F Commands

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	Cisco NX-OS feature name as listed in the **show role feature** command output.

Command Default

None

Command Modes

User role feature group configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

This command does not require a license.

Examples

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

```
switch# configure terminal
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 user role feature group:

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

Related Commands

Command	Description
show role feature-group	Displays the user role feature groups.

feature cts

To enable the Cisco TrustSec feature, use the **feature cts** command. To revert to the default, use the **no** form of this command.

feature cts

no feature cts

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 dot1x** command.

The users can enable feature cts command even without having any license installed.

Note The Cisco TrustSec feature does not have a license grace period. You must install the Advanced Services license to configure this feature.

This command requires the Advanced Services license.

Examples

This example shows how to enable the Cisco TrustSec feature:

```
switch# configure terminal
switch(config)# feature cts
```

This example shows how to disable the Cisco TrustSec feature:

```
switch# configure terminal
switch(config)# no feature cts
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show cts	Displays the Cisco TrustSec status information.

feature dhcp

To enable the 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, including DHCP relay, dynamic ARP inspection (DAI), and IP Source Guard configuration, use the **no** form of this command.

feature dhcp

no feature dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The DHCP snooping feature is disabled by default.

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
- 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.

This command does not require a license.

Examples

This example shows how to enable DHCP snooping:

```
switch# configure terminal
```

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

Related Commands

Command	Description
clear ip dhcp snooping binding	Clears the DHCP snooping binding database.
ip dhcp snooping	Globally enables DHCP snooping on the device.
service dhcp	Enables or disables the DHCP relay agent.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.

feature dot1x

To enable the 802.1X feature, use the **feature dot1x** command. To revert to the default, use the **no** form of this command.

feature dot1x

no feature dot1x

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

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

Note If you disable the 802.1X feature, all 802.1X configuration is lost. If you want to disable 802.1X authentication, use the **no dot1x system-auth-control** command.

This command does not require a license.

Examples

This example shows how to enable 802.1X:

```
switch# configure terminal
switch(config)# feature dot1x
```

This example shows how to disable 802.1X:

```
switch# configure terminal
switch(config)# no feature dot1x
```

Related Commands

Command	Description
show dot1x	Displays 802.1X status information.

feature eou

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

feature eou

no feature eou

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

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

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

This command does not require a license.

Examples

This example shows how to enable EAPoUDP:

```
switch# configure terminal
switch(config)# feature eou
```

This example shows how to disable EAPoUDP:

```
switch# configure terminal
switch(config)# no feature eou
```

Related Commands

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

feature ldap

To enable Lightweight Directory Access Protocol (LDAP), use the **feature ldap** command. To disable LDAP, use the **no** form of this command.

feature ldap

no feature ldap

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

You must use the **feature ldap** command before you configure LDAP.

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

This command does not require a license.

Examples

This example shows how to enable LDAP:

```
switch# configure terminal
switch(config)# feature ldap
```

This example shows how to disable LDAP:

```
switch# configure terminal
switch(config)# no feature ldap
```

Related Commands

Command	Description
show running-config ldap	Displays the LDAP configuration in the running configuration.
show startup-config ldap	Displays the LDAP configuration in the startup configuration.

feature mka

To enable the MACsec Key Agreement (MKA) feature, use the **feature mka** command. To disable the MKA feature, use the **no** form of this command.

feature mka

no feature mka

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
8.2(1)	This command was introduced.

Examples

This example shows how to enable the MKA feature:

```
switch# configure terminal
switch(config)# feature mka
```

This example shows how to disable the MKA feature:

```
switch# configure terminal
switch(config)# no feature mka
```

Related Commands

Command	Description
cipher suite	Configures the cipher suite for encrypting traffic with MACsec.
conf-offset	Configures the confidentiality offset for MKA encryption.
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.
key-octet-string	Configures the text for a MACsec key.

Command	Description
key-server-priority	Configures the preference for a device to serve as the key server for MKA encryption.
macsec keychain policy	Configures the MACsec keychain policy.
macsec policy	Configures the MACsec policy.
sak-expiry-time *time*	Sets an expiry time for a force SAK rekey.
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.

feature password encryption aes

To enable the Advanced Encryption Standard (AES) password encryption feature, use the **feature password encryption aes** command. To disable the AES password encryption feature, use the **no** form of this command.

feature password encryption aes

no feature password encryption aes

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode (config)

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

You can enable the AES password encryption feature without a master key, but encryption starts only when a master key is present in the system. To configure a master key, use the key config-key command.

This command does not require a license.

Examples

This example shows how to enable the AES password encryption feature:

```
switch# configure terminal
switch(config)# feature password encryption aes
switch(config)#
```

This example shows how to disable the AES password encryption feature:

```
switch(config)# no feature password encryption aes
switch(config)#
```

Related Commands

Command	Description
key config-key	Configures the master key for type-6 encryption.
show encryption service stat	Displays the status of the encryption service.

feature port-security

To enable the port security feature globally, use the **feature port-security** command. To disable the port security feature globally, 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

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Port security is disabled globally by default.

Port security is local to each virtual device context (VDC). If necessary, switch to the correct VDC before using this command.

This command does not require a license.

Enabling Port Security

If you enable port security globally, all other commands related to port security become available.

If you are reenabling port security, no port security configuration is restored from the last time that port security was enabled.

Disabling Port Security

If you disable port security globally, all port security configuration is removed, including any interface configuration for port security and all secured MAC addresses, regardless of the method by which the device learned the addresses.

Examples

This example shows how to enable port security globally:

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

Related Commands

Command	Description
clear port-security	Clears dynamically learned, secure MAC addresses.
debug port-security	Provides debugging information for port security.
show port-security	Shows information about port security.
switchport port-security	Enables port security on a Layer 2 interface.

feature privilege

To enable the cumulative privilege of roles for command authorization on 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

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

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

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

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

2010 Feb 12 12:52:06 switch %FEATURE-MGR-2-FM_AUTOCKPT_IN_PROGRESS: AutoCheckpoint
system-fm-privilege's creation in progress...
switch(config)# 2010 Feb 12 12:52:06 switch %FEATURE-MGR-2-FM_AUTOCKPT_SUCCEEDED
AutoCheckpoint created successfully
```

Related Commands

Command	Description
enable *level*	Enables a user to move to a higher privilege level.
enable secret priv-lvl	Enables a secret password for a specific privilege level.

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

feature scp-server

To configure a secure copy (SCP) server on the Cisco NX-OS device in order to copy files to and from a remote device, use the **feature scp-server** command. To disable an SCP server, use the **no** form of this command.

feature scp-server

no feature scp-server

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

After you enable the SCP server, you can execute an SCP command on the remote device to copy the files to or from the Cisco NX-OS device.

The arcfour and blowfish cipher options are not supported for the SCP server.

This command does not require a license.

Examples

This example shows how to enable the SCP server on the Cisco NX-OS device:

```
switch# configure terminal
switch(config)# feature scp-server
switch(config)#
```

This example shows how to disable the SCP server on the Cisco NX-OS device:

```
switch# configure terminal
switch(config)# no feature scp-server
switch(config)#
```

Related Commands

Command	Description
feature sftp-server	Enables the SFTP server on the Cisco NX-OS device.

feature sftp-server

To configure a secure FTP (SFTP) server on the Cisco NX-OS device in order to copy files to and from a remote device, use the **feature sftp-server** command. To disable an SFTP server, use the no form of this command.

feature sftp-server

no feature sftp-server

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

After you enable the SFTP server, you can execute an SFTP command on the remote device to copy the files to or from the Cisco NX-OS device.

This command does not require a license.

Examples

This example shows how to enable the SFTP server on the Cisco NX-OS device:

```
switch# configure terminal
switch(config)# feature sftp-server
switch(config)#
```

This example shows how to disable the SFTP server on the Cisco NX-OS device:

```
switch# configure terminal
switch(config)# no feature sftp-server
switch(config)#
```

Related Commands

Command	Description
feature scp-server	Enables the SCP server on the Cisco NX-OS device.

feature ssh

To enable the Secure Shell (SSH) server for a virtual device context (VDC), use the **feature ssh** command. To disable the SSH server, use the **no** form of this command.

feature ssh

no feature ssh

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced to replace the **ssh server enable** command.

Usage Guidelines

The Cisco NX-OS software supports SSH version 2.

This command does not require a license.

Examples

This example shows how to enable the SSH server:

```
switch# configure terminal
switch(config)# feature ssh
```

This example shows how to disable the SSH server:

```
switch# configure terminal
switch(config)# no feature ssh

XML interface to system may become unavailable since ssh is disabled
```

Related Commands

Command	Description
show feature	Displays the enable status of the features.
show ssh server	Displays the SSH server key information.

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

Command History

Release	Modification
4.0(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.

This command does not require a license.

Examples

This example shows how to enable TACACS+:

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

This example shows how to disable TACACS+:

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

Related Commands

Command	Description
show tacacs+	Displays TACACS+ information.

feature telnet

To enable the Telnet server for a virtual device context (VDC), use the **feature telnet** command. To disable the Telnet server, use the **no** form of this command.

feature telnet

no feature telnet

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced to replace the **telnet server enable** command.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable the Telnet server:

```
switch# configure terminal
switch(config)# feature telnet
```

This example shows how to disable the Telnet server:

```
switch# configure terminal
switch(config)# no feature telnet

XML interface to system may become unavailable since ssh is disabled
```

Related Commands

Command	Description
show feature	Displays the enable status of the features.
show telnet server	Displays the SSH server key information.

filter

To configure one or more certificate mapping filters within the filter map, use the **filter** command.

filter [**subject-name** *subject-name*| **altname-email** *e-mail-ID*| **altname-upn** *user-principal-name*]

Syntax Description

subject-name	(Optional) Specifies the subject name of the certificate.
subject-name	Required subject name in LDAP distinguished name (DN) string format. For example: cn=%username%,ou=PKI,o=Acme,c=US
altname-email	(Optional) Specifies the e-mail ID as an alternate name.
e-mail-ID	E-mail address that must be present in the certificate as a subject alternative name. For example: %username%@*
altname-upn	(Optional) Specifies the user principal name as an alternate name.
user-principal-name	Principal name that must be present in the certificate as a subject alternative name. For example: %username-without-domain%@%hostname%

Command Default

None

Command Modes

Certificate mapping filter configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

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

The validation passes if the certificate passes all of the filters configured in the map.

This command does not require a license.

Examples

This example shows how to configure a certificate mapping filter within the filter map:

```
switch# configure terminal
switch(config)# crypto certificatemap mapname filtermap1
switch(config-certmap-filter)# filter altname-email jsmith@acme.com
```

Related Commands

Command	Description
crypto certificatemap mapname	Creates a filter map.
show crypto certificatemap	Displays the certificate mapping filters.

fips mode enable

To enable Federal Information Processing Standards (FIPS) mode, use the **fips mode enable** command. To disable FIPS mode, use the no form of this command.

fips mode enable

no fips mode enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

Before enabling FIPS mode, ensure that you are in the default virtual device context (VDC).

FIPS has the following prerequisites:

- Disable Telnet. Users should log in using Secure Shell (SSH) only.
- Disable SNMPv1 and v2. Any existing user accounts on the device that have been configured for SNMPv3 should be configured only with SHA for authentication and AES/3DES for privacy.
- Delete all SSH server RSA1 key-pairs.
- Enable HMAC-SHA1 message integrity checking (MIC) for use during the Cisco TrustSec Security Association Protocol (SAP) negotiation. To do so, enter the sap hash-algorithm HMAC-SHA-1 command from the cts-manual or cts-dot1x mode.

This command does not require a license.

Examples

This example shows how to enable FIPS mode:

```
switch# configure terminal
switch(config)# fips mode enable

FIPS mode is enabled
```

This example shows how to disable FIPS mode:

```
switch# configure terminal
switch(config)# no fips mode enable
```

```
FIPS mode is disabled
```

Related Commands

Command	Description
show fips status	Displays the status of Federal Information Processing Standard (FIPS) mode.

fragments

To optimize whether an IPv4 or IPv6 ACL permits or denies noninitial fragments that do not match an explicit **permit** or **deny** command in the ACL, use the **fragments** command. To disable fragment optimization, use the **no** form of this command.

fragments {**deny-all**| **permit-all**}

no fragments {**deny-all**| **permit-all**}

Syntax Description

deny-all	Specifies that noninitial fragments of flows that are matched by the ACL are always dropped.
permit-all	Specifies that any noninitial fragments of a flow are permitted when the initial fragment of the flow was permitted by the ACL.

Command Default

None

Command Modes

IPv4 ACL configuration

IPv6 ACL configuration

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

The **fragments** command allows you to simplify the configuration of an IP ACL when you want to permit or deny noninitial fragments that do not match an explicit **permit** or **deny** command in the ACL. Instead of controlling noninitial fragment handling by using many **permit** or **deny** commands that specify the **fragments** keyword, you can use the **fragments** command instead.

When a device applies to traffic an ACL that contains the **fragments** command, it only matches noninitial fragments that do not match any explicit **permit** or **deny** commands in the ACL.

This command does not require a license.

Examples

This example shows how to enable fragment optimization in an IPv4 ACL named lab-acl. The **permit-all** keyword means that the ACL permits any noninitial fragment that does not match a **deny** command that includes the **fragments** keyword.

```
switch# configure terminal
```

```
switch(config)# ip access-list lab-acl
switch(config-acl)# fragments permit-all
```

This example shows the lab-acl IPv4 ACL, which includes the **fragments** command. The **fragments** command appears at the beginning of the ACL for convenience, but the device permits noninitial fragments only after they do not match all other explicit rules in the ACL.

```
switch(config-acl)# show ip access-lists lab-acl

IP access list lab-acl
fragments permit-all
10 permit tcp 10.0.0.0/8 172.28.254.254/24 eq tacacs
20 permit tcp 10.0.0.0/8 172.28.254.154/24 eq tacacs
30 permit tcp 10.0.0.0/8 172.28.254.54/24 eq tacacs
```

Related Commands

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
deny (IPv6)	Configures a deny rule in an IPv6 ACL.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.
permit (IPv6)	Configures a permit rule in an IPv6 ACL.
show ip access-list	Displays all IPv4 ACLs or a specific IPv4 ACL.
show ipv6 access-list	Displays all IPv6 ACLs or a specific IPv6 ACL.