E Commands

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

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. |

Command Default   Privilege level 15

Command Modes   EXEC configuration mode

Command History

Release	Modification
6.0(2)N1(1)	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.

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
switch#
```

Related Commands

Command	Description
enable secret	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	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* [**all** | **priv-lvl** *priv-lvl*]

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

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.	
all	(Optional) Adds or removes all privilege level secrets.	
priv-lvl *priv-lvl*	(Optional) Specifies the privilege level to which the secret belongs. The range is from 1 to 15.	

Command Default   Disabled

Command Modes   Global configuration mode

Command History	Release	Modification
	6.0(2)N1(1)	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.

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	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	Enables a user to use privilege levels for authorization.

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
	7.3(0)N1(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.