F Commands

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

feature (user role feature group)

To configure a feature in a user role feature group, use the **feature** command. To delete a feature in a user role feature group, use the **no** form of this command.

feature *feature-name*

no feature *feature-name*

Syntax Description

feature-name	Switch feature name as listed in the **show role feature** command output.

Command Default

None

Command Modes

User role feature group configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

Use the **show role** feature command to list the valid feature names to use in this command.

Examples

This example shows how to add features to a user role feature group:

```
switch(config)# role feature-group name SecGroup
switch(config-role-featuregrp)# feature aaa
switch(config-role-featuregrp)# feature radius
switch(config-role-featuregrp)# feature tacacs
```

This example shows how to remove a feature from a user role feature group:

```
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)# no feature callhome
```

Related Commands

Command	Description
role feature-group name	Creates or configures a user role feature group.
show role feature-group	Displays the user role feature groups.

feature dhcp

To enable the Dynamic Host Configuration Protocol (DHCP) snooping feature on the device, use the **feature dhcp** command. To disable the DHCP snooping feature and remove all configuration related to DHCP snooping, use the **no** form of this command.

feature dhcp

no feature dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

The DHCP snooping feature is disabled by default. DHCP snooping can be enabled or disabled on VLANs.

If you have not enabled the DHCP snooping feature, commands related to DCHP snooping are unavailable.

Dynamic ARP inspection and IP Source Guard depend upon the DHCP snooping feature.

If you disable the DHCP snooping feature, the device discards all configuration related to DHCP snooping configuration, including the following features:

- DHCP snooping
- DHCP relay
- Dynamic ARP Inspection (DAI)
- IP Source Guard

If you want to turn off DHCP snooping and preserve configuration related to DHCP snooping, disable DHCP snooping globally with the **no ip dhcp snooping** command.

Access-control list (ACL) statistics are not supported if the DHCP snooping feature is enabled.

Examples

This example shows how to enable DHCP snooping:

```
switch(config)# feature dhcp
switch(config)#
```

This example shows how to disable DHCP snooping:

```
switch(config)# no feature dhcp
switch(config)#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
ip dhcp snooping	Globally enables DHCP snooping on the device.
show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.

feature http-server

To enable HTTP or Hypertext Transfer Protocol Secure (HTTPS) on the switch, use the **feature http-server** command. To disable the HTTP or HTTPS server, use the **no** form of this command.

feature http-server

no feature http-server

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

In releases earlier than Cisco NX-OS Release 5.2(1)N1(1), HTTP and HTTPS are enabled on the switch by default.

Examples

This example shows how to enable the HTTP server on the switch and verify the status of the HTTP server:

```
switch(config)# feature http-server
switch(config)# exit
switch# show feature
Feature Name          Instance  State
--------------------  --------  --------
assoc_mgr             1         enabled
cimserver             1         disabled
dhcp-snooping         1         disabled
fabric-binding        1         disabled
fc-port-security      1         disabled
fcoe                  1         enabled
fcsp                  1         disabled
fex                   1         enabled
fport-channel-trunk   1         disabled
http-server           1         enabled
interface-vlan        1         enabled
lacp                  1         enabled
ldap                  1         disabled
lldp                  1         enabled
niv                   1         disabled
npiv                  1         disabled
npv                   1         disabled
otv                   1         disabled
port_track            1         disabled
```

```
private-vlan          1         enabled
privilege             1         enabled
sshServer             1         enabled
tacacs                1         enabled
telnetServer          1         enabled
udld                  1         enabled
vpc                   1         enabled
vtp                   1         enabled
switch# show http-server
http-server enabled
switch#
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.
show feature	Displays the features enabled or disabled on the switch.
show http-server	Displays the HTTP or HTTPS server configuration.

feature port-security

To enable port security on Layer 2 interfaces, use the **feature port-security** command. To disable port security, use the **no** form of this command.

feature port-security

no feature port-security

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

Use the port security feature to secure a port by limiting and identifying the MAC addresses of the switches that are allowed to access the port.

You can enable port security on a virtual port channel (vPC) port only if the following occurs:

- Port security is enabled on both the vPC peers
- Port security is enabled on the vPC port on both the vPC peers.

This command does not require a license.

Examples

This example shows how to enable port security on the switch:

```
switch# configure terminal
switch(config)# feature port-security
switch(config)#
```

This example shows how to disable port security on the switch:

```
switch# configure terminal
switch(config)# no feature port-security
switch(config)#
```

Related Commands

Command	Description
show feature	Displays the features that are enabled or disabled on the switch.

Command	Description
show port-security	Displays the port security configuration information.
switchport port-security	Configures the switchport parameters to establish port security.

feature privilege

To enable the cumulative privilege of roles for command authorization on RADIUS and TACACS+ servers, use the **feature privilege** command. To disable the cumulative privilege of roles, use the **no** form of this command.

feature privilege

no feature privilege

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

When the **feature privilege** command is enabled, privilege roles inherit the permissions of lower level privilege roles.

Examples

This example shows how to enable the cumulative privilege of roles:

```
switch(config)# feature privilege
switch(config)#
```

This example shows how to disable the cumulative privilege of roles:

```
switch(config)# no feature privilege
switch(config)#
```

Related Commands

Command	Description
enable	Enables a user to move to a higher privilege level.
enable secret priv-lvl	Enables a secret password for a specific privilege level.
show feature	Displays the features enabled or disabled on the switch.
show privilege	Displays the current privilege level, username, and status of cumulative privilege support.
username	Enables a user to use privilege levels for authorization.

feature tacacs+

To enable TACACS+, use the **feature tacacs+** command. To disable TACACS+, use the **no** form of this command.

feature tacacs+

no feature tacacs+

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS+.

Note When you disable TACACS+, the Cisco NX-OS software removes the TACACS+ configuration.

Examples

This example shows how to enable TACACS+:

```
switch(config)# feature tacacs+
```

This example shows how to disable TACACS+:

```
switch(config)# no feature tacacs+
```

Related Commands

Command	Description
show feature	Displays whether or not TACACS+ is enabled on the switch.
show tacacs+	Displays TACACS+ information.