enters Cisco TrustSec 802.1X configuration mode.
cts manual	Enters Cisco TrustSec manual configuration mode for an interface.
show cts interface	Displays the Cisco TrustSec configuration information for interfaces.

encryption delete type6

To delete strongly encrypted passwords on the NX-OS device, use the **encryption delete type6** command.

encryption delete type6

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

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 delete strongly encrypted passwords:

```
switch# configure terminal
encryption delete type6
Please enter current Master Key:
switch(config)#
```

Related Commands

Command	Description
encryption re-encrypt obfuscated	Converts the existing obfuscated passwords to type-6 encrypted passwords
key config-key	Configures the master key for the type-6 encryption.

encryption re-encrypt obfuscated

To convert the existing obfuscated passwords to type-6 encrypted passwords, use the **encryption re-encrypt obfuscated** command.

encryption re-encrypt obfuscated

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

When you use the **encryption re-encrypt obfuscated** command, the encrypted secrets such as, plain or weakly-encrypted passwords, are converted to type-6 encryption if the encryption service is enabled with a master key.

This command does not require a license.

Examples

This example shows how to convert the existing obfuscated passwords to type-6 encrypted passwords:

```
switch # encryption re-encrypt obfuscated
```

Related Commands

Command	Description
encryption decrypt type6	Converts type6 encrypted passwords back to their original state.

enrollment terminal

To enable manual cut-and-paste certificate enrollment through the switch console, use the **enrollment terminal** command. To revert to the default certificate enrollment process, use the **no** form of this command.

enrollment terminal

no enrollment terminal

Syntax Description

This command has no arguments or keywords.

Defaults

The default is the manual cut-and-paste method, which is the only enrollment method that the Cisco NX-OS software supports.

Command Modes

Trustpoint configuration

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 configure trustpoint enrollment through the switch console:

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# enrollment terminal
```

This example shows how to discard a trustpoint enrollment through the switch console:

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

Related Commands

Command	Description
crypto ca authenticate	Authenticates the certificate of the certificate authority.

eou allow clientless

To enable Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) posture validation of clientless endpoint devices, use the **eou allow clientless** command. To disable posture validation of clientless endpoint devices, use the **no** form of this command.

eou allow clientless

no eou allow clientless

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to allow EAPoUDP posture validation of clientless endpoint devices:

```
switch# config t
switch(config)# eou allow clientless
```

This example shows how to prevent EAPoUDP posture validation of clientless endpoint devices:

```
switch# config t
switch(config)# no eou allow clientless
```

Related Commands

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

eou default

To revert to the default global or interface configuration values for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), use the **eou default** command.

eou default

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to change the global EAPoUDP configuration to the default:

```
switch# config t
switch(config)# eou default
```

This example shows how to change the EAPoUDP configuration for an interface to the default:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou default
```

Related Commands

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

eou initialize

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

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

Syntax Description

all	Initializes all EAPoUDP sessions.
authentication	Initializes EAPoUDP sessions for a specific authentication types.
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*	Initializes the EAPoUDP sessions for a specific interface.
ip-address *ipv4-address*	Initializes the EAPoUDP sessions for a specific IPv4 address.
mac-address *mac-address*	Initializes the EAPoUDP sessions for a specific MAC address.
posturetoken *name*	Initializes the EAPoUDP sessions for a specific posture token.

Defaults

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to initialize all the EAPoUDP sessions:

```
switch# eou initialize all
```

This example shows how to initialize the EAPoUDP sessions that were statically authenticated:

```
switch# eou initialize authentication static
```

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

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

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

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

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

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

This example shows how to initialize all the EAPoUDP sessions for a posture token:

```
switch# eou initialize posturetoken healthy
```

Related Commands

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

eou logging

To enable Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) logging, use the **eou logging** command. To disable EAPoUDP logging, use the **no** form of this command.

eou logging

no eou logging

Syntax Description

This command has no arguments or keywords.

Defaults

Global configuration: Disabled

Interface configuration: Global configuration setting

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The setting for EAPoUDP logging on an interface overrides the global setting.

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to enable global EAPoUDP logging:

```
switch# config t
switch(config)# eou logging
```

This example shows how to disable global EAPoUDP logging:

```
switch# config t
switch(config)# no eou logging
```

This example shows how to enable EAPoUDP logging for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou logging
```

This example shows how to disable EAPoUDP logging for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no eou logging
```

Related Commands

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

eou max-retry

To configure the maximum number of attempts for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) globally or for an interface, use the **eou max-retry** command. To revert to the default, use the **no** form of this command.

eou max-retry *count*

no eou max-retry

Syntax Description

count	Maximum number of retry attempts. The range is from 1 to 3.

Defaults

Global configuration: 3

Interface configuration: global configuration value

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The maximum retries for an interface takes precedence over the globally configured value.

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to change the global maximum number of EAPoUDP retry attempts:

```
switch# config t
switch(config)# eou max-retry 2
```

This example shows how to revert to the default global maximum number of EAPoUDP retry attempts:

```
switch# config t
switch(config)# no eou max-retry
```

This example shows how to change the maximum number of EAPoUDP retry attempts for an interface:

```
switch# config t
switch(config) interface ethernet 1/1
switch(config-if)# eou max-retry 3
```

This example shows how to revert to the maximum number of EAPoUDP retry attempts for an interface:

```
switch# config t
switch(config) interface ethernet 1/1
switch(config-if)# no eou max-retry
```

Related Commands

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

eou port

To configure the User Datagram Protocol (UDP) port number for Extensible Authentication Protocol over UDP (EAPoUDP), use the **eou port** command. To revert to the default, use the **no** form of this command.

eou port *udp-port*

no eou port

Syntax Description

udp-port	UDP port number. The range is from 1 to 65535.

Defaults

21862 (0x5566)

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to change the UDP port number for EAPoUDP:

```
switch# config t
switch(config)# eou port 21856
```

This example shows how to revert to the default UDP port number for EAPoUDP:

```
switch# config t
switch(config)# no eou port
```

Related Commands

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

eou ratelimit

To configure the number of simultaneous posture validation sessions for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), use the **eou ratelimit** command. To revert to the default, use the **no** form of this command.

eou ratelimit *sessions*

no eou ratelimit

Syntax Description

sessions	Maximum number of simultaneous EAPoUDP posture validation sessions. The range is from 0 to 200.

Defaults

Global configuration: 20

Interface configuration: Global configuration setting

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Setting the EAPoUDP rate limit to zero (0) allows no simultaneous posture validation sessions.

The EAPoUDP rate limit for an interface overrides the globally EAPoUDP rate limit setting.

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to change the global maximum number of simultaneous EAPoUDP posture-validation sessions:

```
switch# config t
switch(config)# eou ratelimit 30
```

This example shows how to revert to the default global maximum number of simultaneous EAPoUDP posture-validation sessions:

```
switch# config t
switch(config)# no eou ratelimit
```

This example shows how to change the maximum number of simultaneous EAPoUDP posture-validation sessions for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou ratelimit 30
```

This example shows how to revert to the default maximum number of simultaneous EAPoUDP posture-validation sessions for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no eou ratelimit
```

Related Commands

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

eou revalidate (EXEC)

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

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

Syntax Description

all	Revalidates all EAPoUDP sessions.
authentication	Revalidates EAPoUDP sessions for specific authentication types.
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*	Revalidates the EAPoUDP sessions for a specific interface.
ip-address *ipv4-address*	Revalidates the EAPoUDP sessions for a specific IPv4 address.
mac-address *mac-address*	Revalidates the EAPoUDP sessions for a specific MAC address.
posturetoken *name*	Revalidates the EAPoUDP sessions for a specific posture token.

Defaults

None

Command Modes

Any command mode

Note The Cisco NX-OS software supports an **eou revalidate** command in global configuration mode. To use an EXEC-level **eou revalidate** command in global configuration mode, include the required keywords.

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to revalidate all the EAPoUDP sessions:

```
switch# eou revalidate all
```

This example shows how to revalidate all the EAPoUDP sessions:

```
switch# eou revalidate authentication static
```

This example shows how to revalidate all the EAPoUDP sessions:

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

This example shows how to revalidate all the EAPoUDP sessions:

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

This example shows how to revalidate all the EAPoUDP sessions:

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

This example shows how to revalidate all the EAPoUDP sessions:

```
switch# eou revalidate posturetoken healthy
```

Related Commands

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

eou revalidate (global configuration and interface configuration)

To enable automatic periodic revalidation of Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) sessions globally or for a specific interface, use the **eou revalidate** command. To revert to the default, use the **no** form of this command.

eou revalidate

no eou revalidate

Syntax Description

This command has no arguments or keywords.

Defaults

Global configuration: Enabled

Interface configuration: Global configuration value

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The automatic revalidation setting for an interface overrides the global setting for automatic revalidation.

Note The Cisco NX-OS software supports an **eou revalidate** command in EXEC configuration mode. To use an EXEC-level **eou revalidate** command in global configuration mode, include the required keywords.

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to disable global automatic revalidation of EAPoUDP sessions:

```
switch# config t
switch(config)# no eou revalidate
```

This example shows how to enable global automatic revalidation of EAPoUDP sessions:

```
switch# config t
switch(config)# eou revalidate
```

This example shows how to disable automatic revalidation of EAPoUDP sessions for an interface:

```
switch# config t
switch(config)# no eou revalidate
```

This example shows how to enable automatic revalidation of EAPoUDP sessions for an interface:

```
switch# config t
switch(config)# eou revalidate
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
eou timeout	Configures the timeout interval for EAPoUDP automatic periodic validation.
show eou	Displays EAPoUDP information.

eou timeout

To configure timeout intervals for the global Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) timers or for the EAPoUDP timers for an interface, use the **eou timeout** command. To revert to the default, use the **no** form of this command.

eou timeout {**aaa** *seconds* | **hold-period** *seconds* | **retransmit** *seconds* | **revalidation** *seconds* | **status-query** *seconds*}

no eou timeout {**aaa** | **hold-period** | **retransmit** | **revalidation** | **status-query**}

Syntax Description

aaa *seconds*	Specifies the AAA timeout interval. The range is from 0 to 60 seconds. **Note** Setting the AAA timeout interval to zero (0) disables the AAA timer.
hold-period *seconds*	Specifies the hold timeout interval. The range is from 60 to 86400 seconds.
retransmit *seconds*	Specifies the retransmit timeout interval. The range is from 1 to 60 seconds.
revalidation *seconds*	Specifies the period automatic revalidation timeout interval. The range is from 5 to 86400 seconds.
status-query *seconds*	Specifies the status query timeout interval. The range is from 10 to 1800 seconds.

Defaults

Global AAA timeout interval: 60 seconds (1 minute)

Global hold-period timeout: 180 seconds (3 minutes)

Global retransmit timeout interval: 3 seconds

Global revalidation timeout interval: 36000 seconds (10 hours)

Global status query timeout interval: 300 seconds (5 minutes)

Interface timeout intervals: Global configuration values

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The timeout interval values for the interface timers override the global timeout values.

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to change the global AAA timeout interval:

```
switch# config t
switch(config)# eou timeout aaa 50
```

This example shows how to change the AAA timeout interval for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout aaa 60
```

This example shows how to change the global hold-period timeout interval:

```
switch# config t
switch(config)# eou timeout hold-period 480
```

This example shows how to change the hold-period timeout interval for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout hold-period 540
```

This example shows how to change the global retransmit timeout interval:

```
switch# config t
switch(config)# eou timeout retransmit 5
```

This example shows how to change the retransmit timeout interval for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout retransmit 4
```

This example shows how to change the global revalidation timeout interval:

```
switch# config t
switch(config)# eou timeout revalidation 34000
```

This example shows how to change the revalidation timeout interval for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout revalidation 30000
```

This example shows how to change the global status-query timeout interval:

```
switch# config t
switch(config)# eou timeout status-query 240
```

This example shows how to change the status-query timeout interval for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout status-query 270
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
eou revalidate (global configuration)	Enables periodic automatic revalidation of endpoint devices.
show eou	Displays EAPoUDP information.

eq

To specify a single port as a group member in an IP port object group, use the **eq** command. To remove a single port group member from the port object group, use the **no** form of this command.

[*sequence-number*] **eq** *port-number*

no {*sequence-number* | **eq** *port-number*}

Syntax Description

sequence-number	(Optional) Sequence number for this group member. Sequence numbers maintain the order of group members within an object group. Valid sequence numbers are from 1 to 4294967295. If you do not specify a sequence number, the device assigns a number that is 10 greater than the largest sequence number in the current object group.
port-number	Port number that this group member matches. Valid port numbers are from 0 to 65535.

Defaults

None

Command Modes

IP port object group configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

IP port object groups are not directional. Whether an **eq** command matches a source or destination port or whether it applies to inbound or outbound traffic depends upon how you use the object group in an ACL.

This command does not require a license.

Examples

This example shows how to configure an IP port object group named port-group-05 with a group member that matches traffic sent to or from port 443:

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# eq 443
```

Related Commands

Command	Description
gt	Specifies a greater-than group member in an IP port object group.
lt	Specifies a less-than group member in an IP port object group.
neq	Specifies a not-equal-to group member in an IP port object group.

Command	Description
object-group ip port	Configures an IP port object group.
range	Specifies a port-range group member in an IP port object group.
show object-group	Displays object groups.