Show Commands

This chapter describes the Cisco NX-OS security **show** commands.

show aaa accounting

To display AAA accounting configuration information, use the **show aaa accounting** command.

show aaa accounting

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the configuration of the accounting log:

```
switch# show aaa accounting
        default: local
```

show aaa authentication

To display AAA authentication configuration information, use the **show aaa authentication** command.

show aaa authentication [**login error-enable** | **login chap** | **login mschap** | **login mschapv2** | **login ascii-authentication**]

Syntax Description

login error-enable	(Optional) Displays the configuration for login error messages.
login chap	(Optional) Displays the configuration for CHAP authentication.
login mschap	(Optional) Displays the configuration for MS-CHAP authentication.
login mschapv2	(Optional) Displays the configuration for MS-CHAP V2 authentication.
login ascii-authentication	(Optional) Displays the configuration for ASCII authentication for passwords on TACACS+ servers.

Defaults

Displays the console and login authentication methods configuration.

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
5.0(2)	Added the **chap** keyword
4.2(1)	Added the **mschapv2** keyword.
4.1(2)	Added the **ascii-authentication** keyword.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the configured authentication parameters:

```
switch# show aaa authentication
         default: local
         console: local
         dot1x: not configured
         eou: not configured
```

This example shows how to display the authentication-login error-enable configuration:

```
switch# show aaa authentication login error-enable
disabled
```

This example shows how to display the authentication-login CHAP configuration:

```
switch# show aaa authentication login chap
disabled
```

This example shows how to display the authentication-login MSCHAP configuration:

```
switch# show aaa authentication login mschap
disabled
```

This example shows how to display the authentication-login MSCHAP V2 configuration:

```
switch# show aaa authentication login mschapv2
enabled
```

This example shows how to display the status of the ASCII authentication for passwords feature:

```
switch(config)# show aaa authentication login ascii-authentication
disabled
```

Related Commands

Command	Description
aaa authentication login ascii-authentication	Enables ASCII authentication for passwords on a TACACS+ server.
aaa authentication login chap enable	Enables CHAP authentication.
aaa authentication login error-enable	Configures the AAA authentication failure message to display on the console.
aaa authentication login mschap enable	Enables MSCHAP authentication.
aaa authentication login mschapv2 enable	Enables MSCHAP V2 authentication.

show aaa authorization

To display AAA authorization configuration information, use the **show aaa authorization** command.

show aaa authorization [**all**]

Syntax Description

all	(Optional) Displays configured and default values.

Defaults

Displays the configured information.

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the configured authorization methods:

```
switch# show aaa authorization
        pki-ssh-cert: local
         pki-ssh-pubkey: local
AAA command authorization:
         default authorization for config-commands: none
         cts: group radius
```

This example shows how to display the configured authorization methods and defaults:

```
switch# show aaa authorization all
        pki-ssh-cert: local
         pki-ssh-pubkey: local
AAA command authorization:
         default authorization for config-commands: none
         default authorization for commands: local
         cts: group radius
```

Related Commands

Command	Description
aaa authorization	Configures the default AAA authorization method.
feature cts	Enables the Cisco TrustSec feature.
feature ldap	Enables the LDAP feature.
feature tacacs+	Enables the TACACS+ feature.

show aaa groups

To display AAA server group configuration, use the **show aaa groups** command.

show aaa groups

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display AAA group information:

```
switch# show aaa groups
radius
TacServer
```

show aaa user default-role

To display the AAA user default role configuration, use the **show aaa user default-role** command.

show aaa user default-role

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

User the **aaa user default-role** command to configure the AAA user default role.

This command does not require a license.

Examples

This example shows how to display the AAA user default role configuration:

```
switch# show aaa user default-role
enabled
```

Related Commands

Command	Description
aaa user default-role	Enables the AAA user default role.

show access-lists

To display all IPv4, IPv6, and MAC access control lists (ACLs) or a specific ACL, use the **show access-lists** command.

show access-lists [*access-list-name*] [**expanded | summary**]

Syntax Description

access-list-name	(Optional) Name of an ACL, which can be up to 64 alphanumeric, case-sensitive characters.
expanded	(Optional) Specifies that the contents of object groups appear rather than the names of object groups only.
summary	(Optional) Specifies that the command displays information about the ACL. For more information, see the "Usage Guidelines" section.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	Command output is sorted alphabetically by the ACL names. Support was added for the **fragments** command.
4.1(2)	Support for IPv6 ACLs was added.
4.0(1)	This command was introduced.

Usage Guidelines

The device shows all ACLs unless you use the *access-list-name* argument to specify an ACL.

If you do not specify an ACL name, the device lists ACLs alphabetically by the ACL names.

The **expanded** keyword allows you to display the details of object groups used in an ACL rather than only the name of the object groups. For more information about object groups, see the **object-group ip address**, **object-group ipv6 address**, and **object-group ip port** commands.

The **summary** keyword allows you to display information about the ACL rather than the ACL configuration. The information displayed includes the following:

- Whether per-entry statistics are configured for the ACL.
- Whether the **fragments** command is configured for an IP ACL.

- The number of rules in the ACL configuration. This number does not reflect how many entries that the ACL contains when the device applies it to an interface. If a rule in the ACL uses an object group, the number of entries in the ACL when it is applied may be much greater than the number of rules.
- The interfaces that the ACL is applied to.
- The interfaces that the ACL is active on.

The **show access-lists** command displays statistics for each entry in an ACL if the following conditions are both true:

- The ACL configuration contains the **statistics per-entry** command.
- The ACL is applied to an interface that is administratively up.

If an IP ACL includes the **fragments** command, it appears before the explicit permit and deny rules, but the device applies the **fragments** command to noninitial fragments only if they do not match all other explicit rules in the ACL.

This command does not require a license.

Examples

This example shows how to use the **show access-lists** command without specifying an ACL name on a device that has one IP ACL and one MAC ACL configured:

```
switch# show access-lists

IP access list ip-v4-filter
        10 permit ip any any
MAC access list mac-filter
        10 permit 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff ip
```

This example shows how to use the **show access-lists** command to display an IPv4 ACL named ipv4-RandD-outbound-web, including per-entry statistics for the entries except for the MainLab object group:

```
switch# show access-lists ipv4-RandD-outbound-web

IP access list ipv4-RandD-outbound-web
        statistics per-entry
        1000 permit ahp any any [match=732]
        1005 permit tcp addrgroup MainLab any eq telnet
        1010 permit tcp any any eq www [match=820421]
```

This example shows how to use the **show access-lists** command to display an IPv4 ACL named ipv4-RandD-outbound-web. The **expanded** keyword causes the contents of the object group from the previous example to appear, including the per-entry statistics:

```
switch# show access-lists ipv4-RandD-outbound-web expanded

IP access list ipv4-RandD-outbound-web
        statistics per-entry
        1000 permit ahp any any [match=732]
        1005 permit tcp 10.52.34.4/32 any eq telnet [match=5032]
        1005 permit tcp 10.52.34.27/32 any eq telnet [match=433]
        1010 permit tcp any any eq www [match=820421]
```

This example shows how to use the **show access-lists** command with the **summary** keyword to display information about an IPv4 ACL named ipv4-RandD-outbound-web, such as which interfaces the ACL is applied to and active on:

```
switch# show access-lists ipv4-RandD-outbound-web summary
IPV4 ACL ipv4-RandD-outbound-web
```

```
Statistics enabled
Total ACEs Configured: 4
Configured on interfaces:
        Ethernet2/4 - ingress (Router ACL)
Active on interfaces:
        Ethernet2/4 - ingress (Router ACL)
```

Related Commands

Command	Description
fragments	Configures how an IP ACL processes noninitial fragments.
ip access-list	Configures an IPv4 ACL.
mac access-list	Configures a MAC ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.

show accounting log

To display the accounting log contents, use the **show accounting log** command.

show accounting log [*size* | **last-index** | **start-seqnum** *number* | **start-time** *year month day HH*:*MM*:*SS*]

Syntax Description

size	(Optional) Size of the log to display in bytes. The range is from 0 to 250000.
last-index	(Optional) Displays the last index number in the log.
start-seqnum *number*	(Optional) Specifies a sequence number in the log at which to begin display output. The range is from 1 to 1000000.
start-time *year month day HH*:*MM*:*SS*	(Optional) Specifies a start time in the log at which to begin displaying output. The *year* argument is in *yyyy* format. The *month* is the three-letter English abbreviation. The *day* argument range is from 1 to 31. The *HH*:*MM*:*SS* argument is in the standard 24-hour format.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	Added the **last-index** and **start-seqnum** keyword options.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the entire accounting log:

```
switch# show accounting log

Sat Feb 16 10:44:24 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 10:44:25 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
Sat Feb 16 10:45:20 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log
file start-time 2008 Feb 16 10:44:11
Sat Feb 16 10:45:23 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting
log start-time 2008 Feb 16 10:08:57
Sat Feb 16 10:45:24 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 10:45:25 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
Sat Feb 16 10:46:20 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log
file start-time 2008 Feb 16 10:45:11
Sat Feb 16 10:46:22 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting
```

This example shows how to display 400 bytes of the accounting log:

```
switch# show accounting log 400

Sat Feb 16 21:15:24 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting log
start-time 2008 Feb 16 18:31:21
Sat Feb 16 21:15:25 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 21:15:26 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
```

This example shows how to display the accounting log starting at 16:00:00 on February 16, 2008:

```
switch(config)# show accounting log start-time 2008 Feb 16 16:00:00

Sat Feb 16 16:00:18 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log file
start-time 2008 Feb 16 15:59:16
Sat Feb 16 16:00:26 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting log
start-time 2008 Feb 16 12:05:16
Sat Feb 16 16:00:27 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 16:00:28 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
Sat Feb 16 16:01:18 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log file
start-time 2008 Feb 16 16:00:16
Sat Feb 16 16:01:26 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting log
start-time 2008 Feb 16 12:05:16
Sat Feb 16 16:01:27 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 16:01:29 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
Sat Feb 16 16:02:18 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log file
start-time 2008 Feb 16 16:01:16
Sat Feb 16 16:02:26 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting log
start-time 2008 Feb 16 12:05:16
Sat Feb 16 16:02:28 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
```

This example shows how to display the last index number:

```
switch# show accounting log last-index
accounting-log last-index : 1814
```

Related Commands

Command	Description
clear accounting log	Clears the accounting log.

show arp access-lists

To display all ARP access control lists (ACLs) or a specific ARP ACL, use the **show arp access-lists** command.

show arp access-lists [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of an ARP ACL, which can be up to 64 alphanumeric, case-sensitive characters.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The device shows all ARP ACLs, unless you use the *access-list-name* argument to specify an ACL.

This command does not require a license.

Examples

This example shows how to use the **show arp access-lists** command to display all ARP ACLs on a device that has two ARP ACLs:

```
switch# show arp access-lists

ARP access list arp-permit-all
10 permit ip any mac any
ARP access list arp-lab-subnet
10 permit request ip 10.32.143.0 255.255.255.0 mac any
```

This example shows how to use the **show arp access-lists** command to display an ARP ACL named arp-permit-all:

```
switch# show arp access-lists arp-permit-all

ARP access list arp-permit-all
10 permit ip any mac any
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL.
ip arp inspection filter	Applies an ARP ACL to a VLAN.

show class-map type control-plane

To display control plane class map information, use the **show class-map type control-plane** command.

show class-map type control-plane [*class-map-name*]

Syntax Description

class-map-name	(Optional) Name of the control plane class map.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to display control plane class map information:

```
switch# show class-map type control-plane

    class-map type control-plane match-any copp-system-class-critical
      match access-grp name copp-system-acl-arp
      match access-grp name copp-system-acl-msdp

    class-map type control-plane match-any copp-system-class-important
      match access-grp name copp-system-acl-gre
      match access-grp name copp-system-acl-tacas

    class-map type control-plane match-any copp-system-class-normal
      match access-grp name copp-system-acl-icmp
      match redirect dhcp-snoop
      match redirect arp-inspect
      match exception ip option
      match exception ip icmp redirect
      match exception ip icmp unreachable
```

show cli syntax roles network-admin

To display the syntax of the commands that the network-admin role can use but the vdc-admin role cannot, use the **show cli syntax roles network-admin** command.

show cli syntax roles network-admin

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the syntax of the commands that the network-admin role can use but the vdc-admin role cannot:

```
switch# show cli syntax roles network-admin
MODE exec
(0) show debug license
(1) show debug bootvar
(2) show debug cmpproxy
(3) show debug exceptionlog
(4) show debug device_test
(5) show debug diagmgr
(6) show debug diagclient
(7) show debug ntp
(8) show debug port_lb
(9) show debug copp
(10) show debug copp bypass
(11) show license usage vdc-all [ { detail | <license-feature> } ]
(12) show system internal license event-history
(13) show system internal license mem-stats [ detail ]
(14) show system internal loader configuration
(15) show system internal bootvar log
(16) show system internal cmpproxy install-logs
(17) show system internal cmpproxy [ event-history ] errors
(18) show system internal cmpproxy [ event-history ] msgs
(19) show system internal cmpproxy mem-stats [ detail ]
```

```
(20) show system internal epld logging
(21) show system internal access-list status [ ]
(22) show system internal copp ppf-database { policy { subscriptions | sessions
| instances | all } }
(23) show system internal copp [ event-history ] errors
(24) show system internal copp [ event-history ] logs
(25) show system internal copp [ event-history ] msgs
(26) show system internal copp mem-stats [ detail ]
(27)  show system internal copp info
(28) show system reset-reason
(29) show system reset-reason module <module>
(30) show system reset-reason <s0> <santa-cruz-range>
(31) show system redundancy status
(32) show system redundancy ha status
(33) show logging level { license | licmgr }
(34) show logging level bootvar
(35) show logging level cmpproxy
(36) show logging level diagnostic device_test
(37) show logging level diagnostic diagmgr
(38) show logging level diagnostic diagclient
(39) show logging level ntp
(40) show logging level copp
(41) show running-config res_mgr
(42) show running-config vdc [ all ]
(43) show running-config diagnostic [ all ]
(44) show running-config cmp
(45) show running-config ntp [ all ]
(46) show running-config vdc-all [ all ]
(47) show running-config copp [ all ]
(48) show startup-config vdc [ all ]
(49) show startup-config diagnostic [ all ]
(50) show startup-config ntp [ all ]
(51) show startup-config vdc-all
(52) show startup-config copp [ all ]
(53) show tech-support gold
(54) show tech-support cmp
(55) show tech-support dcbx
(56) show tech-support ntp
(57) show tech-support forwarding l2 multicast vdc-all
(58) show tech-support forwarding l3 unicast vdc-all [ module <module> ]
--More--
```

Related Commands

Command	Description
show cli syntax roles network-operator	Displays the syntax of the commands that the network-operator role can use but the vdc-operator role cannot.

show copp diff profile

To display the difference between the previous and latest Control Plane Policing (CoPP) best practice policies or between the currently applied default CoPP best practice policy and the latest CoPP best practice policy, use the **show copp diff profile** command.

show copp diff profile {**lenient** | **moderate** | **strict**} [**prior-ver**] **profile** {**lenient** | **moderate** | **strict**}

Syntax Description

lenient	Displays the lenient profile.
moderate	Displays the moderate profile.
strict	Displays the strict profile.
profile	Specifies the profile.
prior-ver	Specifies the previous profile.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

When you do not include the **prior-ver** option, this command displays the difference between two currently applied default CoPP best practice policies (such as the currently applied strict and currently applied moderate policies).

When you include the **prior-ver** option, this command displays the difference between a currently applied default CoPP best practice policy and a previously applied default CoPP best practice policy (such as the currently applied strict and the previously applied lenient policies).

This command does not require a license.

Examples

This example shows how to display the difference between the currently applied default CoPP best practice policy and the latest CoPP best practice policy:

```
switch# show copp diff profile moderate applied latest
```

Related Commands

Command	Description
show copp profile	Displays the details of the CoPP best practice policy, along with the classes and policer values.

show copp profile

To display the details of the Control Plane Policing (CoPP) best practice policy, along with the classes and policer values, use the **show copp profile** command.

show copp profile {**lenient** | **moderate** | **strict**}

Syntax Description

lenient	Displays the lenient profile.
moderate	Displays the moderate profile.
strict	Displays the strict profile.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

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 display the details of the CoPP best practice policy, along with the classes and policer values:

```
switch# show copp profile moderate

ip access-list copp-system-p-acl-bgp
  permit tcp any gt 1024 any eq bgp
  permit tcp any eq bgp any gt 1024
ipv6 access-list copp-system-p-acl-bgp6
  permit tcp any gt 1024 any eq bgp
  permit tcp any eq bgp any gt 1024
ip access-list copp-system-p-acl-cts
  permit tcp any any eq 64999
  permit tcp any eq 64999 any
ip access-list copp-system-p-acl-dhcp
  permit udp any eq bootpc any
  permit udp any neq bootps any eq bootps
ip access-list copp-system-p-acl-dhcp-relay-response
  permit udp any eq bootps any
```

```
  permit udp any any eq bootpc
ip access-list copp-system-p-acl-eigrp
  permit eigrp any any
ip access-list copp-system-p-acl-ftp
  permit tcp any any eq ftp-data
  permit tcp any any eq ftp
  permit tcp any eq ftp-data any
  permit tcp any eq ftp any
ip access-list copp-system-p-acl-glbp
  permit udp any eq 3222 224.0.0.0/24 eq 3222
--More--
```

Related Commands

Command	Description
copp profile	
copp clone profile	
show copp diff profile	Displays the difference between the currently applied default CoPP best practice policy and the latest or previous CoPP best practice policy.
show copp status	Displays the CoPP status, including the last configuration operation and its status.
show running-config copp	Displays the CoPP configuration in the running configuration.

show cli syntax roles network-operator

To display the syntax of the commands that the network-operator role can use but the vdc-operator role cannot, use the **show cli syntax roles network-operator** command.

show cli syntax roles network-operator

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the syntax of the commands that the network-operator role can use but the vdc-operator role cannot:

```
switch# show cli syntax roles network-operator
MODE exec
(0) show debug license
(1) show debug cmpproxy
(2) show debug exceptionlog
(3) show debug device_test
(4) show debug diagmgr
(5) show debug diagclient
(6) show debug ntp
(7) show debug port_lb
(8) show debug copp
(9) show license usage vdc-all [ { detail | <license-feature> } ]
(10) show system internal license event-history
(11) show system internal license mem-stats [ detail ]
(12) show system internal loader configuration
(13) show system internal bootvar log
(14) show system internal cmpproxy install-logs
(15) show system internal cmpproxy [ event-history ] errors
(16) show system internal cmpproxy [ event-history ] msgs
(17) show system internal cmpproxy mem-stats [ detail ]
(18) show system internal epld logging
(19) show system internal access-list status [ ]
```

```
(20) show system internal copp ppf-database { policy { subscriptions | sessions
| instances | all } }
(21) show system internal copp [ event-history ] errors
--More--
```

Related Commands

Command	Description
show cli syntax roles network-admin	Displays the syntax of the commands that the network-admin role can use but the vdc-admin role cannot.

show copp status

To display the control plane policing (CoPP) configuration status, use the **show copp status** command.

show copp status

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
4.0(2)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to display the CoPP configuration status information:

```
switch# show copp status
Last Config Operation: service-policy input copp-system-policy
Last Config Operation Timestamp: 21:57:58 UTC Jun  4 2008
Last Config Operation Status: Success
Policy-map attached to the control-plane: new-copp-policy
```

show crypto ca certificates

To display configured trustpoint certificates, use the **show crypto ca certificates** command.

show crypto ca certificates *trustpoint-label*

Syntax Description

trustpoint-label	Name of the trustpoint. The name is case sensitive.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use this command to display the fields in the identity certificate, if present, followed by the fields in the CA certificate (or each CA certificate if it is a chain, starting from the lowest to the self-signed root certificate), or the trustpoint. If the trustpoint name is not specified, all trustpoint certificate details are displayed.

This command does not require a license.

Examples

This example shows how to display configured trustpoint certificates:

```
switch# show crypto ca certificates
Trustpoint: admin-ca
certificate:
subject= /CN=switch160
issuer= /C=US/O=cisco/CN=Aparna CA2
serial=6CDB2D9E000100000006
notBefore=Jun  9 10:51:45 2005 GMT
notAfter=May  3 23:10:36 2006 GMT
MD5 Fingerprint=0A:22:DC:A3:07:2A:9F:9A:C2:2C:BA:96:EC:D8:0A:95
purposes: sslserver sslclient ike

CA certificate 0:
subject= /C=US/O=cisco/CN=Aparna CA2
issuer= /emailAddress=amandke@cisco.com/C=IN/ST=Maharashtra/L=Pune/O=cisco/OU=ne
tstorage/CN=Aparna CA1
serial=14A3A877000000000005
```

```
notBefore=May  5 18:43:36 2005 GMT
notAfter=May  3 23:10:36 2006 GMT
MD5 Fingerprint=32:50:26:9B:16:B1:40:A5:D0:09:53:0A:98:6C:14:CC
purposes: sslserver sslclient ike

CA certificate 1:
subject= /emailAddress=amandke@cisco.com/C=IN/ST=Maharashtra/L=Pune/O=cisco/OU=n
etstorage/CN=Aparna CA1
issuer= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/OU
=netstorage/CN=Aparna CA
serial=611B09A1000000000002
notBefore=May  3 23:00:36 2005 GMT
notAfter=May  3 23:10:36 2006 GMT
MD5 Fingerprint=65:CE:DA:75:0A:AD:B2:ED:69:93:EF:5B:58:D4:E7:AD
purposes: sslserver sslclient ike

CA certificate 2:
subject= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/O
U=netstorage/CN=Aparna CA
issuer= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/OU
=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May  3 22:46:37 2005 GMT
notAfter=May  3 22:55:17 2007 GMT
MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
purposes: sslserver sslclient ike
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the certificate of the CA.
show ca trustpoints	Displays trustpoint configurations.

show crypto ca certstore

To display the cert-store configuration, use the **show crypto ca certstore** command.

show crypto ca certstore

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

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 display the cert-store configuration:

```
switch# show crypto ca certstore
Certstore lookup: REMOTE
```

Related Commands

Command	Description
crypto ca lookup	Specifies the cert-store to be used for certificate authentication.
show crypto ca remote-certstore	Displays the remote cert-store configuration.

show crypto ca crl

To display configured certificate revocation lists (CRLs), use the **show crypto ca crl** command.

show crypto ca crl *trustpoint-label*

Syntax Description

trustpoint-label	Name of the trustpoint. The label is case sensitive.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use this command to list the serial numbers of the revoked certificates in the CRL of the specified trustpoint.

This command does not require a license.

Examples

This example shows how to display a configured CRL:

```
switch# show crypto ca crl admin-ca
Trustpoint: admin-ca
CRL:
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: /emailAddress=rviyyoka@cisco.com/C=IN/ST=Kar/L=Bangalore/O=Cisco
 Systems/OU=1/CN=cisco-blr
        Last Update: Sep 22 07:05:23 2005 GMT
        Next Update: Sep 29 19:25:23 2005 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
            keyid:CF:72:E1:FE:14:60:14:6E:B0:FA:8D:87:18:6B:E8:5F:70:69:05:3F

            1.3.6.1.4.1.311.21.1:
                ...
Revoked Certificates:
    Serial Number: 1E0AE838000000000002
        Revocation Date: Mar 15 09:12:36 2005 GMT
```

```
Serial Number: 1E0AE9AB000000000003
    Revocation Date: Mar 15 09:12:45 2005 GMT
Serial Number: 1E721E50000000000004
    Revocation Date: Apr  5 11:04:20 2005 GMT
Serial Number: 3D26E445000000000005
    Revocation Date: Apr  5 11:04:16 2005 GMT
Serial Number: 3D28F8DF000000000006
    Revocation Date: Apr  5 11:04:12 2005 GMT
Serial Number: 3D2C6EF3000000000007
    Revocation Date: Apr  5 11:04:09 2005 GMT
Serial Number: 3D4D7DDC000000000008
    Revocation Date: Apr  5 11:04:05 2005 GMT
Serial Number: 5BF1FE87000000000009
    Revocation Date: Apr  5 11:04:01 2005 GMT
Serial Number: 5BF22FB300000000000A
    Revocation Date: Apr  5 11:03:45 2005 GMT
Serial Number: 5BFA4A4900000000000B
    Revocation Date: Apr  5 11:03:42 2005 GMT
Serial Number: 5C0BC225000000000000C
    Revocation Date: Apr  5 11:03:39 2005 GMT
Serial Number: 5C0DA95E000000000000D
    Revocation Date: Apr  5 11:03:35 2005 GMT
Serial Number: 5C137769000000000000E
    Revocation Date: Apr  5 11:03:31 2005 GMT
Serial Number: 4864FD5A000000000000F
    Revocation Date: Apr  5 11:03:28 2005 GMT
Serial Number: 48642E2E000000000010
    Revocation Date: Apr  5 11:03:24 2005 GMT
Serial Number: 486D4230000000000000011
    Revocation Date: Apr  5 11:03:20 2005 GMT
Serial Number: 7FCB75B9000000000012
    Revocation Date: Apr  5 10:39:12 2005 GMT
Serial Number: 1A7519000000000013
    Revocation Date: Apr  5 10:38:52 2005 GMT
Serial Number: 20F1B0000000000014
    Revocation Date: Apr  5 10:38:38 2005 GMT
Serial Number: 436E43A9000000000023
    Revocation Date: Sep  9 09:01:23 2005 GMT
    CRL entry extensions:
        X509v3 CRL Reason Code:
        Cessation Of Operation
Serial Number: 152D3C5E000000000047
    Revocation Date: Sep 22 07:12:41 2005 GMT
Serial Number: 1533AD7F000000000048
    Revocation Date: Sep 22 07:13:11 2005 GMT
Serial Number: 1F9EB8EA000000000006D
    Revocation Date: Jul 19 09:58:45 2005 GMT
    CRL entry extensions:
        X509v3 CRL Reason Code:
        Cessation Of Operation
Serial Number: 1FCA9DC600000000006E
    Revocation Date: Jul 19 10:17:34 2005 GMT
    CRL entry extensions:
        X509v3 CRL Reason Code:
        Cessation Of Operation
Serial Number: 2F1B5E2E000000000072
    Revocation Date: Jul 22 09:41:21 2005 GMT
    CRL entry extensions:
        X509v3 CRL Reason Code:
        Cessation Of Operation
```

```
Signature Algorithm: sha1WithRSAEncryption
    4e:3b:4e:7a:55:6b:f2:ec:72:29:70:16:2a:fd:d9:9a:9b:12:
    f9:cd:dd:20:cc:e0:89:30:3b:4f:00:4b:88:03:2d:80:4e:22:
    9f:46:a5:41:25:f4:a5:26:b7:b6:db:27:a9:64:67:b9:c0:88:
    30:37:cf:74:57:7a:45:5f:5e:d0
```

Related Commands

Command	Description
crypto ca crl request	Configures a CRL or overwrites the existing one for the trustpoint CA.

show crypto ca remote-certstore

To display the remote cert-store configuration, use the **show crypto ca remote-certstore** command.

show crypto ca remote-certstore

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

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 display the remote cert-store configuration:

```
switch# show crypto ca remote-certstore
Remote Certstore: NONE
```

Related Commands

Command	Description
crypto ca lookup	Specifies the cert-store to be used for certificate authentication.
show crypto ca certstore	Displays the configured cert-store.

show crypto ca trustpoints

To display trustpoint configurations, use the **show crypto ca trustpoints** command.

show crypto ca trustpoints

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

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 display configured trustpoints:

```
switch# show crypto ca trustpoints
trustpoint: CAname; key:
revokation methods:  crl
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the certificate of the CA.
crypto ca trustpoint	Declares the trustpoint certificate authority that the device should trust.
show crypto ca certificates	Displays configured trustpoint certificates.

show crypto certificatemap

To display the certificate mapping filters, use the **show crypto certificatemap** command.

show crypto certificatemap

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

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 display the certificate mapping filters:

```
switch# show crypto certificatemap
```

Related Commands

Command	Description
crypto certificatemap mapname	Creates a filter map.
filter	Configures one or more certificate mapping filters within the filter map.

show crypto key mypubkey rsa

To display the RSA public key configurations, use the **show crypto key mypubkey rsa** command.

show crypto key mypubkey rsa

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

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 display RSA public key configurations:

```
switch# show crypto key mypubkey rsa
key label: myrsa
key size: 512
exportable: yes
```

Related Commands

Command	Description
crypto ca enroll	Requests certificates for the switch's RSA key pair.
crypto key generate rsa	Generate an RSA key pair.
rsakeypair	Configure trustpoint RSA key pair details

show crypto ssh-auth-map

To display the mapping filters configured for SSH authentication, use the **show crypto ssh-auth-map** command.

show crypto ssh-auth-map

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

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 display the mapping filters configured for SSH authentication:

```
switch# show crypto ssh-auth-map
Default Map     : filtermap1
```

Related Commands

Command	Description
crypto certificatemap mapname	Creates a filter map.
crypto cert ssh-authorize	Configures a certificate mapping filter for the SSH protocol.
filter	Configures one or more certificate mapping filters within the filter map.

show cts

To display the global Cisco TrustSec configuration, use the **show cts** command.

show cts

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

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 cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec global configuration:

```
switch# show cts
CTS Global Configuration
============================
  CTS support           : enabled
  CTS device identity   : Device1
  CTS caching support   : disabled

  Number of CTS interfaces in
    DOT1X mode : 0
    Manual mode : 0
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts credentials

To display the Cisco TrustSec device credentials configuration, use the **show cts credentials** command.

show cts credentials

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

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 cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec credentials configuration:

```
switch# show cts credentials
CTS password is defined in keystore, device-id = Device1
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts environment-data

To display the global Cisco TrustSec environment data, use the **show cts environment-data** command.

show cts environment-data

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

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 cts** command.

The Cisco NX-OS device downloads the Cisco TrustSec environment data from the ACS after you have configured the Cisco TrustSec credentials for the device and configured authentication, authorization, and accounting (AAA).

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec environment data:

```
switch# show cts environment-data
CTS Environment Data
============================
  Current State           : CTS_ENV_DNLD_ST_ENV_DOWNLOAD_DONE
  Last Status             : CTS_ENV_SUCCESS
  Local Device SGT        : 0x0002
  Transport Type          : CTS_ENV_TRANSPORT_DIRECT
  Data loaded from cache  : FALSE
  Env Data Lifetime       : 300 seconds after last update
  Last Update Time        : Sat Jan  5 16:29:52 2008

  Server List             : ACSServerList1
     AID:74656d706f72617279 IP:10.64.65.95 Port:1812
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts interface

To display the Cisco TrustSec information for interfaces, use the **show cts interface** command.

show cts interface {**all** | **ethernet** *slot*/*port*}

Syntax Description

all	Displays Cisco TrustSec information for all interfaces.
interface *slot*/*port*	Displays Cisco TrustSec information for the specific interface.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

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 cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec configuration for all interfaces:

```
switch# show cts interface all
CTS Information for Interface Ethernet2/24:
    CTS is enabled, mode:   CTS_MODE_DOT1X
    IFC state:              CTS_IFC_ST_CTS_OPEN_STATE
    Authentication Status:  CTS_AUTHC_SUCCESS
      Peer Identity:        india1
      Peer is:              CTS Capable
      802.1X role:          CTS_ROLE_AUTH
      Last Re-Authentication:
    Authorization Status:   CTS_AUTHZ_SUCCESS
      PEER SGT:             2
      Peer SGT assignment:  Trusted
      Global policy fallback access list:
    SAP Status:             CTS_SAP_SUCCESS
      Configured pairwise ciphers: GCM_ENCRYPT
      Replay protection: Enabled
      Replay protection mode: Strict
      Selected cipher: GCM_ENCRYPT
      Current receive SPI: sci:1b54c1fbff0000 an:0
      Current transmit SPI: sci:1b54c1fc000000 an:0

CTS Information for Interface Ethernet2/25:
    CTS is enabled, mode:   CTS_MODE_DOT1X
    IFC state:              CTS_IFC_ST_CTS_OPEN_STATE
    Authentication Status:  CTS_AUTHC_SUCCESS
      Peer Identity:        india1
      Peer is:              CTS Capable
      802.1X role:          CTS_ROLE_SUP
      Last Re-Authentication:
    Authorization Status:   CTS_AUTHZ_SUCCESS
      PEER SGT:             2
      Peer SGT assignment:  Trusted
      Global policy fallback access list:
    SAP Status:             CTS_SAP_SUCCESS
      Configured pairwise ciphers: GCM_ENCRYPT
      Replay protection: Enabled
      Replay protection mode: Strict
      Selected cipher: GCM_ENCRYPT
      Current receive SPI: sci:1b54c1fc000000 an:0
      Current transmit SPI: sci:1b54c1fbff0000 an:0
```

This example shows how to display the Cisco TrustSec configuration for a specific interface:

```
switch# show cts interface ethernet 2/24
CTS Information for Interface Ethernet2/24:
    CTS is enabled, mode:   CTS_MODE_DOT1X
    IFC state:              CTS_IFC_ST_CTS_OPEN_STATE
    Authentication Status:  CTS_AUTHC_SUCCESS
      Peer Identity:        india1
      Peer is:              CTS Capable
      802.1X role:          CTS_ROLE_AUTH
      Last Re-Authentication:
    Authorization Status:   CTS_AUTHZ_SUCCESS
      PEER SGT:             2
      Peer SGT assignment:  Trusted
      Global policy fallback access list:
    SAP Status:             CTS_SAP_SUCCESS
      Configured pairwise ciphers: GCM_ENCRYPT
      Replay protection: Enabled
      Replay protection mode: Strict
      Selected cipher: GCM_ENCRYPT
      Current receive SPI: sci:1b54c1fbff0000 an:0
      Current transmit SPI: sci:1b54c1fc000000 an:0
```

Table 1 provides information about the values displayed in the **show cts interface** command output.

Table 1 show cts interface Command Output Values Descriptions

Value	Description
Authentication Status Field	
CTS_AUTHC_INIT	The authentication engine is in initial state.
CTS_AUTHC_SUCCESS	The authentication is successful.
CTS_AUTHC_NO_RESPONSE	The Cisco Access Control Server (ACS) is cannot be reached. No response was received from the Cisco ACS.
CTS_AUTHC_UNAUTHORIZED	The authentication is in progress.
CTS_AUTHC_SKIPPED_CONFIG	The Cisco TrustSec configuration indicates that the device should skip the authentication process.
CTS_AUTHC_REJECT	The Cisco ACS rejected the authentication request.
Authorization Status Field	
CTS_AUTHZ_INIT	The authorization engine is in the initial state.
CTS_AUTHZ_SUCCESS	The authorization was successful.
CTS_AUTHZ_REJECT	The ACS rejected the authorization request.
CTS_AUTHZ_SKIPPED_CONFIG	The Cisco TrustSec configuration indicates that the device should skip the authorization process.
CTS_AUTHZ_POL_ACQ_FAILURE	The authorization policy acquisition failed.
CTS_AUTHZ_HW_FAILURE	The hardware authorization programming failed.
CTS_AUTHZ_RBACL_FAILURE	The security group access control groups (SGACLs) failed to download and install.
CTS_AUTHZ_INCOMPLETE	The authorization is in progress

Table 1 show cts interface Command Output Values Descriptions (continued)

Value	Description
SAP Status Field	
CTS_SAP_INIT	The Security Association Protocol (SAP) negotiation is in the initial state.
CTS_SAP_SUCCESS	The SAP negotiation succeeded.
CTS_SAP_FAILURE	The SAP negotiation failed.
CTS_SAP_SKIPPED_CONFIG	The Cisco TrustSec configuration indicates that the device should skip the SAP negotiation.
CTS_SAP_REKEY	The SAP rekey is in progress.
CTS_SAP_INCOMPLETE	The SAP negotiation in progress.

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts pacs

To display the Cisco TrustSec protect access credentials (PACs) provisioned by EAP-FAST, use the **show cts pacs** command.

show cts pacs

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

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 cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec global configuration:

```
switch# show cts pacs
PAC Info :
==============================
  PAC Type            : unknown
  AID                 : 74656d706f72617279
  I-ID                : india1
  AID Info            : ACS Info
  Credential Lifetime : Thu Apr  3 00:36:04 2008

  PAC Opaque          : 000200830002000400097465 6d706f726172790006007000010 1001d
6321a2a55fa81e05cd705c714bea116907503aab89490b07fcbb2bd455b8d873f21b5b6b403eb1d8
125897d93b94669745cfe1abb0baf01a00b77aacf0bda9fbaf7dcd54528b782d8206a7751afdde42
1ff4a3db6a349c652fea81809fba4f30b1fffb7bfffaf9a6608
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts role-based access-list

To display the global Cisco TrustSec security group access control list (SGACL) configuration, use the **show cts role-based access-list** command.

show cts role-based access-list [*list-name*]

Syntax Description

list-name	(Optional) SGACL name.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
4.2(1)	Added list name argument.
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec SGACL configuration:

```
switch# show cts role-based access-list
rbacl:test-3
        deny ip
rbacl:test-1
        deny ip
        deny icmp
        deny tcp src eq 1000 dest eq 2000
        deny udp src range 1000 2000
rbacl:test-2
        permit icmp
        permit igmp
        permit tcp src lt 2000
        permit udp dest gt 4000
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts role-based counters

To display the configuration status of role-based access control list (RBACL) statistics and list the statistics for all RBACL policies, use the **show cts role-based counters** command.

show cts role-based counters [**sgt** {*sgt-value* | **any** | **unknown**}] [**dgt** {*dgt-value* | **any** | **unknown**}]

Syntax Description

sgt	Specifies the source security group tag (SGT).
sgt-value	Source SGT value. The range is from 0 to 65519.
any	Specifies any SGT or DGT.
unknown	Specifies an unknown SGT or DGT.
dgt	Specifies the destination security group tag (DGT).
dgt-value	Destination SGT value. The range is from 0 to 65519.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the configuration status of RBACL statistics and the total number of packets that match RBACL policies for a specific SGT and DGT:

```
switch# show cts role-based counters sgt 10 dgt 20

RBACL policy counters enabled
sgt: 10 dgt: 20 [180]
rbacl test1:
deny tcp src eq 1111 dest eq 2222 [75]
deny tcp src eq 2222 dest eq 3333 [25]
rbacl test2:
deny udp src eq 1111 dest eq 2222 [30]
deny udp src eq 2222 dest eq 3333 [50]
```

Related Commands

Command	Description
clear cts role-based counters	Clears the RBACL statistics so that all counters are reset to 0.
cts role-based counters enable	Enables the RBACL statistics.

show cts role-based enable

To display the Cisco TrustSec security group access control list (SGACL) enable status for VLANs and Virtual Routing and Forwarding instances (VRFs), use the **show cts role-based enable** command.

show cts role-based enable

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

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 cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec SGACL enforcement status:

```
switch# show cts role-based enable

vlan:1
vrf:1
vrf:3
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts role-based policy

To display the global Cisco TrustSec security group access control list (SGACL) policies, use the **show cts role-based policy** command.

show cts role-based policy

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

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 cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec SGACL policies:

```
switch# show cts role-based policy

sgt:unknown
dgt:unknown     rbacl:test-2
        permit icmp
        permit igmp
        permit tcp src lt 2000
        permit udp dest gt 4000

sgt:1000
dgt:2000        rbacl:test-1
        deny ip
        deny icmp
        deny tcp src eq 1000 dest eq 2000
        deny udp src range 1000 2000

sgt:any
dgt:any rbacl:test-3
        deny ip
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts role-based sgt-map

To display the global Cisco TrustSec Security Group Tag (SGT) mapping configuration, use the **show cts role-based sgt-map** command.

show cts role-based sgt-map

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

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 cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec SGT mapping configuration:

```
switch# show cts role-based sgt-map
IP ADDRESS              SGT             VRF/VLAN        SGT CONFIGURATION
5.5.5.5                 5               vlan:10         CLI Configured
5.5.5.6                 6               vlan:10         CLI Configured
5.5.5.7                 7               vlan:10         CLI Configured
5.5.5.8                 8               vlan:10         CLI Configured
10.10.10.10             10              vrf:3           CLI Configured
10.10.10.20             20              vrf:3           CLI Configured
10.10.10.30             30              vrf:3           CLI Configured
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts sxp

To display the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (SXP) configuration, use the **show cts sxp** command.

show cts sxp

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

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 cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec SXP configuration:

```
switch# show cts sxp
CTS SXP Configuration:
SXP enabled
SXP retry timeout:60
SXP reconcile timeout:120
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts sxp connection

To display the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (SXP) connections information, use the **show cts sxp connection** command.

show cts sxp connection

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

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 cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (SXP) connections information:

```
switch# show cts sxp connection
PEER_IP_ADDR    VRF             PEER_SXP_MODE   SELF_SXP_MODE   CONNECTION STATE
10.10.3.3       default         listener        speaker         initializing
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show dot1x

To display the 802.1X feature status, use the **show dot1x** command.

show dot1x

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the 802.1X feature by using the **feature dot1x** command before using this command.

This command does not require a license.

Examples

This example shows how to display the 802.1X feature status:

```
switch# show dot1x
          Sysauthcontrol Enabled
   Dot1x Protocol Version 2
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.

show dot1x all

To display all 802.1X feature status and configuration information, use the **show dot1x all** command.

show dot1x all [**details** | **statistics** | **summary**]

Syntax Description

details	(Optional) Displays detailed information about the 802.1X configuration.
statistics	(Optional) Displays 802.1X statistics.
summary	(Optional) Displays a summary of 802.1X information.

Defaults

Displays global and interface 802.1X configuration

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the 802.1X feature by using the **feature dot1x** command before using this command.

This command does not require a license.

Examples

This example shows how to display all 802.1X feature status and configuration information:

```
switch# show dot1x all
           Sysauthcontrol Enabled
   Dot1x Protocol Version 2

Dot1x Info for Ethernet2/1
-----------------------------------
                       PAE = AUTHENTICATOR
               PortControl = FORCE_AUTH
                  HostMode = SINGLE HOST
         ReAuthentication = Disabled
              QuietPeriod = 60
           ServerTimeout = 30
              SuppTimeout = 30
            ReAuthPeriod = 3600 (Locally configured)
               ReAuthMax = 2
                  MaxReq = 2
                 TxPeriod = 30
          RateLimitPeriod = 0
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.

show dot1x interface ethernet

To display the 802.1X feature status and configuration information for an Ethernet interface, use the **show dot1x interface ethernet** command.

show dot1x interface ethernet *slot*/*port* [**details** | **statistics** | **summary**]

Syntax Description

slot/*port*	Slot and port identifiers for the interface.
details	(Optional) Displays detailed 802.1X information for the interface.
statistics	(Optional) Displays 802.1X statistics for the interface.
summary	(Optional) Displays a summary of the 802.1X information for the interface.

Defaults

Displays the interface 802.1X configuration

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the 802.1X feature by using the **feature dot1x** command before using this command.

This command does not require a license.

Examples

This example shows how to display the 802.1X feature status and configuration information for an Ethernet interface:

```
switch# show dot1x interface ethernet 2/1

Dot1x Info for Ethernet2/1
-----------------------------------
                      PAE = AUTHENTICATOR
              PortControl = FORCE_AUTH
                 HostMode = SINGLE HOST
         ReAuthentication = Disabled
              QuietPeriod = 60
           ServerTimeout = 30
             SuppTimeout = 30
            ReAuthPeriod = 3600 (Locally configured)
               ReAuthMax = 2
                  MaxReq = 2
                TxPeriod = 30
          RateLimitPeriod = 0
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.

show encryption service stat

To display the status of the encryption service, use the show encryption service stat command.

show encryption service stat

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

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 display the status of the encryption service:

```
switch# show encryption service stat
Encryption service is enabled
Master Encryption Key is configured.
Type-6 encryption is being used
switch#
```

Related Commands

Command	Description
show key chain	Displays the configuration for a specific keychain.

show eou

To display Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) status and configuration information, use the **show eou** command.

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

Syntax Description

all	(Optional) Displays all EAPoUDP sessions.
authentication	(Optional) Displays EAPoUDP sessions for specific authentication types.
clientless	Specifies sessions authenticated using clientless posture validation.
eap	Specifies sessions authenticated using EAPoUDP.
static	Specifies sessions statically authenticated using statically configured exception lists.
interface ethernet *slot*/*port*	(Optional) Displays the EAPoUDP sessions for a specific interface.
ip-address *ipv4-address*	(Optional) Displays the EAPoUDP sessions for a specific IPv4 address.
mac-address *mac-address*	(Optional) Displays the EAPoUDP sessions for a specific MAC address.
posturetoken *name*	(Optional) Displays the EAPoUDP sessions for posture tokens.
name	(Optional) Token name.

Defaults

Displays the global EAPoUDP configuration

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the 802.1X feature by using the **feature eou** command before using this command.

This command does not require a license.

Examples

This example shows how to display all 802.1X feature status and configuration information:

```
switch# show eou all
```

This example shows how to display 802.1X clientless authentication information:

```
switch# show eou authentication clientless
```

This example shows how to display 802.1X EAP authentication information:

```
switch# show eou authentication eap
```

This example shows how to display 802.1X static authentication information:

```
switch# show eou interface ethernet 2/1
```

This example shows how to display 802.1X information for an Ethernet interface:

```
switch# show eou ip-address 10.10.10.1
```

This example shows how to display 802.1X information for a MAC address:

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

This example shows how to display 802.1X information for a MAC address:

```
switch# show eou posturetoken healthy
```

Related Commands

Command	Description
feature eou	Enables the 802.1X feature.

show fips status

To display the status of Federal Information Processing Standards (FIPS) mode, use the **show fips status** command.

show fips status

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the status of FIPS mode:

```
switch# show fips status
FIPS mode is disabled
```

Related Commands

Command	Description
fips mode enable	Enables FIPS mode.

show hardware access-list resource pooling

To display information about which I/O modules are configured with the **hardware access-list resource pooling** command, use the **show hardware access-list resource pooling** command.

show hardware access-list resource pooling

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

If no I/O modules are configured with the **hardware access-list resource pooling** command, the **show hardware access-list resource pooling** command has no output.

Examples

This example shows how to display the I/O modules that are configured with the **hardware access-list resource pooling** command:

```
switch# show hardware access-list resource pooling
  Module 1 enabled
  Module 3 enabled

switch#
```

Related Commands

Command	Description
hardware access-list resource pooling	Allows ACL-based features to use more than one TCAM bank on one or more I/O modules.

show hardware access-list status module

To display the access control list (ACL) capture configuration, use the **show hardware access-list status module** command.

show hardware access-list status module *slot*

Syntax Description

slot	Slot ID. The range is from 1 to 18.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

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 display the access control list (ACL) capture configuration:

```
switch(config)# show hardware access-list status module 5

Non-Atomic ACL updates Disabled.

TCAM Default Result is Deny.

Resource-pooling: Disabled
switch(config)#
```

Related Commands

Command	Description
hardware access-list capture	Enables access control list (ACL) capture on all virtual device contexts (VDCs).

show hardware rate-limiter

To display rate limit configuration and statistics, use the **show hardware rate-limiter** command.

show rate-limiter hardware rate-limiter {**access-list-log** [**module** *module*] | **copy** [**module** *module*] | **f1** {**rl-1** [**module** *module*] | **rl-2** [**module** *module*] | **rl-3** [**module** *module*] | **rl-4** [**module** *module*] | **rl-5** [**module** *module*]} | **layer-2** {**l2pt** [**module** *module*] | **mcast-snooping** [**module** *module*] | **port-security** [**module** *module*] | **storm-control** [**module** *module*] | **vpc-low** [**module** *module*]} | **layer-3** {**control** [**module** *module*] | **glean** [**module** *module*] | **mtu** [**module** *module*] | **multicast** {**directly-connect** [**module** *module*] | **local-groups** [**module** *module*] | **rpf-leak** [**module** *module*]} | **ttl** [**module** *module*]} | **module** *module* | **receive** [**module** *module*]

Syntax Description

access-list-log	Displays rate-limit statistics for access-list log packets.
module *module*	Specifies a module number. The range is from 1 to 18.
copy	Displays rate-limit statistics for copy packets.
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	(Optional) Displays Layer 2 packet rate limits.
l2pt	Specifies rate-limit statistics for Layer 2 Tunnel Protocol (L2TP) packets.
mcast-snooping	Specifies rate-limit statistics for Layer 2 multicast-snooping packets.
port-security	Specifies rate-limit statistics for Layer 2 port-security packets.
storm-control	Specifies rate-limit statistics for Layer 2 storm-control packets.
vpc-low	Specifies rate-limit statistics for Layer 2 control packets over the VPC low queue.
layer-3	(Optional) Displays Layer 3 packet rate limits.
control	Specifies rate-limit statistics for Layer 3 control packets.
glean	Specifies rate-limit statistics for Layer 3 glean packets.
mtu	Specifies rate-limit statistics for Layer 3 maximum transmission unit (MTU) packets.
multicast	Specifies Layer 3 multicast rate limits.
directly-connected	Specifies rate-limit statistics for Layer 3 directly connected multicast packets.
local-groups	Specifies rate-limit statistics for Layer 3 local group multicast packets.
rpf-leak	Specifies rate-limit statistics for Layer 3 reverse path forwarding (RPF) leak multicast packets.
ttl	Specifies rate-limit statistics for Layer 3 time-to-live (TTL) packets.
module *module*	(Optional) Displays rate-limit statistics for a specific module. The module number is from 1 to 18.
receive	(Optional) Displays rate-limit statistics for receive packets.

Defaults Displays all rate-limit statistics.

Command Modes Any command mode

SupportedUserRoles network-admin

Command History

Release	Modification
5.1(1)	Added the **f1**, **rl-1**, **rl-2**, **rl-3**, **rl-4**, **rl-5,** and **module** keywords.
5.0(2)	Added the **l2pt** keyword.
4.0(3)	Added the **port-security** keyword.
4.0(1)	This command was introduced.

Usage Guidelines You can use the command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to display all the rate-limit configuration and statistics:

```
switch# show hardware rate-limiter

Units for Config: packets per second
Allowed, Dropped & Total: aggregated since last clear counters

Rate Limiter Class                          Parameters
------------------------------------------------------------
layer-3 mtu                                 Config    : 500
                                            Allowed   : 0
                                            Dropped   : 0
                                            Total     : 0

layer-3 ttl                                 Config    : 500
                                            Allowed   : 0
                                            Dropped   : 0
                                            Total     : 0

layer-3 control                             Config    : 10000
                                            Allowed   : 0
                                            Dropped   : 0
                                            Total     : 0

layer-3 glean                               Config    : 100
                                            Allowed   : 0
                                            Dropped   : 0
                                            Total     : 0

layer-3 multicast directly-connected        Config    : 3000
                                            Allowed   : 0
                                            Dropped   : 0
                                            Total     : 0

layer-3 multicast local-groups              Config    : 3000
                                            Allowed   : 0
                                            Dropped   : 0
                                            Total     : 0

layer-3 multicast rpf-leak                  Config    : 500
                                            Allowed   : 0
                                            Dropped   : 0
                                            Total     : 0
```

```
layer-2 storm-control                   Config    : Disabled

access-list-log                         Config    : 100
                                        Allowed   : 0
                                        Dropped   : 0
                                        Total     : 0

copy                                    Config    : 30000
                                        Allowed   : 0
                                        Dropped   : 0
                                        Total     : 0

receive                                 Config    : 30000
                                        Allowed   : 0
                                        Dropped   : 0
                                        Total     : 0

layer-2 port-security                   Config    : Disabled

layer-2 mcast-snooping                  Config    : 10000
                                        Allowed   : 0
                                        Dropped   : 0
                                        Total     : 0

layer-2 vpc-low                         Config    : 4000
                                        Allowed   : 0
                                        Dropped   : 0
                                        Total     : 0

layer-2 l2pt                            Config    : 500
                                        Allowed   : 0
                                        Dropped   : 0
                                        Total     : 0
```

This example shows how to display the rate-limit configuration and statistics for access-list log packets:

```
switch# show hardware rate-limiter access-list-log

Units for Config: packets per second
Allowed, Dropped & Total: aggregated since last clear counters

Rate Limiter Class                      Parameters
------------------------------------------------------------
access-list-log                         Config    : 100
                                        Allowed   : 0
                                        Dropped   : 0
                                        Total     : 0
```

Related Commands

Command	Description
clear hardware rate-limiter	Clears rate-limit statistics.
hardware rate-limiter	Configures rate limits.

show identity policy

To display the identity policies, use the **show identity policy** command.

show identity policy [*policy-name*]

Syntax Description

policy-name	(Optional) Name of a policy. The name is case sensitive.

Defaults

Displays information for all identity policies.

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin
VDC user

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information for all of the identity policies:

```
switch# show identity policy
```

This example shows how to display information for a specific identity policy:

```
switch# show identity policy AdminPolicy
```

Related Commands

Command	Description
identity policy	Configures identity policies.

show identity profile

To display the identity profiles, use the **show identity profile** command.

show identity profile [**eapoudp**]

Syntax Description

eapoudp	(Optional) Displays the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) identity profile.

Defaults

Displays information for all identity profiles.

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin
VDC user

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the identity profiles:

```
switch# show identity profile
```

This example shows how to display the EAPoUDP identity profile configuration:

```
switch# show identity profile eapoudp
```

Related Commands

Command	Description
identity profile eapoudp	Configures EAPoUDP identity profiles.

show ip access-lists

To display all IPv4 access control lists (ACLs) or a specific IPv4 ACL, use the **show ip access-lists** command.

show ip access-lists [*access-list-name*] [**expanded | summary**]

Syntax Description

access-list-name	(Optional) Name of an IPv4 ACL, which can be up to 64 alphanumeric, case-sensitive characters.
expanded	(Optional) Specifies that the contents of IPv4 address groups or port groups show rather than the names of object groups only.
summary	(Optional) Specifies that the command displays information about the ACL rather than the ACL configuration. For more information, see the "Usage Guidelines" section.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	Command output is sorted alphabetically by the ACL names. Support was added for the **fragments** command.
4.0(1)	This command was introduced.

Usage Guidelines

The device shows all IPv4 ACLs, unless you use the *access-list-name* argument to specify an ACL.

If you do not specify an ACL name, the device lists ACLs alphabetically by the ACL names.

IPv4 address object groups and IP port object groups show only by name, unless you use the **expanded** keyword.

The **expanded** keyword allows you to display the details of object groups used in an ACL rather than only the name of the object groups. For more information about object groups, see the **object-group ip address** and **object-group ip port** commands.

The **summary** keyword allows you to display information about the ACL rather than the ACL configuration. The information displayed includes the following:

- Whether per-entry statistics are configured for the ACL.
- Whether the **fragments** command is configured for the ACL.
- The number of rules in the ACL configuration. This number does not reflect how many entries that the ACL contains when the device applies it to an interface. If a rule in the ACL uses an object group, the number of entries in the ACL when it is applied may be much greater than the number of rules.
- The interfaces that the ACL is applied to.
- The interfaces that the ACL is active on.

The **show ip access-lists** command displays statistics for each entry in an ACL if the following conditions are both true:

- The ACL configuration contains the **statistics per-entry** command.
- The ACL is applied to an interface that is administratively up.

If an IP ACL includes the **fragments** command, it appears before the explicit permit and deny rules, but the device applies the **fragments** command to noninitial fragments only if they do not match all other explicit rules in the ACL.

This command does not require a license.

Examples

This example shows how to use the **show ip access-lists** command to display all IPv4 ACLs on a device that has a single IPv4 ACL:

```
switch# show ip access-lists

IP access list ipv4-open-filter
        10 permit ip any any
```

This example shows how to use the **show ip access-lists** command to display an IPv4 ACL named ipv4-RandD-outbound-web, including per-entry statistics for the entries except for the MainLab object group:

```
switch# show ip access-lists ipv4-RandD-outbound-web

IP access list ipv4-RandD-outbound-web
        statistics per-entry
        fragments deny-all
        1000 permit ahp any any [match=732]
        1005 permit tcp addrgroup MainLab any eq telnet
        1010 permit tcp any any eq www [match=820421]
```

This example shows how to use the **show ip access-lists** command to display an IPv4 ACL named ipv4-RandD-outbound-web. The **expanded** keyword causes the contents of the object group from the previous example to appear, including the per-entry statistics:

```
switch# show ip access-lists ipv4-RandD-outbound-web expanded

IP access list ipv4-RandD-outbound-web
        statistics per-entry
        1000 permit ahp any any [match=732]
        1005 permit tcp 10.52.34.4/32 any eq telnet [match=5032]
        1005 permit tcp 10.52.34.27/32 any eq telnet [match=433]
        1010 permit tcp any any eq www [match=820421]
```

This example shows how to use the **show ip access-lists** command with the **summary** keyword to display information about an IPv4 ACL named ipv4-RandD-outbound-web, such as which interfaces the ACL is applied to and active on:

```
switch# show ip access-lists ipv4-RandD-outbound-web summary
IPV4 ACL ipv4-RandD-outbound-web

        Statistics enabled
        Total ACEs Configured: 4
        Configured on interfaces:
                Ethernet2/4 - ingress (Router ACL)
        Active on interfaces:
                Ethernet2/4 - ingress (Router ACL)
```

Related Commands

Command	Description
fragments	Configures how an IP ACL processes noninitial fragments.
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays all ACLs or a specific ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.
statistics per-entry	Starts recording statistics for packets permitted or denied by each entry in an ACL.

show ip access-lists capture session

To display the ACL capture session configuration, use the **show ip access-lists capture session** command.

show ip access-lists capture session *session*

Syntax Description

session	Session ID. The range is from 0 to 4294967295.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

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 display the ACL capture session configuration:

```
switch# show ip access-lists capture session 5
switch#
```

Related Commands

Command	Description
monitor session *session* **type acl-capture**	Configures an ACL capture session.
destination interface	Configures a destination for ACL capture packets.

show ip arp inspection

To display the Dynamic ARP Inspection (DAI) configuration status, use the **show ip arp inspection** command.

show ip arp inspection

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the status of the DAI configuration:

```
switch# show ip arp inspection

Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled

Vlan : 1
-----------
Configuration    : Enabled
Operation State  : Active

ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
```

Related Commands

Command	Description
ip arp inspection vlan	Enables DAI for a specified list of VLANs.
show ip arp inspection interface	Displays the trust state and the ARP packet rate for a specified interface.
show ip arp inspection log	Displays the DAI log configuration.
show ip arp inspection statistics	Displays the DAI statistics.
show ip arp inspection vlan	Displays DAI status for a specified list of VLANs.
show running-config dhcp	Displays DHCP snooping configuration, including DAI configuration.

show ip arp inspection interface

To display the trust state for the specified interface, use the **show ip arp inspection interface** command.

show ip arp inspection interface {**ethernet** *slot/port* | **port-channel** *channel-number*}

Syntax Description

ethernet *slot/port*	(Optional) Specifies that the output is for an Ethernet interface.
port-channel *channel-number*	(Optional) Specifies that the output is for a port-channel interface. Valid port-channel numbers are from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the trust state for a trusted interface:

```
switch# show ip arp inspection interface ethernet 2/1

 Interface        Trust State
 -------------    -----------
 Ethernet2/46        Trusted
switch#
```

Related Commands

Command	Description
ip arp inspection vlan	Enables Dynamic ARP Inspection (DAI) for a specified list of VLANs.
show ip arp inspection	Displays the DAI configuration status.
show ip arp inspection log	Displays the DAI log configuration.
show ip arp inspection statistics	Displays the DAI statistics.

Command	Description
show ip arp inspection vlan	Displays DAI status for a specified list of VLANs.
show running-config dhcp	Displays DHCP snooping configuration, including DAI configuration.

show ip arp inspection log

To display the Dynamic ARP Inspection (DAI) log configuration, use the **show ip arp inspection log** command.

show ip arp inspection log

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the DAI log configuration:

```
switch# show ip arp inspection log

Syslog Buffer Size : 32
Syslog Rate        : 5 entries per 1 seconds
switch#
```

Related Commands

Command	Description
clear ip arp inspection log	Clears the DAI logging buffer.
ip arp inspection log-buffer	Configures the DAI logging buffer size.
show ip arp inspection	Displays the DAI configuration status.
show ip arp inspection interface	Displays the trust state and the ARP packet rate for a specified interface.
show running-config dhcp	Displays DHCP snooping configuration, including DAI configuration.

show ip arp inspection statistics

Use the **show ip arp inspection statistics** command to display the Dynamic ARP Inspection (DAI) statistics. You can specify a VLAN or range of VLANs.

show ip arp inspection statistics [**vlan** *vlan-list*]

Syntax Description

vlan *vlan-list*	(Optional) Specifies the list of VLANs for which to display DAI statistics. Valid VLAN IDs are from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the DAI statistics for VLAN 1:

```
switch# show ip arp inspection statistics vlan 1

Vlan : 1
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switch#
```

Related Commands

Command	Description
clear ip arp inspection statistics vlan	Clears the DAI statistics for a specified VLAN.
show ip arp inspection	Displays the DAI configuration status.
show ip arp inspection interface	Displays the trust state and the ARP packet rate for a specified interface.
show ip arp inspection log	Displays the DAI log configuration.
show running-config dhcp	Displays DHCP snooping configuration, including DAI configuration.

show ip arp inspection vlan

Use the **show ip arp inspection vlan** command to display Dynamic ARP Inspection (DAI) status for the specified list of VLANs.

show ip arp inspection vlan *vlan-list*

Syntax Description

vlan-list	VLANs with DAI status that this command shows. The *vlan-list* argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges (see the "Examples" section). Valid VLAN IDs are from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

This example shows how to display DAI status for VLANs 1 and 13:

```
switch# show ip arp inspection vlan 1,13

Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled

Vlan : 1
-----------
Configuration    : Enabled
Operation State  : Active

Vlan : 13
-----------
Configuration    : Enabled
Operation State  : Inactive
switch#
```

Related Commands

Command	Description
clear ip arp inspection statistics vlan	Clears the DAI statistics for a specified VLAN.
ip arp inspection vlan	Enables DAI for a specified list of VLANs.
show ip arp inspection	Displays the DAI configuration status.
show ip arp inspection interface	Displays the trust state and the ARP packet rate for a specified interface.
show running-config dhcp	Displays DHCP snooping configuration, including DAI configuration.

show ip device tracking

To display IP device tracking information, use the **show ip device tracking** command.

show ip device tracking {**all** | **interface ethernet** *slot*/*port* | **ip-address** *ipv4-address* | **mac-address** *mac-address*}

Syntax Description

all	Displays all IP device tracking information.
interface ethernet *slot*/*port*	Displays IP tracking device information for an interface.
ip-address *ipv4-address*	Displays IP tracking device information for an IPv4 address in the A.B.C.D format.
mac-address *mac-address*	Displays IP tracking information for a MAC address in the XXXX.XXXX.XXXX format.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin
VDC user

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display all IP device tracking information:

```
switch# show ip device tracking all
```

This example shows how to display the IP device tracking information for an interface:

```
switch# show ip device tracking ethernet 1/2
```

This example shows how to display the IP device tracking information for an IP address:

```
switch# show ip device tracking ip-address 10.10.1.1
```

This example shows how to display the IP device tracking information for a MAC address:

```
switch# show ip device tracking mac-address 0018.bad8.3fbd
```

Related Commands

Command	Description
ip device tracking	Configures IP device tracking.

show ip dhcp relay

To display DHCP snooping relay status, including DHCP server addresses configured on interfaces, use the **show ip dhcp relay** command.

show ip dhcp relay

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

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 display the DHCP relay status and configured DHCP server addresses:

```
switch# show ip dhcp relay
DHCP relay service is enabled
Insertion of option 82 is enabled
Insertion of VPN suboptions is enabled
Helper addresses are configured on the following interfaces:
 Interface        Relay Address     VRF Name
 -------------    -------------     --------
 Ethernet1/4       10.10.10.1       red
switch#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp relay	Enables the DHCP relay agent.
show ip dhcp relay address	Shows DHCP server addresses configured on the device.

show ip dhcp relay address

To display DHCP server addresses configured on the device, use the **show ip dhcp relay address** command.

show ip dhcp relay address [**interface** {**ethernet** *list* | **port-channel** *list*}]

show ip dhcp relay address [**interface** *interface-list*]

Syntax Description

interface	(Optional) Restricts the output to a DHCP addresses configured on range or set of Ethernet or port-channel interfaces and subinterfaces.
ethernet	(Optional) Restricts the output to a DHCP addresses configured on range or set of Ethernet interfaces and subinterfaces.
list	Single interface, range of interfaces, or comma-separated interfaces and ranges (see the “Examples” section).
port-channel	(Optional) Restricts the output to a DHCP addresses configured on range or set of port-channel interfaces and subinterfaces.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
5.0(2)	Support was added for the **interface** keyword and for VRF awareness.
4.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display all the DHCP relay addresses configured on a device:

```
switch# show ip dhcp relay address
 Interface        Relay Address     VRF Name
 -------------    -------------     --------
 Ethernet1/2       10.1.1.1
 Ethernet1/3       10.1.1.1         red
 Ethernet1/4       10.1.1.1         red
 Ethernet1/5       10.1.1.1         red
 Ethernet1/6       10.1.1.1         red
 Ethernet1/7       10.1.1.1         red
 Ethernet1/8       10.1.1.1         red

switch#
```

This example shows how to display the DHCP relay addresses configured Ethernet interfaces 1/2 through 1/4 and Ethernet 1/8:

```
switch(config-if)# show ip dhcp relay address interface ethernet 1/2-4,ethernet 1/8
 Interface        Relay Address     VRF Name
 -------------    -------------     --------
 Ethernet1/2       10.1.1.1
 Ethernet1/3       10.1.1.1         red
 Ethernet1/4       10.1.1.1         red
 Ethernet1/8       10.1.1.1         red
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp relay	Enables the DHCP relay agent.
show ip dhcp relay	Shows DHCP relay status and server addresses configured on the device.

show ip dhcp snooping

To display general status information for DHCP snooping, use the **show ip dhcp snooping** command.

show ip dhcp snooping

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display general status information about DHCP snooping:

```
switch# show ip dhcp snooping
DHCP snooping service is enabled
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
1,13
DHCP snooping is operational on the following VLANs:
1
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface             Trusted
------------          -------
Ethernet2/3           Yes

switch#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp snooping	Globally enables DHCP snooping on the device.
show ip dhcp snooping binding	Displays IP-MAC address bindings, including the static IP source entries.
show ip dhcp snooping statistics	Displays DHCP snooping statistics.
show running-config dhcp	Displays DHCP snooping configuration.

show ip dhcp snooping binding

To display IP-to-MAC address bindings for all interfaces or a specific interface, use the **show ip dhcp snooping binding** command. It includes static IP source entries. Static entries appear with the term "static" in the Type column.

show ip dhcp snooping binding [*IP-address*] [*MAC-address*] [**interface ethernet** *slot*/*port*] [**vlan** *vlan-id*]

show ip dhcp snooping binding [**dynamic**]

show ip dhcp snooping binding [**static**]

Syntax Description

IP-address	(Optional) IPv4 address that the bindings shown must include. Valid entries are in dotted-decimal format.
MAC-address	(Optional) MAC address that the bindings shown must include. Valid entries are in dotted-hexadecimal format.
interface ethernet *slot*/*port*	(Optional) Specifies the Ethernet interface that the bindings shown must be associated with.
vlan *vlan-id*	(Optional) Specifies a VLAN ID that the bindings shown must be associated with. Valid VLAN IDs are from 1 to 4096.
dynamic	(Optional) Limits the output to all dynamic IP-MAC address bindings.
static	(Optional) Limits the output to all static IP-MAC address bindings.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display all bindings:

```
switch# show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type        VLAN  Interface
------------------  ---------------  --------  ----------  ----  -------------
0f:00:60:b3:23:33   10.3.2.2         infinite  static      13    Ethernet2/46
0f:00:60:b3:23:35   10.2.2.2         infinite  static      100   Ethernet2/10
switch#
```

Related Commands

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

show ip dhcp snooping statistics

To display DHCP snooping statistics, use the **show ip dhcp snooping statistics** command.

show ip dhcp snooping statistics

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display DHCP snooping statistics:

```
switch# show ip dhcp snooping statistics
Packets processed 0
Packets received through cfsoe 0
Packets forwarded 0
Packets forwarded on cfsoe 0
Total packets dropped 0
Packets dropped from untrusted ports 0
Packets dropped due to MAC address check failure 0
Packets dropped due to Option 82 insertion failure 0
Packets dropped due to o/p intf unknown 0
Packets dropped which were unknown 0
Packets dropped due to dhcp relay not enabled 0
Packets dropped due to no binding entry 0
Packets dropped due to interface error/no interface 0
Packets dropped due to max hops exceeded 0
switch#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
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 ip dhcp snooping binding	Displays IP-MAC address bindings, including the static IP source entries.
show running-config dhcp	Displays DHCP snooping configuration.

show ip verify source

To display the IP-to-MAC address bindings, use the **show ip verify source** command.

show ip verify source [**interface** {**ethernet** *slot*/*port* | **port-channel** *channel-number*}]

Syntax Description

interface	(Optional) Specifies that the output is limited to IP-to-MAC address bindings for a particular interface.
ethernet *slot*/*port*	(Optional) Specifies that the output is limited to bindings for the Ethernet interface given.
port-channel *channel-number*	(Optional) Specifies that the output is limited to bindings for the port-channel interface given. Valid port-channel numbers are from 1 to 4096.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the IP-to-MAC address bindings:

```
switch# show ip verify source
switch#
```

Related Commands

Command	Description
ip source binding	Creates a static IP source entry for the specified Ethernet interface.
ip verify source dhcp-snooping-vlan	Enables IP Source Guard on an interface.
show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.

show ipv6 access-lists

To display all IPv6 access-control lists (ACLs) or a specific IPv6 ACL, use the **show ipv6 access-lists** command.

show ipv6 access-lists [*access-list-name*] [**expanded | summary**]

Syntax Description

access-list-name	(Optional) Name of an IPv6 ACL, which can be up to 64 alphanumeric, case-sensitive characters.
expanded	(Optional) Specifies that the contents of IPv6 address groups or port groups show rather than the names of object groups only.
summary	(Optional) Specifies that the command displays information about the ACL rather than the ACL configuration. For more information, see the "Usage Guidelines" section.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	Command output is sorted alphabetically by the ACL names. Support was added for the **fragments** command.
4.1(2)	This command was introduced.

Usage Guidelines

The device shows all IPv6 ACLs, unless you use the *access-list-name* argument to specify an ACL.

If you do not specify an ACL name, the device lists ACLs alphabetically by the ACL names.

IPv6 address object groups and IP port object groups show only by name, unless you use the **expanded** keyword.

The **expanded** keyword allows you to display the details of object groups used in an ACL rather than only the name of the object groups. For more information about object groups, see the **object-group ipv6 address** and **object-group ip port** commands.

The **summary** keyword allows you to display information about the ACL rather than the ACL configuration. The information displayed includes the following:

- Whether per-entry statistics are configured for the ACL.
- Whether the **fragments** command is configured for the ACL.
- The number of rules in the ACL configuration. This number does not reflect how many entries that the ACL contains when the device applies it to an interface. If a rule in the ACL uses an object group, the number of entries in the ACL when it is applied may be much greater than the number of rules.
- The interfaces that the ACL is applied to.
- The interfaces that the ACL is active on.

The **show ipv6 access-lists** command displays statistics for each entry in an ACL if the following conditions are both true:

- The ACL configuration contains the **statistics per-entry** command.
- The ACL is applied to an interface that is administratively up.

If an IP ACL includes the **fragments** command, it appears before the explicit permit and deny rules, but the device applies the **fragments** command to noninitial fragments only if they do not match all other explicit rules in the ACL.

This command does not require a license.

Examples

This example shows how to use the **show ipv6 access-lists** command to display all IPv6 ACLs on a device that has a single IPv6 ACL:

```
switch# show ipv6 access-lists

IPv6 access list ipv6-main-filter
        10 permit ipv6 any any
```

This example shows how to use the **show ipv6 access-lists** command to display an IPv6 ACL named ipv6-RandD-outbound-web, including per-entry statistics for the entries except for the LowerLab object group:

```
switch# show ipv6 access-lists ipv6-RandD-outbound-web

IPv6 access list ipv6-RandD-outbound-web
        statistics per-entry
        fragments deny-all
        1000 permit ahp any any [match=732]
        1005 permit tcp addrgroup LowerLab any eq telnet
        1010 permit tcp any any eq www [match=820421]
```

This example shows how to use the **show ipv6 access-lists** command to display an IPv6 ACL named ipv6-RandD-outbound-web. The **expanded** keyword causes the contents of the object group from the previous example to appear, including the per-entry statistics:

```
switch# show ipv6 access-lists ipv6-RandD-outbound-web expanded

IPv6 access list ipv6-RandD-outbound-web
        statistics per-entry
        1000 permit ahp any any [match=732]
        1005 permit tcp 2001:db8:0:3ab0::1/128 any eq telnet [match=5032]
        1005 permit tcp 2001:db8:0:3ab0::32/128 any eq telnet [match=433]
        1010 permit tcp any any eq www [match=820421]
```

This example shows how to use the **show ipv6 access-lists** command with the **summary** keyword to display information about an IPv6 ACL named ipv6-RandD-outbound-web, such as which interfaces the ACL is applied to and active on:

```
switch# show ipv6 access-lists ipv6-RandD-outbound-web summary
IPV6 ACL ipv6-RandD-outbound-web

        Statistics enabled
        Total ACEs Configured: 4
        Configured on interfaces:
                Ethernet2/4 - ingress (Router ACL)
        Active on interfaces:
                Ethernet2/4 - ingress (Router ACL)
```

Related Commands

Command	Description
fragments	Configures how an IP ACL processes noninitial fragments.
ipv6 access-list	Configures an IPv6 ACL.
show access-lists	Displays all ACLs or a specific ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.
statistics per-entry	Starts recording statistics for packets permitted or denied by each entry in an ACL.

show key chain

To display the configuration for a specific keychain, use the **show key chain** command.

show key chain *keychain-name* [**mode decrypt**]

Syntax Description

keychain-name	Name of the keychain to configure, up to 63 alphanumerical characters.
mode decrypt	(Optional) Shows the key text configuration in cleartext. This option is available only when access the device with a user account that is assigned a network-admin or vdc-admin user role.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display keychain configuration for the keychain glbp-key, which contains one key (key 13) which has specific accept and send lifetimes:

```
switch# show key chain
Key-Chain glbp-keys
  Key 13 -- text 7 071a33595c1d0c1702170203163e3e21213c20361a021f11
    accept lifetime UTC (00:00:00 Jun 13 2008) - (23:59:59 Sep 12 2008)
    send lifetime UTC (00:00:00 Jun 13 2008) - (23:59:59 Aug 12 2008)
```

Related Commands

Command	Description
accept-lifetime	Configures an accept lifetime for a key.
key	Configures a key.
key chain	Configures a keychain.

Command	Description
key-string	Configures a key string.
send-lifetime	Configures a send lifetime for a key.

show ldap-search-map

To display information about the configured Lightweight Directory Access Protocol (LDAP) attribute maps, use the **show ldap-search-map** command.

show ldap-search-map

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must use the **feature ldap** command before you can display LDAP information.

This command does not require a license.

Examples

This example shows how to display information about the configured LDAP attribute maps:

```
switch# show ldap-search-map
total number of search maps : 1

following LDAP search maps are configured:
    SEARCH MAP  s0:
      User Profile:
        BaseDN: DN1
        Attribute Name: map1
        Search Filter: filter1
```

Related Commands

Command	Description
attribute-name	Configures the attribute name, search filter, and base-DN for the user profile, trusted certificate, CRL, certificate DN match, public key match, or user-switchgroup lookup search operation.
feature ldap	Enables LDAP.

Command	Description
ldap search-map	Configures an LDAP search map.
ldap-server host	Specifies the IPv4 or IPv6 address or hostname for an LDAP server.

show ldap-server

To display the Lightweight Directory Access Protocol (LDAP) server configuration, use the **show ldap-server** command.

show ldap-server

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must use the **feature ldap** command before you can display LDAP information.

This command does not require a license.

Examples

This example shows how to display the LDAP server configuration:

```
switch# show ldap-server
     timeout : 5
        port : 389
    deadtime : 0
total number of servers : 0
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap-server host	Specifies the IPv4 or IPv6 address or hostname for an LDAP server.

show ldap-server groups

To display the Lightweight Directory Access Protocol (LDAP) server group configuration, use the **show ldap-server groups** command.

show ldap-server groups

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must use the **feature ldap** command before you can display LDAP information.

This command does not require a license.

Examples

This example shows how to display the LDAP server group configuration:

```
switch# show ldap-server groups
total number of groups: 1

following LDAP server groups are configured:
    group LDAPgroup1:
        Use-vrf: default
        Mode: UnSecure
        Authentication: Search and Bind
        Bind and Search : append with basedn (cn=$userid)
        Authentication: Do bind instead of compare
        Bind and Search : compare passwd attribute userPassword
        Authentication Mech: Default(PLAIN)
        Search map:
```

Related Commands

Command	Description
aaa group server ldap	Creates an LDAP server group and enters the LDAP server group configuration mode for that group.
feature ldap	Enables LDAP.

show ldap-server statistics

To display the Lightweight Directory Access Protocol (LDAP) server statistics, use the **show ldap-server statistics** command.

show ldap-server statistics {*ipv4-address* | *ipv6-address* | *host-name*}

Syntax Description

ipv4-address	Server IPv4 address in the *A.B.C.D* format.
ipv6-address	Server IPv6 address in the *X:X:X:X* format.
host-name	Server name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must use the **feature ldap** command before you can display LDAP information.

This command does not require a license.

Examples

This example shows how to display the statistics for an LDAP server:

```
switch# show ldap-server statistics 10.10.1.1
Server is not monitored

Authentication Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap-server host	Specifies the IPv4 or IPv6 address or hostname for an LDAP server.

show mac access-lists

To display all MAC access control lists (ACLs) or a specific MAC ACL, use the **show mac access-lists** command.

show mac access-lists [*access-list-name*] [**summary**]

Syntax Description

access-list-name	(Optional) Name of a MAC ACL, which can be up to 64 alphanumeric, case-sensitive characters.
summary	(Optional) Specifies that the command displays information about the ACL rather than the ACL configuration. For more information, see the "Usage Guidelines" section.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	Command output is sorted alphabetically by the ACL names.
4.0(1)	This command was introduced.

Usage Guidelines

The device shows all MAC ACLs, unless you use the *access-list-name* argument to specify an ACL.

If you do not specify an ACL name, the device lists ACLs alphabetically by the ACL names.

The **summary** keyword allows you to display information about the ACL rather than the ACL configuration. The information displayed includes the following:

- Whether per-entry statistics are configured for the ACL.
- The number of rules in the ACL configuration. This number does not reflect how many entries that the ACL contains when the device applies it to an interface. If a rule in the ACL uses an object group, the number of entries in the ACL when it is applied may be much greater than the number of rules.
- The interfaces that the ACL is applied to.
- The interfaces that the ACL is active on.

The **show mac access-lists** command displays statistics for each entry in an ACL if the following conditions are both true:

- The ACL configuration contains the **statistics per-entry** command.
- The ACL is applied to an interface that is administratively up.

This command does not require a license.

Examples

This example shows how to use the **show mac access-lists** command to show all MAC ACLs on a device with a single MAC ACL:

```
switch# show mac access-lists

MAC access list mac-filter
        10 permit any any ip
```

This example shows how to use the **show mac access-lists** command to display a MAC ACL named mac-lab-filter, including per-entry statistics:

```
switch# show mac access-lists mac-lab-filter

MAC access list mac-lab-filter
        statistics per-entry
        10 permit 0600.ea5f.22ff 0000.0000.0000 any [match=820421]
        20 permit 0600.050b.3ee3 0000.0000.0000 any [match=732]
```

This example shows how to use the **show mac access-lists** command with the **summary** keyword to display information about a MAC ACL named mac-lab-filter, such as which interfaces the ACL is applied to and active on:

```
switch# show mac access-lists mac-lab-filter summary

MAC ACL mac-lab-filter

        Statistics enabled
        Total ACEs Configured: 2
        Configured on interfaces:
                Ethernet2/3 - ingress (Port ACL)
        Active on interfaces:
                Ethernet2/3 - ingress (Port ACL)
```

Related Commands

Command	Description
mac access-list	Configures a MAC ACL.
show access-lists	Displays all ACLs or a specific ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.
show ipv6 access-lists	Displays all IPv6 ACLs or a specific IPv6 ACL.

show password strength-check

To display password-strength checking status, use the **show password strength-check** command.

show password strength-check

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display password-strength checking status:

```
switch# show password strength-check
Password strength check enabled
```

Related Commands

Command	Description
password strength-check	Enables password-strength checking.
show running-config security	Displays security feature configuration in the running configuration.

show policy-map type control-plane

To display control plane policy map information, use the **show policy-map type control-plane** command.

show policy-map type control-plane [**expand**] [**name** *policy-map-name*]

Syntax Description

expand	(Optional) Displays expanded control plane policy map information.
name *policy-map-name*	(Optional) Specifies the name of the control plane policy map. The name is case sensitive.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to display control plane policy map information:

```
switch# show policy-map type control-plane

  policy-map type control-plane copp-system-policy
    class copp-system-class-critical
      police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform transmit
        exceed transmit violate drop
    class copp-system-class-important
      police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform transmit
        exceed transmit violate drop
    class copp-system-class-normal
      police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform transmit
        exceed transmit violate drop
    class class-default
      police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform transmit
        exceed transmit violate drop
```

show port-security

To show the state of port security on the device, use the **show port-security** command.

show port-security [**state**]

Syntax Description

state	(Optional) Shows that port security is enabled.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	Support for Layer 2 port-channel interfaces was added.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to use the **show port-security** command to view the status of the port security feature on a device:

```
switch# show port-security

Total Secured Mac Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

--------------------------------------------------------------------------------
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
--------------------------------------------------------------------------------
Ethernet1/4           5              1              0              Shutdown
================================================================================
switch#
```

Related Commands

Command	Description
feature port-security	Enables the port security feature.
show port-security address	Shows MAC addresses secured by the port security feature.
show port-security interface	Shows the port security status for a specific interface.
switchport port-security	Configures port security on a Layer 2 interface.

show port-security address

To show information about MAC addresses secured by the port security feature, use the **show port-security address** command.

show port-security address [**interface** {**port-channel** *channel-number* | **ethernet** *slot*/*port*}]

Syntax Description

interface	(Optional) Limits the port-security MAC address information to a specific interface.
port-channel *channel-number*	Specifies a Layer 2 port-channel interface. The *channel-number* argument can be a whole number from 1 to 4096.
ethernet *slot*/*port*	Specifies an Ethernet interface.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	Support for Layer 2 port-channel interfaces was added.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to use the **show port-security address** command to view information about all MAC addresses secured by port security:

```
switch# show port-security address

Total Secured Mac Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

-------------------------------------------------------------------------
                    Secure Mac Address Table
-------------------------------------------------------------------------
Vlan    Mac Address             Type             Ports      Remaining Age
                                                               (mins)
----    -----------             ------           -----     -------------
   1    0054.AAB3.770F          STATIC        port-channel1     0
   1    00EE.378A.ABCE          STATIC        Ethernet1/4       0
=========================================================================
switch#
```

This example shows how to use the **show port-security address** command to view the MAC addresses secured by the port security feature on the Ethernet 1/4 interface:

```
switch# show port-security address interface ethernet 1/4
                     Secure Mac Address Table
-------------------------------------------------------------------------
Vlan    Mac Address             Type             Ports      Remaining Age
                                                               (mins)
----    -----------             ------           -----     -------------
   1    00EE.378A.ABCE          STATIC        Ethernet1/4       0
-------------------------------------------------------------------------
switch#
```

Related Commands

Command	Description
feature port-security	Enables the port security feature.
show port-security	Shows the status of the port security feature.
show port-security interface	Shows the port security status for a specific interface.
switchport port-security	Configures port security on a Layer 2 interface.

show port-security interface

To show the state of port security on a specific interface, use the **show port-security interface** command.

show port-security interface {**port-channel** *channel-number* | **ethernet** *slot*/*port*}

Syntax Description

port-channel *channel-number*	Specifies a Layer 2 port-channel interface. The *channel-number* argument can be a whole number from 1 to 4096.
ethernet *slot*/*port*	Specifies an Ethernet interface.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	Support for Layer 2 port-channel interfaces was added.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to use the **show port-security interface** command to view the status of the port security feature on the Ethernet 1/4 interface:

```
switch# show port-security interface ethernet 1/4
Port Security              : Enabled
Port Status                : Secure Down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
Maximum MAC Addresses      : 5
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Security violation count   : 0
switch#
```

Related Commands

Command	Description
feature port-security	Enables the port security feature.
show port-security	Shows the status of the port security feature.
show port-security address	Shows MAC addresses secured by the port security feature.
switchport port-security	Configures port security on a Layer 2 interface.

show privilege

To show the current privilege level, username, and status of cumulative privilege support, use the **show privilege** command.

show privilege

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

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 use the **show privilege** command to view the current privilege level, username, and status of cumulative privilege support:

```
switch# show privilege
User name: admin
Current privilege level: -1
Feature privilege: Enabled
switch#
```

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.
feature privilege	Enables the cumulative privilege of roles for command authorization on TACACS+ servers.
username *username* **priv-lvl**	Enables a user to use privilege levels for authorization.

show radius

To display the RADIUS Cisco Fabric Services (CFS) distribution status and other details, use the **show radius** command.

show radius {**distribution status** | **merge status** | **pending** [**cmds**] | **pending-diff** | **session status** | **status**}

Syntax Description

distribution status	Displays the status of the RADIUS CFS distribution.
merge status	Displays the status of a RADIUS merge.
pending	Displays the pending configuration that is not yet applied to the running configuration.
cmds	(Optional) Displays the commands for the pending configuration.
pending-diff	Displays the difference between the active configuration and the pending configuration.
session status	Displays the status of the RADIUS CFS session.
status	Displays the status of the RADIUS CFS.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the RADIUS CFS distribution status:

```
switch# show radius distribution status
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: not yet initiated after enable

last operation: enable
last operation status: success
```

This example shows how to display the RADIUS merge status:

```
switch# show radius merge status
Result: Waiting
```

This example shows how to display the RADIUS CFS session status:

```
switch# show radius session status
Last Action Time Stamp     : None
Last Action                : Distribution Enable
Last Action Result         : Success
Last Action Failure Reason : none
```

This example shows how to display the RADIUS CFS status:

```
switch# show radius status
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: not yet initiated after enable

last operation: enable
last operation status: success
```

This example shows how to display the pending RADIUS configuration:

```
switch# show radius pending
radius-server host 10.10.1.1 key 7 qxz123aaa group server radius aaa-private-sg
```

This example shows how to display the pending RADIUS configuration commands:

```
switch# show radius pending cmds
radius-server host 10.10.1.1 key 7 qxz12345 auth_port 1812 acct_port 1813 authentication
accounting
```

This example shows how to display the differences between the pending RADIUS configuration and the current RADIUS configuration:

```
switch(config)# show radius pending-diff
    +radius-server host 10.10.1.1 authentication accounting
```

show radius-server

To display RADIUS server information, use the **show radius-server** command.

show radius-server [*hostname* | *ipv4-address* | *ipv6-address*]
[**directed-request** | **groups** | **sorted** | **statistics**]

Syntax Description

hostname	(Optional) RADIUS server Domain Name Server (DNS) name. The name is case sensitive.
ipv4-address	(Optional) RADIUS server IPv4 address in the *A.B.C.D* format.
ipv6-address	(Optional) RADIUS server IPv6 address in the *X:X:X:X* format.
directed-request	(Optional) Displays the directed request configuration.
groups	(Optional) Displays information about the configured RADIUS server groups.
sorted	(Optional) Displays sorted-by-name information about the RADIUS servers.
statistics	(Optional) Displays RADIUS statistics for the RADIUS servers.

Defaults

Displays the global RADIUS server configuration

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

RADIUS preshared keys are not visible in the **show radius-server** command output. Use the **show running-config radius** command to display the RADIUS preshared keys.

This command does not require a license.

Examples

This example shows how to display information for all RADIUS servers:

```
switch# show radius-server
Global RADIUS shared secret:********
retransmission count:1
timeout value:5
deadtime value:0
total number of servers:2

following RADIUS servers are configured:
        10.10.1.1:
                available for authentication on port:1812
                available for accounting on port:1813
        10.10.2.2:
                available for authentication on port:1812
                available for accounting on port:1813
```

This example shows how to display information for a specified RADIUS server:

```
switch# show radius-server 10.10.1.1
        10.10.1.1:
                available for authentication on port:1812
                available for accounting on port:1813
                idle time:0
                test user:test
                test password:********
```

This example shows how to display the RADIUS directed request configuration:

```
switch# show radius-server directed-request
enabled
```

This example shows how to display information for RADIUS server groups:

```
switch# show radius-server groups
total number of groups:2

following RADIUS server groups are configured:
        group radius:
                server: all configured radius servers
        group RadServer:
                deadtime is 0
                vrf is management
```

This example shows how to display information for a specified RADIUS server group:

```
switch# show radius-server groups RadServer
        group RadServer:
                deadtime is 0
                vrf is management
```

This example shows how to display sorted information for all RADIUS servers:

```
switch# show radius-server sorted
Global RADIUS shared secret:********
retransmission count:1
timeout value:5
deadtime value:0
total number of servers:2

following RADIUS servers are configured:
        10.10.0.0:
                available for authentication on port:1812
                available for accounting on port:1813
        10.10.1.1:
                available for authentication on port:1812
                available for accounting on port:1813
```

This example shows how to display statistics for a specified RADIUS server:

```
switch# show radius-server statistics 10.10.1.1
Server is not monitored

Authentication Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Accounting Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
```

Related Commands

Command	Description
show running-config radius	Displays the RADIUS information in the running configuration file.

show role

To display the user role configuration, use the **show role** command.

show role [**name** *role-name*]

Syntax Description

name *role-name*	(Optional) Displays information for a specific user role name. The role name is case sensitive.

Defaults

Displays information for all user roles.

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information for a specific user role:

```
switch(config)# show role name MyRole

role: MyRole
  description: new role
  vlan policy: deny
  permitted vlan
  1-10
  interface policy: deny
  permitted interface
  Ethernet2/1-8
  vrf policy: permit (default)
```

This example shows how to display information for all user roles in the default virtual device context (VDC):

```
switch(config)# show role

role: network-admin
  description: Predefined network admin role has access to all commands
  on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

role: network-operator
  description: Predefined network operator role has access to all read
  commands on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read

role: vdc-admin
  description: Predefined vdc admin role has access to all commands within
  a VDC instance
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

role: vdc-operator
  description: Predefined vdc operator role has access to all read commands
  within a VDC instance
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read

role: MyRole
  description: new role
  vlan policy: deny
  permitted vlan
  1-10
  interface policy: deny
  permitted interface
  Ethernet2/1-8
  vrf policy: permit (default)
```

This example shows how to display information for all user roles in a nondefault virtual device context (VDC):

```
switch-MyVDC# show role

role: vdc-admin
  description: Predefined vdc admin role has access to all commands within
  a VDC instance
  ----------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------------
  1       permit  read-write

role: vdc-operator
  description: Predefined vdc operator role has access to all read commands
  within a VDC instance
  ----------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------------
  1       permit  read
```

Related Commands

Command	Description
role name	Configures user roles.

show role feature

To display the user role features, use the **show role feature** command.

show role feature [**detail** | **name** *feature-name*]

Syntax Description

detail	(Optional) Displays detailed information for all features.
name *feature-name*	(Optional) Displays detailed information for a specific feature. The feature name is case sensitive.

Defaults

Displays a list of user role feature names.

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the user role features:

```
switch(config)# show role feature
feature: aaa
feature: access-list
feature: arp
feature: callhome
feature: cdp
feature: crypto
feature: gold
feature: install
feature: l3vm
feature: license
feature: ping
feature: platform
feature: qosmgr
feature: radius
feature: scheduler
feature: snmp
feature: syslog
<content deleted>
```

This example shows how to display detailed information for all the user role features:

```
switch(config)# show role feature detail
feature: aaa
  show aaa *
  config t ; aaa *
  aaa *
  clear aaa *
  debug aaa *
  show accounting *
  config t ; accounting *
  accounting *
  clear accounting *
  debug accounting *
feature: access-list
  show ip access-list *
  show ipv6 access-list *
  show mac access-list *
  show arp access-list *
  show vlan access-map *
  config t ; ip access-list *
  config t ; ipv6 access-list *
  config t ; mac access-list *
  config t ; arp access-list *
  config t ; vlan access-map *
  clear ip access-list *
  clear ipv6 access-list *
  clear mac access-list *
  clear arp access-list *
  clear vlan access-map *
  debug aclmgr *
feature: arp
  show arp *
  show ip arp *
  config t; ip arp *
  clear ip arp *
  debug ip arp *
  debug-filter ip arp *
<content deleted>
```

This example shows how to display detailed information for a specific user role feature:

```
switch(config)# show role feature name dot1x
feature: dot1x
  show dot1x *
  config t ; dot1x *
  dot1x *
  clear dot1x *
  debug dot1x *
```

Related Commands

Command	Description
role feature-group	Configures feature groups for user roles.
rule	Configures rules for user roles.

show role feature-group

To display the user role feature groups, use the **show role feature-group** command.

show role feature-group [**detail** | **name** *group-name*]

Syntax Description

detail	(Optional) Displays detailed information for all feature groups.
name *group-name*	(Optional) Displays detailed information for a specific feature group. The group name is case sensitive.

Defaults

Displays a list of user role feature groups.

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the user role feature groups:

```
switch(config)# show role feature-group

feature group: L3
feature: router-bgp
feature: router-eigrp
feature: router-isis
feature: router-ospf
feature: router-rip

feature group: SecGroup
feature: aaa
feature: radius
feature: tacacs
```

This example shows how to display detailed information about all the user role feature groups:

```
switch(config)# show role feature-group detail

feature group: L3
feature: router-bgp
  show bgp *
  config t ; bgp *
  bgp *
  clear bgp *
  debug bgp *
  show ip bgp *
  show ip mbgp *
  show ipv6 bgp *
  show ipv6 mbgp *
  clear ip bgp *
  clear ip mbgp *
  debug-filter ip *
  debug-filter ip bgp *
  config t ; router bgp *
feature: router-eigrp
  show eigrp *
  config t ; eigrp *
  eigrp *
  clear eigrp *
  debug eigrp *
  show ip eigrp *
  clear ip eigrp *
  debug ip eigrp *
  config t ; router eigrp *
feature: router-isis
  show isis *
  config t ; isis *
  isis *
  clear isis *
  debug isis *
  debug-filter isis *
  config t ; router isis *
feature: router-ospf
  show ospf *
  config t ; ospf *
  ospf *
  clear ospf *
  debug ospf *
  show ip ospf *
  show ospfv3 *
  show ipv6 ospfv3 *
  debug-filter ip ospf *
  debug-filter ospfv3 *
  debug ip ospf *
  debug ospfv3 *
  clear ip ospf *
  clear ip ospfv3 *
  config t ; router ospf *
  config t ; router ospfv3 *
feature: router-rip
  show rip *
  config t ; rip *
  rip *
  clear rip *
  debug rip *
  show ip rip *
  show ipv6 rip *
  overload rip *
```

```
debug-filter rip *
clear ip rip *
clear ipv6 rip *
config t ; router rip *
```

This example shows how to display information for a specific user role feature group:

```
switch(config)# show role feature-group name SecGroup

feature group: SecGroup
feature: aaa
feature: radius
feature: tacacs
```

Related Commands

Command	Description
role feature-group	Configures feature groups for user roles.
rule	Configures rules for user roles.

show role pending

To display the pending user role configuration differences for the Cisco Fabric Services distribution session, use the **show role pending** command.

show role pending

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays the user role configuration differences for the Cisco Fabric Services session:

```
switch# show role pending
Role: test-user
  Description: new role
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ----------------------------------------------------------------
  Rule    Perm    Type        Scope           Entity
  ----------------------------------------------------------------
  1       permit  read-write  feature             aaa
```

Related Commands

Command	Description
role distribute	Enables Cisco Fabric Services distribution for the user role configuration.

show role pending-diff

To display the differences between the pending user role configuration for the Cisco Fabric Services distribution session and the running configuration, use the **show role pending-diff** command.

show role pending-diff

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays the user role configuration differences for the Cisco Fabric Services session:

```
switch# show role pending
+Role: test-user
    +  Description: new role
    +  Vlan policy: permit (default)
    +  Interface policy: permit (default)
    +  Vrf policy: permit (default)
    +  ----------------------------------------------------------------
    +  Rule    Perm    Type        Scope           Entity

    +  ----------------------------------------------------------------
    +  1       permit  read-write  feature             aaa
```

Related Commands

Command	Description
role distribute	Enables Cisco Fabric Services distribution for the user role configuration.

show role session

To display the status information for a user role Cisco Fabric Services session, use the **show role session** command.

show role session status

Syntax Description

status	(Optional) Displays the role session status.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays the user role configuration differences for the Cisco Fabric Services session:

```
switch# show role session status
Last Action Time Stamp     : Thu Nov 20 12:43:26 2008
Last Action                : Distribution Enable
Last Action Result         : Success
Last Action Failure Reason : none
```

Related Commands

Command	Description
role distribute	Enables Cisco Fabric Services distribution for the user role configuration.

show role status

To display the status for the Cisco Fabric Services distribution for the user role feature, use the **show role status** command.

show role status

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays the user role configuration differences for the Cisco Fabric Services session:

```
switch# show role status
Distribution: Enabled
Session State: Locked
```

Related Commands

Command	Description
role distribute	Enables Cisco Fabric Services distribution for the user role configuration.

show running-config aaa

To display authentication, authorization, and accounting (AAA) configuration information in the running configuration, use the **show running-config aaa** command.

show running-config aaa [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the configured AAA information in the running configuration:

```
switch# show running-config aaa
version 4.0(1)
```

show running-config aclmgr

To display the user-configured access control lists (ACLs) in the running configuration, use the **show running-config aclmgr** command.

show running-config aclmgr [**all** | **inactive-if-config**]

Syntax Description

all	Displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.
inactive-if-config	Displays the inactive policies in the running configuration.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

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 display user-configured ACLs in the running configuration:

```
switch# show running-config aclmgr all
!Command: show running-config aclmgr all
!Time: Wed May 25 08:03:46 2011

version 5.2(1)
ip access-list acl1
ip access-list cisco123-copp-acl-bgp
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
ipv6 access-list cisco123-copp-acl-bgp6
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
ip access-list cisco123-copp-acl-cts
  10 permit tcp any any eq 64999
  20 permit tcp any eq 64999 any
ip access-list cisco123-copp-acl-dhcp
  10 permit udp any eq bootpc any
  20 permit udp any neq bootps any eq bootps
```

```
ip access-list cisco123-copp-acl-dhcp-relay-response
  10 permit udp any eq bootps any
  20 permit udp any any eq bootpc
ip access-list cisco123-copp-acl-eigrp
  10 permit eigrp any any
ip access-list cisco123-copp-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any
ip access-list cisco123-copp-acl-glbp
  10 permit udp any eq 3222 224.0.0.0/24 eq 3222
ip access-list cisco123-copp-acl-hsrp
  10 permit udp any 224.0.0.0/24 eq 1985
ipv6 access-list cisco123-copp-acl-hsrp6
  10 permit udp any ff02::66/128 eq 2029
ip access-list cisco123-copp-acl-icmp
  10 permit icmp any any echo
  20 permit icmp any any echo-reply
ipv6 access-list cisco123-copp-acl-icmp6
  10 permit icmp any any echo-request
  20 permit icmp any any echo-reply
ipv6 access-list cisco123-copp-acl-icmp6-msgs
  10 permit icmp any any router-advertisement
  20 permit icmp any any router-solicitation
  30 permit icmp any any nd-na
  40 permit icmp any any nd-ns
  50 permit icmp any any mld-query
  60 permit icmp any any mld-report
  70 permit icmp any any mld-reduction
ip access-list cisco123-copp-acl-igmp
  10 permit igmp any 224.0.0.0/3
mac access-list cisco123-copp-acl-mac-cdp-udld-vtp
  10 permit any 0100.0ccc.cccc 0000.0000.0000
mac access-list cisco123-copp-acl-mac-cfsoe
  10 permit any 0180.c200.000e 0000.0000.0000 0x8843
mac access-list cisco123-copp-acl-mac-dot1x
  10 permit any 0180.c200.0003 0000.0000.0000 0x888e
mac access-list cisco123-copp-acl-mac-fabricpath-isis
  10 permit any 0180.c200.0015 0000.0000.0000
  20 permit any 0180.c200.0014 0000.0000.0000
mac access-list cisco123-copp-acl-mac-flow-control
  10 permit any 0180.c200.0001 0000.0000.0000 0x8808
mac access-list cisco123-copp-acl-mac-gold
  10 permit any any 0x3737
mac access-list cisco123-copp-acl-mac-l2pt
  10 permit any 0100.0ccd.cdd0 0000.0000.0000
mac access-list cisco123-copp-acl-mac-lacp
  10 permit any 0180.c200.0002 0000.0000.0000 0x8809
mac access-list cisco123-copp-acl-mac-lldp
  10 permit any 0180.c200.000c 0000.0000.0000 0x88cc
mac access-list cisco123-copp-acl-mac-otv-isis
  10 permit any 0100.0cdf.dfdf 0000.0000.0000
mac access-list cisco123-copp-acl-mac-sdp-srp
  10 permit any 0180.c200.000e 0000.0000.0000 0x3401
mac access-list cisco123-copp-acl-mac-stp
  10 permit any 0100.0ccc.cccd 0000.0000.0000
  20 permit any 0180.c200.0000 0000.0000.0000
mac access-list cisco123-copp-acl-mac-undesirable
  10 permit any any
--More--
```

Related Commands

Command	Description
show running-config copp	Displays the CoPP configuration in the running configuration.
show startup-config aclmgr	Displays the user-configured ACLs in the startup configuration.
show startup-config copp	Displays the CoPP configuration in the startup configuration.

show running-config copp

To display control plane policing configuration information in the running configuration, use the **show running-config copp** command.

show running-config copp [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to display the configured control plane policing information in the running configuration:

```
switch# show running-config copp
version 4.0(1)
class-map type control-plane match-any copp-system-class-critical
  match access-group name copp-system-acl-arp
  match access-group name copp-system-acl-msdp
class-map type control-plane match-any copp-system-class-important
  match access-group name copp-system-acl-gre
  match access-group name copp-system-acl-tacas
class-map type control-plane match-any copp-system-class-normal
  match access-group name copp-system-acl-icmp
  match redirect dhcp-snoop
  match redirect arp-inspect
  match exception ip option
  match exception ip icmp redirect
  match exception ip icmp unreachable
```

```
policy-map type control-plane copp-system-policy
  class copp-system-class-critical
    police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform transmit exceed
transmit violate drop
  class copp-system-class-important
    police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform transmit exceed
transmit violate drop
  class copp-system-class-normal
    police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform transmit exceed
transmit violate drop
  class class-default
    police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform transmit exceed
transmit violate drop
```

This example shows how to display the configured and default control plane policing information in the running configuration:

```
switch# show running-config copp all
version 4.0(1)
class-map type control-plane match-any copp-system-class-critical
  match access-group name copp-system-acl-arp
  match access-group name copp-system-acl-msdp
class-map type control-plane match-any copp-system-class-important
  match access-group name copp-system-acl-gre
  match access-group name copp-system-acl-tacas
class-map type control-plane match-any copp-system-class-normal
  match access-group name copp-system-acl-icmp
  match redirect dhcp-snoop
  match redirect arp-inspect
  match exception ip option
  match exception ip icmp redirect
  match exception ip icmp unreachable
policy-map type control-plane copp-system-policy
  class copp-system-class-critical
    police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform transmit exceed
transmit violate drop
  class copp-system-class-important
    police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform transmit exceed
transmit violate drop
  class copp-system-class-normal
    police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform transmit exceed
transmit violate drop
  class class-default
    police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform transmit exceed
transmit violate drop
```

show running-config cts

To display the Cisco TrustSec configuration in the running configuration, use the **show running-config cts** command.

show running-config cts

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any configuration mode

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

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 cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec configuration in the running configuration:

```
switch# show running-config cts
version 4.0(1)
feature cts
cts role-based enforcement
cts role-based sgt-map 10.10.1.1 10
cts role-based access-list MySGACL
  permit icmp
cts role-based sgt 65535 dgt 65535 access-list MySGACL
cts sxp enable
cts sxp connection peer 10.10.3.3 source 10.10.2.2 password default mode listener
vlan 1
  cts role-based enforcement
vrf context MyVRF
  cts role-based enforcement
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show running-config dhcp

To display the Dynamic Host Configuration Protocol (DHCP) snooping configuration in the running configuration, use the **show running-config dhcp** command.

show running-config dhcp [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the DHCP snooping feature using the **feature dhcp** command.

This command does not require a license.

Examples

This example shows how to display the DHCP snooping configuration:

```
switch# show running-config dhcp
version 4.0(1)
feature dhcp

interface Ethernet2/46
  ip verify source dhcp-snooping-vlan
  ip arp inspection trust
ip dhcp snooping
ip arp inspection validate src-mac dst-mac ip
ip source binding 10.3.2.2 0f00.60b3.2333 vlan 13 interface Ethernet2/46
ip source binding 10.2.2.2 0060.3454.4555 vlan 100 interface Ethernet2/10
ip dhcp snooping vlan 1
ip arp inspection vlan 1
ip dhcp snooping vlan 13
ip arp inspection vlan 13

switch#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
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 ip dhcp snooping binding	Displays IP-MAC address bindings, including the static IP source entries.

show running-config dot1x

To display 802.1X configuration information in the running configuration, use the **show running-config dot1x** command.

show running-config dotx1 [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the 802.1X feature by using the **feature dot1x** command before using this command.

This command does not require a license.

Examples

This example shows how to display the configured 802.1X information in the running configuration:

```
switch# show running-config dot1x
version 4.0(1)
```

show running-config eou

To display the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) configuration information in the running configuration, use the **show running-config eou** command.

show running-config eou [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the EAPoUDP feature by using the **feature eou** command before using this command.

This command does not require a license.

Examples

This example shows how to display the configured EAPoUDP information in the running configuration:

```
switch# show running-config eou
version 4.0(1)
```

show running-config ldap

To display Lightweight Directory Access Protocol (LDAP) server information in the running configuration, use the **show running-config ldap** command.

show running-config ldap [**all**]

Syntax Description

all	(Optional) Displays default LDAP configuration information.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must use the **feature ldap** command before you can display LDAP information.

This command does not require a license.

Examples

This example shows how to display LDAP information in the running configuration:

```
switch# show running-config ldap
```

Related Commands

Command	Description
show ldap-server	Displays LDAP information.

show running-config port-security

To display port-security information in the running configuration, use the **show running-config port-security** command.

show running-config port-security [**all**]

Syntax Description

all	(Optional) Displays default port-security configuration information.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information for port-security in the running configuration:

```
switch# show running-port-security
version 4.0(3)
feature port-security
logging level port-security 5

interface Ethernet2/3
  switchport port-security
```

Related Commands

Command	Description
show startup-config port-security	Displays port-security information in the startup configuration.

show running-config radius

To display RADIUS server information in the running configuration, use the **show running-config radius** command.

show running-config radius [**all**]

Syntax Description

all	(Optional) Displays default RADIUS configuration information.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information for RADIUS in the running configuration:

```
switch# show running-config radius
```

Related Commands

Command	Description
show radius-server	Displays RADIUS information.

show running-config security

To display a user account, Secure Shell (SSH) server, and Telnet server information in the running configuration, use the **show running-config security** command.

show running-config security [**all**]

Syntax Description

all	(Optional) Displays the default user account, SSH server, and Telnet server configuration information.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display user account, SSH server, and Telnet server information in the running configuration:

```
switch# show running-config security
version 5.1(1)
username admin password 5 $1$7Jwq/LDM$XF0M/UWeT43DmtjZy8VP91  role network-admin
username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na.  role network-operator
username user1 password 5 $1$qEclQ5Rx$CAX9fXiAoFPYSvbVzpazj/  role network-operator
telnet server enable
ssh key rsa 1024 force
```

show running-config tacacs+

To display TACACS+ server information in the running configuration, use the **show running-config tacacs+** command.

show running-config tacacs+ [**all**]

Syntax Description

all	(Optional) Displays default TACACS+ configuration information.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you can display TACACS+ information.

This command does not require a license.

Examples

This example shows how to display TACACS+ information in the running configuration:

```
switch# show running-config tacacs+
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ information.

show ssh key

To display the Secure Shell (SSH) server key for a virtual device context (VDC), use the **show ssh key** command.

show ssh key

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command is available only when SSH is enabled using the **feature ssh** command.

This command does not require a license.

Examples

This example shows how to display the SSH server key:

```
switch# show ssh key
**************************************
rsa Keys generated:Wed Aug 11 11:45:14 2010

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDypfN6FSHZDbFPWEoz7sgWCamhfoqjqYNoZMvySSb4
056LhWZ75D90KPo+G+XTo7QAyQMpLJSkwKcRkidgD4lwJaDd/Ic/Sl5SJ3i0jyM61Bwvi+8+J3JoIdft
AvgH47GT5BdDD6hM7aUHq+efSQSq8pGyDAR4Cw6UdY9HNAWoTw==

bitcount:1024
fingerprint:
cd:8d:e3:0c:2a:df:58:d3:6e:9c:bd:72:75:3f:2e:45
**************************************
could not retrieve dsa key information
**************************************
```

Related Commands

Command	Description
ssh server key	Configures the SSH server key.

show ssh server

To display the Secure Shell (SSH) server status for a virtual device context (VDC), use the **show ssh server** command.

show ssh server

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the SSH server status:

```
switch# show ssh server
ssh is enabled
version 2 enabled
```

Related Commands

Command	Description
feature ssh	Enables the SSH server.

show startup-config aaa

To display authentication, authorization, and accouting (AAA) configuration information in the startup configuration, use the **show startup-config aaa** command.

show startup-config aaa

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the AAA information in the startup configuration:

```
switch# show startup-config aaa
version 4.0(1)
```

show startup-config aclmgr

To display the user-configured access control lists (ACLs) in the startup configuration, use the **show startup-config aclmgr** command.

show startup-config aclmgr [**all**]

Syntax Description

all	Displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

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 display the user-configured ACLs in the startup configuration:

```
switch(config)# show startup-config aclmgr all
!Command: show startup-config aclmgr all
!Time: Wed May 25 08:04:36 2011
!Startup config saved at: Mon May 23 05:44:16 2011

version 5.2(1)
ip access-list acl1
ip access-list copp-system-p-acl-bgp
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
ipv6 access-list copp-system-p-acl-bgp6
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
ip access-list copp-system-p-acl-cts
  10 permit tcp any any eq 64999
  20 permit tcp any eq 64999 any
ip access-list copp-system-p-acl-dhcp
  10 permit udp any eq bootpc any
  20 permit udp any neq bootps any eq bootps
```

```
ip access-list copp-system-p-acl-dhcp-relay-response
  10 permit udp any eq bootps any
  20 permit udp any any eq bootpc
ip access-list copp-system-p-acl-eigrp
  10 permit eigrp any any
ip access-list copp-system-p-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any
ip access-list copp-system-p-acl-glbp
  10 permit udp any eq 3222 224.0.0.0/24 eq 3222
ip access-list copp-system-p-acl-hsrp
  10 permit udp any 224.0.0.0/24 eq 1985
ipv6 access-list copp-system-p-acl-hsrp6
  10 permit udp any ff02::66/128 eq 2029
ip access-list copp-system-p-acl-icmp
  10 permit icmp any any echo
  20 permit icmp any any echo-reply
ipv6 access-list copp-system-p-acl-icmp6
  10 permit icmp any any echo-request
  20 permit icmp any any echo-reply
ipv6 access-list copp-system-p-acl-icmp6-msgs
  10 permit icmp any any router-advertisement
  20 permit icmp any any router-solicitation
  30 permit icmp any any nd-na
  40 permit icmp any any nd-ns
  50 permit icmp any any mld-query
  60 permit icmp any any mld-report
  70 permit icmp any any mld-reduction
ip access-list copp-system-p-acl-igmp
  10 permit igmp any 224.0.0.0/3
mac access-list copp-system-p-acl-mac-cdp-udld-vtp
  10 permit any 0100.0ccc.cccc 0000.0000.0000
mac access-list copp-system-p-acl-mac-cfsoe
  10 permit any 0180.c200.000e 0000.0000.0000 0x8843
mac access-list copp-system-p-acl-mac-dot1x
  10 permit any 0180.c200.0003 0000.0000.0000 0x888e
mac access-list copp-system-p-acl-mac-fabricpath-isis
  10 permit any 0180.c200.0015 0000.0000.0000
  20 permit any 0180.c200.0014 0000.0000.0000
mac access-list copp-system-p-acl-mac-flow-control
--More--
```

Related Commands

Command	Description
show running-config aclmgr	Displays the user-configured ACLs in the running configuration.
show running-config copp	Displays the CoPP configuration in the running configuration.
show startup-config copp	Displays the CoPP configuration in the startup configuration.

show startup-config copp

To display the Control Plane Policing (CoPP) configuration information in the startup configuration, use the **show startup-config copp** command.

show startup-config copp

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to display the control plane policing information in the startup configuration:

```
switch# show startup-config copp
version 4.0(1)
class-map type control-plane match-any MyClassMap
  match redirect dhcp-snoop
class-map type control-plane match-any copp-system-class-critical
  match access-group name copp-system-acl-arp
  match access-group name copp-system-acl-msdp
class-map type control-plane match-any copp-system-class-important
  match access-group name copp-system-acl-gre
  match access-group name copp-system-acl-tacas
class-map type control-plane match-any copp-system-class-normal
  match access-group name copp-system-acl-icmp
  match redirect dhcp-snoop
  match redirect arp-inspect
  match exception ip option
  match exception ip icmp redirect
  match exception ip icmp unreachable
```

```
policy-map type control-plane MyPolicyMap
  class MyClassMap
    police cir 0 bps bc 0 bytes conform drop violate drop
policy-map type control-plane copp-system-policy
  class copp-system-class-critical
    police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform transmit exceed
transmit violate drop
  class copp-system-class-important
    police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform transmit exceed
transmit violate drop
  class copp-system-class-normal
    police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform transmit exceed
transmit violate drop
  class class-default
    police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform transmit exceed
transmit violate drop
policy-map type control-plane x
  class class-default
    police cir 0 bps bc 0 bytes conform drop violate drop
```

show startup-config dhcp

To display the Dynamic Host Configuration Protocol (DHCP) snooping configuration in the startup configuration, use the **show startup-config dhcp** command.

show startup-config dhcp [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the DHCP snooping feature using the **feature dhcp** command.

This command does not require a license.

Examples

This example shows how to display the DHCP snooping configuration in the startup configuration:

```
switch# show startup-config dhcp
version 4.0(1)
feature dhcp

interface Ethernet2/46
  ip verify source dhcp-snooping-vlan
  ip arp inspection trust
ip dhcp snooping
ip arp inspection validate src-mac dst-mac ip
ip source binding 10.3.2.2 0f00.60b3.2333 vlan 13 interface Ethernet2/46
ip source binding 10.2.2.2 0060.3454.4555 vlan 100 interface Ethernet2/10
ip dhcp snooping vlan 1
ip arp inspection vlan 1
ip dhcp snooping vlan 13
ip arp inspection vlan 13

switch#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
show running-config dhcp	Shows DHCP snooping configuration in the running configuration.

show startup-config dot1x

To display 802.1X configuration information in the startup configuration, use the **show startup-config dot1x** command.

show startup-config dot1x

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the 802.1X feature by using the **feature dot1x** command before using this command.

This command does not require a license.

Examples

This example shows how to display the 802.1X information in the startup configuration:

```
switch# show startup-config dot1x
version 4.0(1)
```

show startup-config eou

To display the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) configuration information in the startup configuration, use the **show startup-config eou** command.

show startup-config eou

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the EAPoUDP feature by using the **feature eou** command before using this command.

This command does not require a license.

Examples

This example shows how to display the EAPoUDP information in the startup configuration:

```
switch# show startup-config eou
version 4.0(1)
```

show startup-config ldap

To display Lightweight Directory Access Protocol (LDAP) configuration information in the startup configuration, use the **show startup-config ldap** command.

show startup-config ldap

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must use the **feature ldap** command before you can display LDAP information.

This command does not require a license.

Examples

This example shows how to display the LDAP information in the startup configuration:

```
switch# show startup-config ldap
!Command: show startup-config ldap
!Time: Wed Feb 17 13:02:31 2010
!Startup config saved at: Wed Feb 17 10:32:23 2010

version 5.0(2)
feature ldap
aaa group server ldap LDAPgroup1
  no ldap-search-map
aaa group server ldap LdapServer1
  no ldap-search-map
```

Related Commands

Command	Description
show ldap-server	Displays LDAP information.

show startup-config port-security

To display port-security information in the startup configuration, use the **show startup-config port-security** command.

show startup-config port-security [**all**]

Syntax Description

all	(Optional) Displays default port-security configuration information.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information for port-security in the startup configuration:

```
switch# show startup-port-security
version 4.0(3)
feature port-security
logging level port-security 5

interface Ethernet2/3
  switchport port-security
```

Related Commands

Command	Description
show running-config port-security	Displays port-security information in the running configuration.

show startup-config radius

To display RADIUS configuration information in the startup configuration, use the **show startup-config radius** command.

show startup-config radius

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the RADIUS information in the startup configuration:

```
switch# show startup-config radius
version 4.0(1)
```

show startup-config security

To display user account, Secure Shell (SSH) server, and Telnet server configuration information in the startup configuration, use the **show startup-config security** command.

show startup-config security

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the user account, SSH server, and Telnet server information in the startup configuration:

```
switch# show startup-config security
version 5.1(1)
username admin password 5 $1$7Jwq/LDM$XF0M/UWeT43DmtjZy8VP91  role network-admin
username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na.  role network-operator
username user1 password 5 $1$qEclQ5Rx$CAX9fXiAoFPYSvbVzpazj/  role network-operator
telnet server enable
ssh key rsa 1024 force
```

show startup-config tacacs+

To display TACACS+ configuration information in the startup configuration, use the **show startup-config tacacs+** command.

show startup-config tacacs+

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the TACACS+ information in the startup configuration:

```
switch# show startup-config tacacs+
version 4.0(1)
```

show system internal pktmgr internal control sw-rate-limit

To display the inband and outband global rate limit configuration for packets that reach the supervisor module, use the **show system internal pktmgr internal control sw-rate-limit** command.

show system internal pktmgr internal control sw-rate-limit

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the inband and outband global rate limit configuration for packets that reach the supervisor module:

```
switch# show system internal pktmgr internal control sw-rate-limit
inband pps global threshold 12500  outband pps global threshold 15500
switch#
```

Related Commands

Command	Description
rate-limit cpu direction pps action log	Configures rate limits globally on the device for packets that reach the supervisor module.

show tacacs+

To display the TACACS+ Cisco Fabric Services (CFS) distribution status and other details, use the **show tacacs+** command.

show tacacs+ {**distribution status** | **pending** [**cmds**] | **pending-diff**}

Syntax Description

distribution status	Displays the status of the TACACS+ CFS distribution.
pending	Displays the pending configuration that is not yet applied to the running configuration.
cmds	(Optional) Displays the commands for the pending configuration.
pending-diff	Displays the difference between the active configuration and the pending configuration.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the TACACS+ CFS status:

```
switch# show tacacs+ distribution status
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: not yet initiated after enable

last operation: enable
last operation status: success
```

This example shows how to display the TACACS+ merge status:

```
switch# show tacacs+ merge status
Result: Waiting
```

This example shows how to display the pending TACACS+ configuration:

```
switch# show tacacs+ pending
tacacs-server host 10.10.2.2 key 7 qxz12345
```

This example shows how to display the pending TACACS+ configuration commands:

```
switch# show tacacs+ pending cmds
 tacacs-server host 10.10.2.2 key 7 qxz12345 port 49
```

This example shows how to display the differences between the pending TACACS+ configuration and the current TACACS+configuration:

```
switch# show tacacs+ pending-diff
    +tacacs-server host 10.10.2.2
```

show tacacs-server

To display TACACS+ server information, use the **show tacacs-server** command.

show tacacs-server [*hostname* | *ip4-address* | *ipv6-address*]
[**directed-request** | **groups** | **sorted** | **statistics**]

Syntax Description

hostname	(Optional) TACACS+ server Domain Name Server (DNS) name. The maximum character size is 256.
ipv4-address	(Optional) TACACS+ server IPv4 address in the *A.B.C.D* format.
ipv6-address	(Optional) TACACS+ server IPv6 address in the *X:X:X::X* format.
directed-request	(Optional) Displays the directed request configuration.
groups	(Optional) Displays information about the configured TACACS+ server groups.
sorted	(Optional) Displays sorted-by-name information about the TACACS+ servers.
statistics	(Optional) Displays TACACS+ statistics for the TACACS+ servers.

Defaults

Displays the global TACACS+ server configuration

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

TACACS+ preshared keys are not visible in the **show tacacs-server** command output. Use the **show running-config tacacs+** command to display the TACACS+ preshared keys.

You must use the **feature tacacs+** command before you can display TACACS+ information.

This command does not require a license.

Examples

This example shows how to display information for all TACACS+ servers:

```
switch# show tacacs-server
Global TACACS+ shared secret:********
timeout value:5
deadtime value:0
total number of servers:2

following TACACS+ servers are configured:
        10.10.2.2:
                available on port:49
        10.10.1.1:
                available on port:49
```

This example shows how to display information for a specified TACACS+ server:

```
switch# show tacacs-server 10.10.2.2
        10.10.2.2:
                available for authentication on port:1812
                available for accounting on port:1813
                idle time:0
                test user:test
                test password:********
```

This example shows how to display the TACACS+ directed request configuration:

```
switch# show tacacs-server directed-request
enabled
```

This example shows how to display information for TACACS+ server groups:

```
switch# show tacacs-server groups
total number of groups:1

following TACACS+ server groups are configured:
        group TacServer:
                server 10.10.2.2 on port 49
                deadtime is 0
                vrf is vrf3
```

This example shows how to display information for a specified TACACS+ server group:

```
switch# show tacacs-server groups TacServer
        group TacServer:
                server 10.10.2.2 on port 49
                deadtime is 0
                vrf is vrf3
```

This example shows how to display sorted information for all TACACS+ servers:

```
switch# show tacacs-server sorted
Global TACACS+ shared secret:********
timeout value:5
deadtime value:0
total number of servers:2

following TACACS+ servers are configured:
        10.10.1.1:
                available on port:49
        10.10.2.2:
                available on port:49
```

This example shows how to display statistics for a specified TACACS+ servers:

```
switch# show tacacs-server statistics 10.10.2.2
Server is not monitored

Authentication Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Authorization Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Accounting Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
```

Related Commands

Command	Description
show running-config tacacs+	Displays the TACACS+ information in the running configuration file.

show telnet server

To display the Telnet server status for a virtual device context (VDC), use the **show telnet server** command.

show telnet server

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the Telnet server status:

```
switch# show telnet server
telnet service enabled
```

Related Commands

Command	Description
telnet server enable	Enables the Telnet server.

show time-range

To display all time ranges or a specific time range, use the **show time-range** command.

show time-range [*time-range-name*]

Syntax Description

time-range-name	(Optional) Name of a time range, which can be up to 64 alphanumeric, case-sensitive characters.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The device shows all time ranges unless you use the *time-range-name* argument to specify a time range.

If you do not specify a time-range name, the device lists time ranges alphabetically by the time-range names.

The output of the **show time-range** command indicates whether a time range is active, which means that the current system time on the device falls within the configured time range.

This command does not require a license.

Examples

This example shows how to use the **show time-range** command without specifying a time-range name on a device that has two time ranges configured, where one of the time ranges is inactive and the other is active:

```
switch(config-time-range)# show time-range

time-range entry: december (inactive)
   10 absolute start 0:00:00 1 December 2009 end 11:59:59 31 December 2009
time-range entry: november (active)
   10 absolute start 0:00:00 1 November 2009 end 23:59:59 30 November 2009
```

Related Commands

Command	Description
time-range	Configures a time range.
permit (IPv4)	Configures a permit rule for an IPv4 ACL.
permit (IPv6)	Configures a permit rule for an IPv6 ACL.
permit (MAC)	Configures a permit rule for a MAC ACL.
show access-lists	Displays all ACLs or a specific ACL.

show user-account

To display information for the user accounts in a virtual device context (VDC), use the **show user-account** command.

show user-account

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information for user accounts in the default virtual device context (VDC):

```
switch# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:adminbackup
        this user account has no expiry date
        roles:network-operator
```

This example shows how to display information for user accounts in a nondefault VDC:

```
switch-MyVDC# show user-account
user:admin
        this user account has no expiry date
        roles:vdc-admin
```

Related Commands

Command	Description
telnet server enable	Enables the Telnet server.

show username

To display the public key for the specified user, use the **show username** command.

show username *username* **keypair**

Syntax Description

username	Name of the user. You can enter up to 28 alphanumeric characters.
keypair	Displays the Secure Shell (SSH) user keys.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

For security reasons, this command does not show the private key.

Examples

This example shows how to display the public key for the specified user:

```
switch# show username admin keypair
**************************************

rsa Keys generated:Mon Feb 15 08:10:45 2010

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEA0+rIeMgXwv004lt/hwOoyqIKbFGl1tmkFNm/tozuazfL
4dH/asAXZoJePDdiO1ILBGfrQgzyS5u3prXuXfgnWkTu0/4WlD0DF/EPdsd3NNzNbpPFzNDVylPDyDfR
X5SfVICioEirjX9Y59DZP+Nng6rJD7Z/YHVXs/jRNLPBOIs=

bitcount:262144
fingerprint:
a4:a7:b1:d1:43:09:49:6f:7c:f8:60:62:8e:a2:c1:d1
**************************************

could not retrieve dsa key information
**************************************
switch#
```

Related Commands

Command	Description
username *username* **keypair generate**	Generates the SSH public and private keys and stores them in the home directory of the Cisco NX-OS device for the specified user.

show users

To display the user session information for a virtual device context (VDC), use the **show users** command.

show users

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display user session information in the default virtual device context (VDC):

```
switch# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    pts/1        Mar 17 15:18   .          5477 (172.28.254.254)
admin    pts/9        Mar 19 11:19   .         23101 (10.82.234.56)*
```

This example shows how to display information for user accounts in a nondefault VDC:

```
switch-MyVDC# show users
admin     pts/10       Mar 19 12:54   .         30965 (10.82.234.56)*
```

Related Commands

Command	Description
username	Configures user accounts.

show vlan access-list

To display the contents of the IPv4 access control list (ACL), IPv6 ACL, or MAC ACL associated with a specific VLAN access map, use the **show vlan access-list** command.

show vlan access-list *access-list-name*

Syntax Description

access-list-name	Name of the VLAN access map, which can be up to 64 alphanumeric, case-sensitive characters.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to use the **show vlan access-list** command to display the contents of the ACL that the VLAN access map named vacl-01 is configured to use:

```
switch# show vlan access-list vacl-01

IP access list ipv4acl
        5 deny ip 10.1.1.1/32 any
        10 permit ip any any
```

Related Commands

Command	Description
vlan access-map	Configures an VLAN access map.
show access-lists	Displays all ACLs or a specific ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.
show vlan access-map	Displays all VLAN access maps or a specific VLAN access map.

show vlan access-map

To display all VLAN access maps or a VLAN access map, use the **show vlan access-map** command.

show vlan access-map *map-name*

Syntax Description

map-name	VLAN access map, which can be up to 64 alphanumeric, case-sensitive characters.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.2(1)	Command output is sorted alphabetically by the ACL names.
4.0(1)	This command was introduced.

Usage Guidelines

The device shows all VLAN access maps, unless you use the *map-name* argument to specify an access map.

If you do not specify an access-map name, the device lists VLAN access maps alphabetically by access-map name.

For each VLAN access map displayed, the device shows the access-map name, the ACL specified by the **match** command, and the action specified by the **action** command.

Use the **show vlan filter** command to see which VLANs have a VLAN access map applied to them.

This command does not require a license.

Examples

This example shows how to remove dynamically learned, secure MAC addresses from the Ethernet 2/1 interface:

```
switch# show vlan access-map

Vlan access-map austin-vlan-map

        match ip: austin-corp-acl
        action: forward
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

show vlan filter

To display information about instances of the **vlan filter** command, including the VLAN access-map and the VLAN IDs affected by the command, use the **show vlan filter** command.

show vlan filter [**access-map** *map-name* | **vlan** *vlan-ID*]

Syntax Description

access-map *map-name*	(Optional) Limits the output to VLANs that the specified access map is applied to.
vlan *vlan-ID*	(Optional) Limits the output to access maps that are applied to the specified VLAN only. Valid VLAN IDs are from 1 to 4096.

Defaults

The device shows all instances of VLAN access maps applied to a VLAN, unless you use the **access-map** keyword and specify an access map, or you use the **vlan** keyword and specify a VLAN ID.

Command Modes

Any command mode

SupportedUserRoles

network-admin
network-operator
vdc-admin
vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display all VLAN access map information on a device that has only one VLAN access map applied (austin-vlan-map) to VLANs 20 through 35 and 42 through 80:

```
switch# show vlan filter

vlan map austin-vlan-map:
        Configured on VLANs:    20-35,42-80
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.

Command	Description
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.