F to H Commands

This chapter describes the Cisco NX-OS Security commands that begin with F to H.

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.

Defaults

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.

Defaults

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.

Defaults

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.

Defaults

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.

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.

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.

Defaults

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 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.

Defaults

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.

Defaults

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.

Defaults

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.

Defaults

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.

Defaults

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.

Defaults

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.

Defaults

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.

Defaults

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%

Defaults

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.

Defaults

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 t
switch(config)# fips mode enable
FIPS mode is enabled
```

This example shows how to disable FIPS mode:

```
switch# configure t
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.

Defaults

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.

gt

To specify a greater-than group member for an IP port object group, use the **gt** command. A greater-than group member matches port numbers that are greater than (and not equal to) the port number specified in the member. To remove a greater-than group member from the port-object group, use the **no** form of this command.

[*sequence-number*] **gt** *port-number*

no {*sequence-number* | **gt** *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 traffic matching this group member exceeds. The *port-number* argument can be a whole number between 0 and 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 a **gt** 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 49152 through port 65535:

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# gt 49151
```

Related Commands

Command	Description
eq	Specifies an equal-to group member in an IP port object group.
lt	Specifies a less-than group member in an IP port object group.

Command	Description
neq	Specifies a not-equal-to group member in an IP port object group.
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.

hardware access-list allow deny ace

To enable deny ace support for seq based feature, use the **hardware access-list allow deny ace** command. To disable this feature, use the **no** form of the command.

hardware access-list allow deny ace

no hardware access-list allow deny ace

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
6.1(3)	This command was introduced.

Usage Guidelines

This command does not require a license.

Note Deny ace feature is not supported on F1 module.

This example shows how to enable deny ace feature:

```
switch# configure terminal
switch(config)# hardware access-list allow deny ace
switch(config)#
```

This example shows how to disable deny ace feature:

```
switch# configure terminal
switch(config)# no hardware access-list allow deny ace
switch(config)#
```

Related Commands

Command	Description
hardware access-list update	Configures how a supervisor module updates an I/O module with changes to an ACL.

hardware access-list capture

To enable access control list (ACL) capture on all virtual device contexts (VDCs), use the **hardware access-list capture** command. To disable ACL capture, use the **no** form of the command.

hardware access-list capture

no hardware access-list capture

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
6.1(1)	Added support for M2 series modules.
5.2(1)	This command was introduced.

Usage Guidelines

Only M Series modules support ACL capture.

ACL capture is a -assisted feature and is not supported for the management interface or for control packets originating in the supervisor. It is also not supported for software ACLs such as SNMP community ACLs and virtual teletype (VTY) ACLs.

Enabling ACL capture disables ACL logging for all VDCs and the rate limiter for ACL logging.

Only one ACL capture session can be active at any given time in the system across VDCs.

This command does not require a license.

Examples

This example shows how to enable ACL capture on all VDCs:

```
switch# configure terminal
switch(config)# hardware access-list capture

This example shows how to disable ACL capture on all VDCs:

switch # configure terminal
switch(config)# no hardware access-list capture
```

Related Commands

Command	Description
hardware access-list update	Configures how a supervisor module updates an I/O module with changes to an ACL.

hardware access-list resource feature bank-mapping

To enable access control list (ACL) ternary control address memory (TCAM) bank mapping for feature groups and classes, use the **hardware access-list resource feature bank-mapping** command. To disable ACL TCAM bank mapping, use the **no** form of the command.

hardware access-list resource feature bank-mapping

no hardware access-list resource feature bank-mapping

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command is available only in the default virtual device context (VDC) but applies to all VDCs.

F1 Series modules do not support ACL TCAM bank mapping. Resource pooling and ACL TCAM bank mapping cannot be enabled at the same time.

Examples

This example shows how to enable ACL TCAM bank mapping for feature groups and classes:

```
switch(config)# hardware access-list resource feature bank-mapping
```

Related Commands

Command	Description
show system internal access-list feature bank-class map	Displays the ACL TCAM bank mapping feature group and class combination tables.

hardware access-list resource pooling

To allow ACL-based features to use more than one TCAM bank on one or more I/O modules, use the **hardware access-list resource pooling** command. You can also enable flexible TCAM bank chaining feature with PORT-VLAN or VLAN-VLAN modes. To restrict ACL-based features to using one TCAM bank on an I/O module, use the **no** form of this command.

hardware access-list resource pooling [**port-vlan** | **vlan-vlan**] **module** {*module-number* | **all**}

no hardware access-list resource pooling [**port-vlan** | **vlan-vlan**] **module** {*module-number* | **all**}

Syntax Description

module	Specifies the module.
port-vlan	Specifies the port-vlan mode that allows you to configure a single port feature and a single VLAN feature on a destination per direction.
vlan-vlan	Specifies the vlan-vlan mode that allows you to configure two VLAN features on a destination per direction.
module-number	Specifies the I/O module(s). The *slot-number-list* argument allows you to specify modules by the slot number that they occupy. You can specify a single I/O module, a range of slot numbers, or comma-separated slot numbers and ranges.
all	Specifies all the modules. Note that the PORT-VLAN and VLAN-VLAN modes are supported only on the F3 modules. So, you cannot enable the flexible TCAM bank chaining for all the modules.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was modified to support flexible bank chaining feature with VLAN-VLAN and PORT-VLAN modes.
4.2(1)	The hyphen was removed between the **resource** and **pooling** keywords.
4.1(2)	This command was introduced.

Usage Guidelines

By default, each ACL-based feature can use one TCAM bank on an I/O module. This default behavior limits each feature to 16,000 TCAM entries. If you have very large security ACLs, you may encounter this limit. The command allows you to make more than 16,000 TCAM entries available to ACL-based features.

If you want to enable bank chaining for the entire system, Cisco recommends adding the configuration for the entire module range, even if a module is not present, using the module range command, as described in the Examples section.

This command does not require a license.

Examples

This example shows how to enable ACL programming across TCAM banks on the I/O module in slot 1:

```
switch# config t
switch(config)# hardware access-list resource pooling module 1
```

This example shows how to enable bank chaining for all modules in a 10-slot chassis (excluding supervisor slots 5 and 6):

```
switch# config t
switch(config)# hardware access-list resource pooling module 1-4, 7-10
```

When a new module is inserted, bank chaining is enabled automatically for that module, without you having to remember to enter the command.

This example shows how to enable VLAN-VLAN mode for the module 3:

```
switch# config t
switch(config)# hardware access-list resource pooling vlan-vlan module 3
```

Related Commands

Command	Description
hardware access-list update	Configures atomic or non-atomic update of access-list, and default access-list result during the non-atomic hardware update.
show running-config all	Displays the running configuration, including the default configuration.
show system internal access-list globals	Displays the access control list (ACL) ternary content addressable memory (TCAM) common information along with the bank chaining mode.

hardware access-list update

To configure how a supervisor module updates an I/O module with changes to an access-control list (ACL), use the **hardware access-list update** command in the default virtual device context (VDC). To disable atomic updates, use the **no** form of this command.

hardware access-list update {**atomic** | **default-result permit**}

no hardware access-list update {**atomic** | **default-result permit**}

Syntax Description

atomic	Specifies that the device performs atomic updates, which do not disrupt traffic during the update. By default, a Cisco Nexus 7000 Series device performs atomic ACL updates.
default-result permit	Specifies that, during non-atomic updates, the device permits traffic that the updated ACL applies to.

Defaults

atomic

Command Modes

Global configuration

Command History

Release	Modification
4.1(4)	This command is available only in the default VDC.
4.1(2)	This command was introduced to replace the **platform access-list update** command.

Usage Guidelines

In Cisco NX-OS Release 4.1(4) and later releases, the **hardware access-list update** command is available in the default VDC only and affects all VDCs.

By default, when a supervisor module of a Cisco Nexus 7000 Series device updates an I/O module with changes to an ACL, it performs an atomic ACL update. An atomic update does not disrupt traffic that the updated ACL applies to; however, an atomic update requires that an I/O module that receives an ACL update has enough available resources to store each updated ACL entry in addition to all preexisting entries in the affected ACL. After the update occurs, the additional resources used for the update are freed. If the I/O module lacks the required resources, the device generates an error message and the ACL update to the I/O module fails.

If an I/O module lacks the resources required for an atomic update, you can disable atomic updates by using the **no hardware access-list update atomic** command in the default VDC; however, during the brief time required for the device to remove the preexisting ACL and implement the updated ACL, traffic that the ACL applies to is dropped by default.

If you want to permit all traffic that an ACL applies to while it receives a nonatomic update, use the **hardware access-list update default-result permit** command in the default VDC.

This command does not require a license.

Examples

Note In Cisco NX-OS Release 4.1(4) and later releases, the **hardware access-list update** command is available in the default VDC only. To verify that the current VDC is the VDC 1 (the default VDC), use the **show vdc current-vdc** command.

This example shows how to disable atomic ACL updates:

```
switch# config t
switch(config)# no hardware access-list update atomic
```

This example shows how to permit affected traffic during a nonatomic ACL update:

```
switch# config t
switch(config)# hardware access-list update default-result permit
```

This example shows how to revert to the atomic update method:

```
switch# config t
switch(config)# no hardware access-list update default-result permit
switch(config)# hardware access-list update atomic
```

Related Commands

Command	Description
show running-config all	Displays the running configuration, including the default configuration.

hardware rate-limiter

To configure rate limits in packets per second on supervisor-bound traffic, use the **hardware rate-limiter** command. To revert to the default, use the **no** form of this command.

hardware rate-limiter {**access-list-log** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **copy** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **f1** {**rl-1** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-2** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-3** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-4** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-5** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **layer-2** {**l2pt** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **mcast-snooping** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **port-security** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **storm-control** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **vpc-low** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **layer-3** {**control** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **glean** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **glean-fast** {*packets* | **disable**} [**module** *module* [**port** *start end]*] | **mtu** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **multicast** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **ttl** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **receive** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | [**portgroup-multiplier** *multiplier* **module** *module*]

no hardware rate-limiter {**access-list-log** {*packets* | **disable**} [**module** *module* [**port** *start end*]] || **copy** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **f1** {**rl-1** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-2** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-3** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-4** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-5** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **layer-2** {**l2pt** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **mcast-snooping** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **port-security** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **storm-control** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **vpc-low** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **layer-3** {**control** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **glean** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **glean-fast** {*packets* | **disable**} [**module** *module* [**port** *start end]*] | **mtu** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **multicast** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **ttl** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **receive** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | [**portgroup-multiplier** *multiplier* **module** *module*]

Syntax Description

access-list-log	Specifies packets copied to the supervisor module for access list logging. The default rate is 100 packets per second.
packets	Number of packets per second. The range is from 1 to 33554431.
disable	Disables the rate limiter.
module *module*	(Optional) Specifies a module number. The range is from 1 to 18.
port *start end*	(Optional) Specifies a port start index. The range is from 1 to 32. You specify the start port and and end port with a space in between them.
copy	Specifies data and control packets copied to the supervisor module. The default rate is 30000 packets per second.
f1	Specifies the control packets from the F1 modules to the supervisor.
rl-1	Specifies the F1 rate-limiter 1.
rl-2	Specifies the F1 rate-limiter 2.

rl-3	Specifies the F1 rate-limiter 3.
rl-4	Specifies the F1 rate-limiter 4.
rl-5	Specifies the F1 rate-limiter 5.
layer-2	Specifies Layer 2 packet rate limits.
l2pt	Specifies Layer 2 Tunnel Protocol (L2TP) packets. The default rate is 4096 packets per second.
mcast-snooping	Specifies Layer 2 multicast-snooping packets. The default rate is 10000 packets per second.
port-security	Specifies port security packets. The default is disabled.
storm-control	Specifies broadcast, multicast, and unknown unicast storm-control packets. The default is disabled.
vpc-low	Specifies Layer 2 control packets over the virtual port channel (vPC) low queue. It synchronizes control-plane communication between vPC peer switches that are of a lower priority and protects the control plane when a vPC peer switch misbehaves or excessive traffic occurs between the two. The default rate is 4000 packets per second.
layer-3	Specifies Layer 3 packet rate limits.
control	Specifies Layer-3 control packets. The default rate is 10000 packets per second.
glean	Specifies Layer-3 glean packets. The default rate is 100 packets per second.
glean-fast	Specifies Layer 3 glean fast-path packets. The default rate is 100 packets per second.
mtu	Specifies Layer-3 maximum transmission unit (MTU) failure redirected packets. The default rate is 500 packets per second.
multicast	Specifies Layer-3 multicast packets per second.
ttl	Specifies Layer-3 failed time-to-live redirected packets. The default rate is 500 packets per second.
receive	Specifies packets redirected to the supervisor module. The default rate is 30000 packets per second.
portgroup-multiplier *multiplier*	Specifies the *multiplier* value. The range is from 0.10 to 3.00. The default value is 1.00. **Note** This applies to F2, F2e, and F3 cards.

Defaults

See the Syntax Description for the default rate limits.

Default rate limits for the F1 Series modules:

RL-1: 4500 packets per second

RL-2: 1000 packets per second

RL-3: 1000 packets per second

RL-4: 100 packets per second

RL-5: 1500 packets per second

Command Modes

Global configuration

Command History

Release	Modification
6.2(12)	Added the **portgroup-multiplier** keyword and the *multiplier* parameter.
6.2(2)	Added the **glean-fast** keyword.
5.1(1)	Added the **f1**, **rl**-1, **rl-2**, **rl-3**, **rl-4**, and **rl-5** keywords. Also, added the following keywords: **module**, **disable**, and **port**.
5.0(2)	Added the **l2pt** keyword.
4.1(2)	This command was introduced to replace the **platform rate-limit** command.

Usage Guidelines

Glean fast-path is enabled by default. If glean fast-path programming does not occur due to adjacency resource exhaustion, the system falls back to regular glean programming.

The **hardware rate-limiter layer-3 glean-fast** {*packets* | **disable**} [**module** *module* [**port** *start end*]] command sends packets to the supervisor from F2e, M1, or M2 Series modules.

The **hardware rate-limiter portgroup-multiplier** *multiplier* **module** *module* command applies the *multiplier* to the rate limit. For example, if you configured the ttl rate-limiter as 1000 pps and the multiplier value was 0.5, each ASIC instance would be programmed with 500 pps.

This command does not require a license.

Examples

This example shows how to configure a rate limit for control packets:

```
switch# configure terminal
switch(config)# hardware rate-limiter layer-3 control 20000
```

This example shows how to revert to the default rate limit for control packets:

```
switch# configure terminal
switch(config)# no hardware rate-limiter layer-3 control
```

```
This example shows how to configure the port group multiplier:

switch# configure terminal
switch(config)# hardware rate-limiter portgroup-multiplier 0.5 module 3
```

Related Commands

Command	Description
clear hardware rate-limiter	Clears rate-limit statistics.
show hardware rate-limiter	Displays rate-limit information.
show running-config	Displays the running configuration.

host (IPv4)

To specify a host or a subnet as a member of an IPv4-address object group, use the **host** command. To remove a group member from an IPv4-address object group, use the **no** form of this command.

[*sequence-number*] **host** *IPv4-address*

no {*sequence-number* | **host** *IPv4-address*}

[*sequence-number*] *IPv4-address network-wildcard*

no *IPv4-address network-wildcard*

[*sequence-number*] *IPv4-address*/*prefix-len*

no *IPv4-address*/*prefix-len*

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.
host *IPv4-address*	Specifies that the group member is a single IPv4 address. Enter *IPv4-address* in dotted-decimal format.
IPv4-address network-wildcard	IPv4 address and network wildcard. Enter *IPv4-address* and *network-wildcard* in dotted-decimal format. Use *network-wildcard* to specify which bits of *IPv4-address* are the network portion of the address, as follows: `switch(config-ipaddr-ogroup)# 10.23.176.0 0.0.0.255` A *network-wildcard* value of 0.0.0.0 indicates that the group member is a specific IPv4 address.
IPv4-address/*prefix-len*	IPv4 address and variable-length subnet mask. Enter *IPv4-address* in dotted-decimal format. Use *prefix-len* to specify how many bits of *IPv4-address* are the network portion of the address, as follows: `switch(config-ipaddr-ogroup)# 10.23.176.0/24` A *prefix-len* value of 32 indicates that the group member is a specific IP address.

Defaults

None

Command Modes

IPv4 address object group configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To specify a subnet as a group member, use either of the following forms of this command:

[*sequence-number*] *IPv4-address network-wildcard*

[*sequence-number*] *IPv4-address*/*prefix-len*

Regardless of the command form that you use to specify a subnet, the device shows the *IP-address*/*prefix-len* form of the group member when you use the **show object-group** command.

To specify a single IPv4 address as a group member, use any of the following forms of this command:

[*sequence-number*] **host** *IPv4-address*

[*sequence-number*] *IPv4-address* 0.0.0.0

[*sequence-number*] *IPv4-address*/32

Regardless of the command form that you use to specify a single IPv4 address, the device shows the **host** *IP-address* form of the group member when you use the **show object-group** command.

This command does not require a license.

Examples

This example shows how to configure an IPv4-address object group named ipv4-addr-group-13 with two group members that are specific IPv4 addresses and one group member that is the 10.23.176.0 subnet:

```
switch# config t
switch(config)# object-group ip address ipv4-addr-group-13
switch(config-ipaddr-ogroup)# host 10.121.57.102
switch(config-ipaddr-ogroup)# 10.121.57.234/32
switch(config-ipaddr-ogroup)# 10.23.176.0 0.0.0.255
switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13
        10 host 10.121.57.102
        20 host 10.121.57.234
        30 10.23.176.0/24
switch(config-ipaddr-ogroup)#
```

Related Commands

Command	Description
object-group ip address	Configures an IPv4 address group.
show object-group	Displays object groups.

host (IPv6)

To specify a host or a subnet as a member of an IPv6-address object group, use the **host** command. To remove a group member from an IPv6-address object group, use the **no** form of this command.

[*sequence-number*] **host** *IPv6-address*

no {*sequence-number* | **host** *IPv6-address*}

[*sequence-number*] *IPv6-address/network-prefix*

no *IPv6-address/network-prefix*

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.
host *IPv6-address*	Specifies that the group member is a single IPv6 address. Enter *IPv6-address* in colon-separated, hexadecimal format.
IPv6-address/network-prefix	IPv6 address and a variable-length subnet mask. Enter *IPv6-address* in colon-separated, hexadecimal format. Use *network-prefix* to specify how many bits of *IPv6-address* are the network portion of the address, as follows: `switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab7::/96` A *network-prefix* value of 128 indicates that the group member is a specific IPv6 address.

Defaults

None

Command Modes

IPv6 address object group configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To specify a subnet as a group member, use the following form of this command:

[*sequence-number*] *IPv6-address/network-prefix*

To specify a single IP address as a group member, use any of the following forms of this command:

[*sequence-number*] **host** *IPv6-address*

[*sequence-number*] *IPv6-address*/128

Regardless of the command form that you use to specify a single IPv6 address, the device shows the **host** *IPv6-address* form of the group member when you use the **show object-group** command.

This command does not require a license.

Examples

This example shows how to configure an IPv6-address object group named ipv6-addr-group-A7 with two group members that are specific IPv6 addresses and one group member that is the 2001:db8:0:3ab7:: subnet:

```
switch# config t
switch(config)# object-group ipv6 address ipv6-addr-group-A7
switch(config-ipv6addr-ogroup)# host 2001:db8:0:3ab0::1
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab0::2/128
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)# show object-group ipv6-addr-group-A7
        10 host 2001:db8:0:3ab0::1
        20 host 2001:db8:0:3ab0::2
        30 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)#
```

Related Commands

Command	Description
object-group ipv6 address	Configures an IPv6 address group.
show object-group	Displays object groups.