



Cisco IOS Security Command Reference: Commands S to Z, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)

First Published: January 11, 2013

Last Modified: January 11, 2013

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

CHAPTER 1

sa ipsec through sessions maximum 1

- server_(Diameter) 2
- server (RADIUS) 4
- server name (IPv6 TACACS+) 7
- server-private (RADIUS) 8
- server-private (TACACS+) 11
- service password-encryption 14
- service password-recovery 16

CHAPTER 2

set aggressive-mode client-endpoint through show content-scan 23

- show aaa servers 24
- show access-lists 32
- show authentication interface 35
- show authentication registrations 37
- show authentication sessions 39

CHAPTER 3

show diameter peer through show object-group 45

- show dot1x 46
- show ip access-lists 50
- show ip admission 54
- show ip ssh 60
- show ipv6 access-list 61
- show mab 65
- show mac-address-table 67

CHAPTER 4

show parameter-map type consent through show users 79

- show port-security 80
- show privilege 82

[show radius statistics](#) 83

[show ssh](#) 89

CHAPTER 5

[show vlan group through switchport port-security violation](#) 91

[single-connection](#) 92

[source](#) 93

[ssh](#) 95

[switchport port-security](#) 100

CHAPTER 6

[tacacs-server administration through title-color](#) 103

[tacacs server](#) 104

[tacacs-server host](#) 106

[telnet](#) 109

[test aaa group](#) 115

[timeout \(TACACS+\)](#) 119

CHAPTER 7

[traffic-export through zone security](#) 121

[username](#) 122

[username secret](#) 129



sa ipsec through sessions maximum

- [server_\(Diameter\), page 2](#)
- [server \(RADIUS\), page 4](#)
- [server name \(IPv6 TACACS+\), page 7](#)
- [server-private \(RADIUS\), page 8](#)
- [server-private \(TACACS+\), page 11](#)
- [service password-encryption, page 14](#)
- [service password-recovery, page 16](#)

server_(Diameter)

To associate a Diameter server with a Diameter authentication, authorization, and accounting (AAA) server group, use the **server** command in Diameter server group configuration submode. To remove a server from the server group, enter the **no** form of this command.

server *name*

no server *name*

Syntax Description

<i>name</i>	Character string used to name the Diameter server.
Note	The name specified for this command should match the name of a Diameter peer defined using the diameter peer command.

Command Default

No server is associated with a Diameter AAA server group.

Command Modes

Diameter server group configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The **server** command allows you to associate a Diameter server with a Diameter server group.

Examples

The following example shows how to associate a Diameter server with a Diameter server group:

```
Router (config-sg-diameter)# server
dia_peer_1
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication login	Set AAA authentication at login.
aaa authorization	Sets parameters that restrict user access to a network.

Command	Description
aaa group server diameter	Configures a server group for Diameter.

server (RADIUS)

To configure the IP address of the RADIUS server for the group server, use the **server** command in server-group configuration mode. To remove the associated server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

no server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

Syntax Description

<i>ip-address</i>	IP address of the RADIUS server host.
auth-port <i>port-number</i>	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests. The <i>port-number</i> argument specifies the port number for authentication requests. The host is not used for authentication if this value is set to 0.
acct-port <i>port-number</i>	(Optional) Specifies the UDP destination port for accounting requests. The <i>port-number</i> argument specifies the port number for accounting requests. The host is not used for accounting services if this value is set to 0.

Command Default

If no port attributes are defined, the defaults are as follows:

- Authentication port: 1645
- Accounting port: 1646

Command Modes

Server-group configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(7)T	The following new keywords/arguments were added: <ul style="list-style-type: none"> • auth-port <i>port-number</i> • acct-port <i>port-number</i>
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **server** command to associate a particular server with a defined group server. There are two different ways in which you can identify a server, depending on the way you want to offer AAA services. You can identify the server simply by using its IP address, or you can identify multiple host instances or entries using the optional **auth-port** and **acct-port** keywords.

When you use the optional keywords, the network access server identifies RADIUS security servers and host instances associated with a group server on the basis of their IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS host entries providing a specific AAA service. If two different host entries on the same RADIUS server are configured for the same service--for example, accounting--the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order they are configured.)

Examples

Examples

The following example shows the network access server configured to recognize several RADIUS host entries with the same IP address. Two different host entries on the same RADIUS server are configured for the same services--authentication and accounting. The second host entry configured acts as fail-over backup to the first one. (The RADIUS host entries are tried in the order in which they are configured.)

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default radius
! The next set of commands configures multiple host entries for the same IP address.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 2000 acct-port 2000
```

Examples

In this example, the network access server is configured to recognize two different RADIUS group servers. One of these groups, group1, has two different host entries on the same RADIUS server configured for the same services. The second host entry configured acts as failover backup to the first one.

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS group server and associates servers
! with it.
aaa group server radius group1
    server 172.20.0.1 auth-port 1000 acct-port 1001
! The following commands define the group2 RADIUS group server and associates servers
! with it.
aaa group server radius group2
    server 172.20.0.1 auth-port 2000 acct-port 2001
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined group servers.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
```

```
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.31.0.1 auth-port 1645 acct-port 1646
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

server name (IPv6 TACACS+)

To specify an IPv6 TACACS+ server, use the **server name** command in TACACS+ group server configuration mode. To remove the IPv6 TACACS+ server from configuration, use the **no** form of this command.

server name *server-name*

no server name *server-name*

Syntax Description

server-name	The IPv6 TACACS+ server to be used.
-------------	-------------------------------------

Command Default

No server name is specified.

Command Modes

TACACS+ group server configuration (config-sg-tacacs+)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

You must configure the **aaa group server tacacs** command before configuring this command.

Enter the **server name** command to specify an IPv6 TACACS+ server.

Examples

The following example shows how to specify an IPv6 TACACS+ server named server1:

```
Router(config)# aaa group server tacacs+
Router(config-sg-tacacs+)# server name server1
```

Related Commands

Command	Description
aaa group server tacacs	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

server-private (RADIUS)

To configure the IP address of the private RADIUS server for the group server, use the **server-private** command in server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server-private *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

no server-private *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

Syntax Description

<i>ip-address</i>	IP address of the private RADIUS server host.
auth-port <i>port-number</i>	(Optional) User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645.
acct-port <i>port-number</i>	(Optional) UDP destination port for accounting requests. The default value is 1646.
non-standard	(Optional) RADIUS server is using vendor-proprietary RADIUS attributes.
timeout <i>seconds</i>	(Optional) Time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the radius-server timeout command. If no timeout value is specified, the global value is used.
retransmit <i>retries</i>	(Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the radius-server retransmit command.
key <i>string</i>	(Optional) Authentication and encryption key used between the router and the RADIUS daemon running on the RADIUS server. This key overrides the global setting of the radius-server key command. If no key string is specified, the global value is used.

Command Default

If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between Virtual Route Forwardings (VRFs), private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default "radius" server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

**Note**

If the **radius-server directed-request** command is configured, then a private RADIUS server cannot be used as the group server by configuring the **server-private (RADIUS)** command.

Examples

The following example shows how to define the sg_water RADIUS group server and associate private servers with it:

```
aaa group server radius sg_water
 server-private 10.1.1.1 timeout 5 retransmit 3 key xyz
 server-private 10.2.2.2 timeout 5 retransmit 3 key xyz
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-mode l	Enables the AAA access control model.

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server directed-request	Allows users logging into a Cisco network access server (NAS) to select a RADIUS server for authentication.

server-private (TACACS+)

To configure the IPv4 or IPv6 address of the private TACACS+ server for the group server, use the **server-private** command in server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server-private {*ip-address*| *name*| *ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [0 | 7] *string*]

no server-private

Syntax Description

<i>ip-address</i>	IP address of the private RADIUS or TACACS+ server host.
<i>name</i>	Name of the private RADIUS or TACACS+ server host.
<i>ipv6-address</i>	IPv6 address of the private RADIUS or TACACS+ server host.
nat	(Optional) Specifies the port Network Address Translation (NAT) address of the remote device. This address is sent to the TACACS+ server.
single-connection	(Optional) Maintains a single open connection between the router and the TACACS+ server.
port <i>port-number</i>	(Optional) Specifies a server port number. This option overrides the default, which is port 49.
timeout <i>seconds</i>	(Optional) Specifies a timeout value. This value overrides the global timeout value set with the tacacs-server timeout command for this server only.
key [0 7]	(Optional) Specifies an authentication and encryption key. This key must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global tacacs-server key command for this server only. <ul style="list-style-type: none"> If no number or 0 is entered, the string that is entered is considered to be plain text. If 7 is entered, the string that is entered is considered to be encrypted text.
<i>string</i>	(Optional) Character string specifying the authentication and encryption key.

Command Default If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

Command Modes Server-group configuration (server-group)

Command History	Release	Modification
	12.3(7)T	This command was introduced.
	12.2(33)SRA1	This command was integrated into Cisco IOS Release 12.2(33)SRA1.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
	12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.
	Cisco IOS XE Release 3.2S	This command was modified. The <i>ipv6-address</i> argument was added.

Usage Guidelines Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between virtual route forwardings (VRFs), private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default "TACACS+" server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

Examples The following example shows how to define the tacacs1 TACACS+ group server and associate private servers with it:

```
aaa group server tacacs+ tacacs1
  server-private 10.1.1.1 port 19 key cisco
  ip vrf cisco
  rd 100:1
  interface Loopback0
  ip address 10.0.0.2 255.0.0.0
  ip vrf forwarding cisco
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-mode l	Enables the AAA access control model.

Command	Description
ip tacacs source-interface	Uses the IP address of a specified interface for all outgoing TACACS+ packets.
ip vrf forwarding (server-group)	Configures the VRF reference of an AAA RADIUS or TACACS+ server group.
tacacs-server host	Specifies a TACACS+ server host.

service password-encryption

To encrypt passwords, use the **service password-encryption** command in global configuration mode. To restore the default, use the **no** form of this command.

service password-encryption

no service password-encryption

Syntax Description This command has no arguments or keywords.

Command Default No passwords are encrypted.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines The actual encryption process occurs when the current configuration is written or when a password is configured. Password encryption is applied to all passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords, and Border Gateway Protocol neighbor passwords. This command is primarily useful for keeping unauthorized individuals from viewing your password in your configuration file.

When password encryption is enabled, the encrypted form of the passwords is displayed when a **more system:running-config** command is entered.



Caution

This command does not provide a high level of network security. If you use this command, you should also take additional network security measures.



Note

You cannot recover a lost encrypted password. You must clear NVRAM and set a new password.

Examples

The following example causes password encryption to take place:

```
service password-encryption
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
key-string (authentication)	Specifies the authentication string for a key.
neighbor password	Enables MD5 authentication on a TCP connection between two BGP peers.

service password-recovery

To enable password recovery capability, use the **service password-recovery** command in global configuration mode. To disable password recovery capability, use the **no service password-recovery** command.

service password-recovery

no service password-recovery

Syntax Description This command has no arguments or keywords.

Command Default Password recovery capability is enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.3(8)YA	This command was introduced.
	12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Note

This command is not available on all platforms. Use Feature Navigator to ensure that it is available on your platform.

If you plan to disable the password recovery capability with the **no service password-recovery** command, we recommend that you save a copy of the system configuration file in a location away from the device. If you are using a device that is operating in VTP transparent mode, we recommend that you also save a copy of the vlan.dat file in a location away from the device.



Caution

Entering the **no service password-recovery** command at the command line disables password recovery. Always disable this command before downgrading to an image that does not support password recovery capability, because you cannot recover the password after the downgrade.

The configuration register boot bit must be enabled so that there is no way to break into ROMMON when this command is configured. Cisco IOS software should prevent the user from configuring the boot field in the config register.

Bit 6, which ignores the startup configuration, and bit 8, which enables a break should be set.

The Break key should be disabled while the router is booting up and disabled in Cisco IOS software when this feature is enabled.

It may be necessary to use the **config-register** global configuration command to set the configuration register to autoboot *before* entering the **no service password-recovery** command. The last line of the **show version** EXEC command displays the configuration register setting. Use the **show version** EXEC command to obtain the current configuration register value, configure the router to autoboot with the **config-register** command if necessary, then enter the **no service password-recovery** command.

Once disabled, the following configuration register values are *invalid* for the **no service password-recovery** command:

- 0x0
- 0x2002 (bit 8 restriction)
- 0x0040 (bit 6)
- 0x8000 (bit 15)

Catalyst Switch Operation

Use the **service password-recovery** command to reenable the password-recovery mechanism (the default). This mechanism allows a user with physical access to the switch to hold down the **Mode** button and interrupt the boot process while the switch is powering up and to assign a new password. Use the **no** form of this command to disable the password-recovery capability.

When the password-recovery mechanism is disabled, interrupting the boot process is allowed only if the user agrees to set the system back to the default configuration. Use the **show version** EXEC command to verify if password recovery is enabled or disabled on a switch.

The **service password-recovery** command is valid only on Catalyst 3550 Fast Ethernet switches; it is not available for Gigabit Ethernet switches.

Examples

Examples

The following example shows how to obtain the configuration register setting (which in this example is set to autoboot), disable the password-recovery capability, and then verify that the configuration persists through a system reload. The **noconfirm** keyword prevents a confirmation prompt from interrupting the booting process.

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 5300 Software (C7200-P-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Wed 05-Mar-03 10:16 by xxx
Image text-base: 0x60008954, data-base: 0x61964000
ROM: System Bootstrap, Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
BOOTLDR: 7200 Software (C7200-KBOOT-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
Router uptime is 10 minutes
System returned to ROM by reload at 16:28:11 UTC Thu Mar 6 2003
.
.
.
125440K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2012
Router# configure terminal
Router(config)# no service password-recovery noconfirm
WARNING:
```

Executing this command will disable the password recovery mechanism.
Do not execute this command without another plan for password recovery.
Are you sure you want to continue? [yes/no]: **yes**

```
.
.
Router(config)# exit
Router#
Router# reload
Proceed with reload? [confirm] yes
00:01:54: %SYS-5-RELOAD: Reload requested
System Bootstrap, 12.3(8)YA...
Copyright (c) 1994-2004 by Cisco Systems, Inc.
C7400 platform with 262144 Kbytes of main memory
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
.
.
.
```

The following example shows what happens when a break is confirmed and when a break is not confirmed.

Examples

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x80013000, size: 0x8396a8
Self decompressing the image :
#####
[OK] !The 5-second window starts.
telnet> send break

Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco IOS Software, C831 Software (C831-K903SY6-M), Version 12.3(8)YA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 13-Aug-04 03:21
Image text-base: 0x80013200, data-base: 0x81020514
PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to factory default configuration and proceed [y/n]?
!The user enters "y" here.
Reset router configuration to factory default.
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for compliance with U.S. and
local country laws. By using this product you agree to comply with applicable laws and
regulations. If you are unable to comply with U.S. and local laws, return this product
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco C831 (MPC857DSL) processor (revision 0x00) with 46695K/2457K bytes of memory.
Processor board ID 0000 (1314672220), with hardware revision 0000 CPU rev number 7
3 Ethernet interfaces
4 FastEthernet interfaces
128K bytes of NVRAM
24576K bytes of processor board System flash (Read/Write)
2048K bytes of processor board Web flash (Read/Write)
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
!Start up config is erased.
SETUP: new interface FastEthernet1 placed in "up" state
SETUP: new interface FastEthernet2 placed in "up" state
SETUP: new interface FastEthernet3 placed in "up" state
SETUP: new interface FastEthernet4 placed in "up" state
Press RETURN to get started!
Router> enable
Router# show startup configuration
startup-config is not present
```

```
Router# show running-config | incl service
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption !The "no service password-recovery" is disabled.
=====
```

Examples

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
telnet> send break
program load complete, entry point: 0x80013000, size: 0x8396a8
Self decompressing the image :
=====
[OK]
telnet> send break
Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco IOS Software, C831 Software (C831-K9O3SY6-M), Version 12.3(8)YA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 13-Aug-04 03:21
Image text-base: 0x80013200, data-base: 0x81020514
PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to factory default configuration and proceed [y/n]?
!The user enters "n" here.
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for compliance with U.S. and
local country laws. By using this product you agree to comply with applicable laws and
regulations. If you are unable to comply with U.S. and local laws, return this product
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco C831 (MPC857DSL) processor (revision 0x00) with 46695K/2457K bytes of memory.
Processor board ID 0000 (1314672220), with hardware revision 0000 CPU rev number 7
3 Ethernet interfaces
4 FastEthernet interfaces
128K bytes of NVRAM
24576K bytes of processor board System flash (Read/Write)
2048K bytes of processor board Web flash (Read/Write)
Press RETURN to get started! !The Cisco IOS software boots as if it is not interrupted.
Router> enable
Router# show startup configuration
Using 984 out of 131072 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service password-recovery
!
hostname Router
!
boot-start-marker
boot-end-marker
!
memory-size iomem 5
!
no aaa new-model
ip subnet-zero
!
ip ips po max-events 100
no ftp-server write-enable
```

```

!
interface Ethernet0
 no ip address
 shutdown
!
interface Ethernet1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet2
 no ip address
 shutdown
!
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet3
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet4
 no ip address
 duplex auto
 speed auto
!
ip classless
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
 no modem enable
 transport preferred all
 transport output all
line aux 0
line vty 0 4
!
scheduler max-task-time 5000
end
Router# show running-configuration | incl service
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service password-recovery

```

Examples

The **no service password-recovery** command expects the router configuration register to be configured to autoboot. If the configuration register is set to something other than to autoboot *before* the **no service password-recovery** command is entered, a prompt like the one shown in the following example asking you to use the **config-register** global configuration command to change the setting.

```

Router(config)# no service password-recovery
Please setup auto boot using config-register first.

```


**Note**

To avoid any unintended result due to the behavior of this command, use the **show version** command to obtain the current configuration register value. If not set to autoboot, then the router needs to be configured to autoboot with the **config-register** command before entering the **no service password-recovery** command.

Once password recovery is disabled, you cannot set the bit pattern value to 0x40, 0x8000, or 0x0 (disables autoboot). The following example shows the messages displayed when invalid configuration register settings are attempted on a router with password recovery disabled.

```
Router(config)# config-register 0x2143
Password recovery is disabled, cannot enable diag or ignore configuration.
The command resets the invalid bit pattern and continue to allow modification of nonrelated bit patterns. The
configuration register value resets to 0x3 at the next system reload, which can be verified by checking the last
line of the show version command output:
```

```
Configuration register is 0x2012 (will be 0x3 at next reload)
```

Examples

The following example shows how to disable password recovery on a switch so that a user can only reset a password by agreeing to return to the default configuration:

```
Switch(config)# no service-password recovery
Switch(config)# exit
```

To use the password-recovery procedure, a user with physical access to the switch holds down the **Mode** button while the unit powers up and for a second or two after the LED above port 1X goes off. When the button is released, the system continues with initialization. If the password-recovery mechanism is disabled, the following message is displayed:

```
The password-recovery mechanism has been triggered, but is currently disabled. Access to
the boot loader prompt through the password-recovery mechanism is disallowed at this point.
However, if you agree to let the system be reset back to the default system configuration,
access to the boot loader prompt can still be allowed.
```

```
Would you like to reset the system back to the default configuration (y/n)?
```

If you choose not to reset the system back to the default configuration, the normal boot process continues, as if the **Mode** button had not been pressed. If you choose to reset the system back to the default configuration, the configuration file in flash memory is deleted and the VLAN database file, flash:vlan.dat (if present), is deleted.

The following is sample output from the **show version** command on a device when password recovery is disabled:

```
Switch# show version
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 24-Oct-01 06:20 by xxx
Image text-base: 0x00003000, data-base: 0x004C1864
ROM: Bootstrap program is C3550 boot loader
flam-1-6 uptime is 1 week, 6 days, 3 hours, 59 minutes
System returned to ROM by power-on
Cisco WS-C3550-48 (PowerPC) processor with 65526K/8192K bytes of memory.
Last reset from warm-reset
Running Layer2 Switching Only Image
Ethernet-controller 1 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 2 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 3 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 4 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 5 has 1 Gigabit Ethernet/IEEE 802.3 interface
Ethernet-controller 6 has 1 Gigabit Ethernet/IEEE 802.3 interface
```

```
48 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
The password-recovery mechanism is disabled.
32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: AA:00:0B:2B:02:00
Configuration register is 0x10F
```

Related Commands

Command	Description
config-register	Changes the configuration register settings.
show version	Displays version information for the hardware and firmware.



set aggressive-mode client-endpoint through show content-scan

- [show aaa servers, page 24](#)
- [show access-lists, page 32](#)
- [show authentication interface, page 35](#)
- [show authentication registrations, page 37](#)
- [show authentication sessions, page 39](#)

show aaa servers

To display the status and number of packets that are sent to and received from all public and private authentication, authorization, and accounting (AAA) RADIUS servers as interpreted by the AAA Server MIB, use the **show aaa servers** command in user EXEC or privileged EXEC mode.

show aaa servers [**private**| **public**]

Syntax Description

private	(Optional) Displays private AAA servers only, which are also displayed by the AAA Server MIB.
public	(Optional) Displays public AAA servers only, which are also displayed by the AAA Server MIB.

Command Modes

User EXEC (>) privileged EXEC (#)

Command History

Release	Modification
12.2(6)T	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)S	This command was modified. Support for private RADIUS servers in CISCO-AAA-SERVER-MIB was added.
15.1(4)M	This command was modified. Support for private RADIUS servers in CISCO-AAA-SERVER-MIB was added.
15.2(4)S1	This command was modified. Support for displaying the estimated outstanding and throttled transactions (access and accounting) in the command output was added.

Usage Guidelines

Only RADIUS servers are supported by the **show aaa servers** command.

The command displays information about packets sent and received for all AAA transaction types--authentication, authorization, and accounting.

Examples

The following is sample output from the **show aaa servers private** command. Only the first four lines of the display pertain to the status of private RADIUS servers, and the output fields in this part of the display are described in the table below.

```
Router# show aaa servers private

RADIUS: id 24, priority 1, host 172.31.164.120, auth-port 1645, acct-port 1646
  State: current UP, duration 375742s, previous duration 0s
  Dead: total time 0s, count 0
  Quarantined: No
  Authen: request 5, timeouts 1, failover 0, retransmission 1
    Response: accept 4, reject 0, challenge 0
    Response: unexpected 0, server error 0, incorrect 0, time 14ms
    Transaction: success 4, failure 0
    Throttled: transaction 0, timeout 0, failure 0
  Author: request 0, timeouts 0, failover 0, retransmission 0
    Response: accept 0, reject 0, challenge 0
    Response: unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction: success 0, failure 0
    Throttled: transaction 0, timeout 0, failure 0
  Account: request 5, timeouts 0, failover 0, retransmission 0
    Request: start 3, interim 0, stop 2
    Response: start 3, interim 0, stop 2
    Response: unexpected 0, server error 0, incorrect 0, time 12ms
    Transaction: success 5, failure 0
    Throttled: transaction 0, timeout 0, failure 0
  Elapsed time since counters last cleared: 4d8h22m
  Estimated Outstanding Access Transactions: 0
  Estimated Outstanding Accounting Transactions: 0
  Estimated Throttled Access Transactions: 0
  Estimated Throttled Accounting Transactions: 0
  Maximum Throttled Transactions: access 0, accounting 0
  Requests per minute past 24 hours:
    high - 8 hours, 22 minutes ago: 0
    low - 8 hours, 22 minutes ago: 0
    average: 0
```

The table below describes the significant fields in the display.

Table 1: show aaa servers Field Descriptions

Field	Description
id	A unique identifier for all AAA servers defined on the router.
priority	Order of use for servers within a group.
host	IP address of the private RADIUS server host.
auth-port	UDP destination port on the AAA server that is used for authentication and authorization requests. The default value is 1645.
acct-port	UDP destination port on the AAA server that is used for accounting requests. The default value is 1646.

Field	Description
State	<p>Describes the current state of the AAA server; the duration, in seconds, that the server has been in that state; and the duration, in seconds, that the server was in the previous state.</p> <p>The following states are possible:</p> <ul style="list-style-type: none">• DEAD--Indicates that the server is currently down and, in the case of failovers, this server will be omitted unless it is the last server in the group.• duration--Indicates the amount of time the server is assumed to be in the current state, either UP or DEAD.• previous duration--Indicates the amount of time the server was considered to be in the previous state.• UP--Indicates that the server is currently considered alive and attempts will be made to communicate with it.
Dead	<p>Indicates the number of times that this server has been marked dead, and the cumulative amount of time, in seconds, that it spent in that state.</p>

Field	Description
Authen	

Field	Description
	<p>Provides information about authentication packets that were sent to and received from the server, and authentication transactions that were successful or that failed. The following information may be reported in this field:</p> <ul style="list-style-type: none"> • request--Number of authentication requests that were sent to the AAA server. • timeouts--Number of timeouts (no responses) that were observed when a transmission was sent to this server. • Response--Provides statistics about responses that were observed from this server and includes the following reports: <ul style="list-style-type: none"> • unexpected--Number of unexpected responses. A response is considered unexpected when it is received after the timeout period for the packet has expired. This may happen if the link to the server is severely congested, for example. An unexpected response can also be produced when a server generates a response for no apparent reason. • server error--Number of server errors. This category is a “catchall” for error packets that do not fall into one of the previous categories. • incorrect--Number of incorrect responses. A response is considered incorrect if it is of the wrong format than the one expected by the protocol. This frequently happens when an incorrect server key is configured on the router. • time--Time (in milliseconds) taken to respond to an authentication packets. • Transaction: These fields provide information about authentication, authorization, and accounting transactions related to the server. A transaction is defined as a request for authentication, authorization, or accounting information that is sent by the AAA module, or by an AAA client (such as PPP) to an AAA protocol (RADIUS or TACACS+), which may involve multiple packet transmissions and retransmissions. Transactions may require

Field	Description
	<p>packet retransmissions to one or more servers in a single server group, to verify success or failure. Success or failure is reported to AAA by the RADIUS and TACACS+ protocols as follows</p> <ul style="list-style-type: none"> • success--Incremented when a transaction is successful. • failure--Incremented when a transaction fails; for example, packet retransmissions to another server in the server group failed or did not succeed. A negative response to an Access-Request, such as Access-Reject, is considered to be a successful transaction.
Author	The fields in this category are similar to those in the Authen: fields. An important difference, however, is that because authorization information is carried in authentication packets for the RADIUS protocol, these fields are not incremented when using RADIUS.
Account	The fields in this category are similar to those in the Authen: fields, but provide accounting transaction and packet statistics.
Elapsed time since counters last cleared	Displays the time in days, hours, and minutes that have passed since the counters were last cleared.

**Note**

In case of Intelligent Services Gateway (ISG), the estimated outstanding accounting transactions will take some time to become zero. This is because there is a constant churn in the interim accounting requests.

The fields in the output of the **show aaa servers** command are mapped to Simple Network Management Protocol (SNMP) objects in the Cisco AAA-SERVER-MIB and are used in SNMP reporting. The first line of the sample output of the **show aaa servers** command (RADIUS: id 24, priority 1, host 172.31.164.120, auth-port 1645, acct-port 1646) is mapped to the Cisco AAA-SERVER-MIB as follows:

- id maps to casIndex
- priority maps to casPriority
- host maps to casAddress
- auth-port maps to casAuthenPort
- acct-port maps to casAcctPort

Mapping the following set of objects listed in the Cisco AAA-SERVER-MIB map to fields displayed by the **show aaa servers** command is more straightforward. For example, the casAuthenRequests field corresponds to the Authen: request portion of the report, casAuthenRequestTimeouts corresponds to the Authen: timeouts portion of the report, and so on.

- casAuthenRequests
- casAuthenRequestTimeouts
- casAuthenUnexpectedResponses
- casAuthenServerErrorResponses
- casAuthenIncorrectResponses
- casAuthenResponseTime
- casAuthenTransactionSuccesses
- casAuthenTransactionFailures
- casAuthorRequests
- casAuthorRequestTimeouts
- casAuthorUnexpectedResponses
- casAuthorServerErrorResponses
- casAuthorIncorrectResponses
- casAuthorResponseTime
- casAuthorTransactionSuccesses
- casAuthorTransactionFailures
- casAcctRequests
- casAcctRequestTimeouts
- casAcctUnexpectedResponses
- casAcctServerErrorResponses
- casAcctIncorrectResponses
- casAcctResponseTime
- casAcctTransactionSuccesses
- casAcctTransactionFailures
- casState
- casCurrentStateDuration
- casPreviousStateDuration
- casTotalDeadTime
- casDeadCount

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <http://www.cisco.com/go/mibs>.

Related Commands

Command	Description
radius-server dead-criteria	Forces one or both of the criteria--used to mark a RADIUS server as dead--to be the indicated constant.
server-private	Associates a particular private RADIUS server with a defined server group.

show access-lists

To display the contents of current access lists, use the **show access-lists** command in user EXEC or privileged EXEC mode.

show access-lists [*access-list-number*| *access-list-name*]

Syntax Description

<i>access-list-number</i>	(Optional) Number of the access list to display. The system displays all access lists by default.
<i>access-list-name</i>	(Optional) Name of the IP access list to display.

Command Default

The system displays all access lists.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(6)S	The output was modified to identify the compiled ACLs.
12.1(1)E	This command was implemented on the Cisco 7200 series.
12.1(5)T	The command output was modified to identify compiled ACLs.
12.1(4)E	This command was implemented on the Cisco 7100 series.
12.2(2)T	The command output was modified to show information for IPv6 access lists.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The show access-lists command is used to display the current ACLs operating in the router. Each access list is flagged using the Compiled indication if it is operating as an accelerated ACL.

The display also shows how many packets have been matched against each entry in the ACLs, enabling the user to monitor the particular packets that have been permitted or denied. This command also indicates whether the access list is running as a compiled access list.

Examples

The following is sample output from the **show access-lists** command when access list 101 is specified:

```
Router# show access-lists 101
Extended IP access list 101
  permit tcp host 198.92.32.130 any established (4304 matches) check=5
  permit udp host 198.92.32.130 any eq domain (129 matches)
  permit icmp host 198.92.32.130 any
  permit tcp host 198.92.32.130 host 171.69.2.141 gt 1023
  permit tcp host 198.92.32.130 host 171.69.2.135 eq smtp (2 matches)
  permit tcp host 198.92.32.130 host 198.92.30.32 eq smtp
  permit tcp host 198.92.32.130 host 171.69.108.33 eq smtp
  permit udp host 198.92.32.130 host 171.68.225.190 eq syslog
  permit udp host 198.92.32.130 host 171.68.225.126 eq syslog
  deny ip 150.136.0.0 0.0.255.255 224.0.0.0 15.255.255.255
  deny ip 171.68.0.0 0.1.255.255 224.0.0.0 15.255.255.255 (2 matches) check=1
  deny ip 172.24.24.0 0.0.1.255 224.0.0.0 15.255.255.255
  deny ip 192.82.152.0 0.0.0.255 224.0.0.0 15.255.255.255
  deny ip 192.122.173.0 0.0.0.255 224.0.0.0 15.255.255.255
  deny ip 192.122.174.0 0.0.0.255 224.0.0.0 15.255.255.255
  deny ip 192.135.239.0 0.0.0.255 224.0.0.0 15.255.255.255
  deny ip 192.135.240.0 0.0.7.255 224.0.0.0 15.255.255.255
  deny ip 192.135.248.0 0.0.3.255 224.0.0.0 15.255.255.255
```

An access list counter counts how many packets are allowed by each line of the access list. This number is displayed as the number of matches. Check denotes how many times a packet was compared to the access list but did not match.

The following is sample output from the show access-lists command when the Turbo Access Control List (ACL) feature is configured on all of the following access lists.



Note

The permit and deny information displayed by the show access-lists command may not be in the same order as that entered using the access-list command.

```
Router# show access-lists
Standard IP access list 1 (Compiled)
  deny any
Standard IP access list 2 (Compiled)
  deny 192.168.0.0, wildcard bits 0.0.0.255
  permit any
Standard IP access list 3 (Compiled)
  deny 0.0.0.0
  deny 192.168.0.1, wildcard bits 0.0.0.255
  permit any
Standard IP access list 4 (Compiled)
  permit 0.0.0.0
  permit 192.168.0.2, wildcard bits 0.0.0.255
```

The following is sample output from the **show access-lists** command that shows information for IPv6 access lists when IPv6 is configured on the network:

```
Router# show access-lists
IPv6 access list list2
  deny ipv6 FEC0:0:0:2::/64 any sequence 10
  permit ipv6 any any sequence 20
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
clear access-list counters	Clears the counters of an access list.
clear access-template	Clears a temporary access list entry from a dynamic access list manually.
ip access-list	Defines an IP access list by name.
show ip access-lists	Displays the contents of all current IP access lists.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

show authentication interface

To display information about the Auth Manager for a given interface, use the **show authentication interface** command in privileged EXEC mode.

show authentication interface *type number*

Syntax Description

<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>number</i>	Interface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Use the **show authentication interface** command to display information about the Auth Manager for a given interface.

Examples

The following is sample output from the **show authentication interface** command:

```
Switch# show authentication interface g1/0/23
Client list:
  MAC Address      Domain    Status      Handle      Interface
  000e.84af.59bd   DATA    Authz Success  0xE0000000  GigabitEthernet1/0/23
Available methods list:
  Handle  Priority  Name
  3        0        dot1x
Runnable methods list:
  Handle  Priority  Name
  3        0        dot1x
```

The table below describes the significant fields shown in the display. Other fields are self-explanatory.

Table 2: show authentication interface Field Descriptions

Field	Description
MAC Address	The MAC address of the client.

Field	Description
Domain	The domain of the client--either DATA or voice.
Status	<p>The status of the authentication session. The possible values are:</p> <ul style="list-style-type: none"> • Authc Failed--an authentication method has run for this session and authentication failed. • Authc Success--an authentication method has run for this session and authentication was successful. • Authz Failed--a feature has failed and the session has terminated. • Authz Success--all features have been applied to the session and the session is active. • Idle--this session has been initialized but no authentication methods have run. This is an intermediate state. • No methods--no authentication method has provided a result for this session. • Running--an authentication method is running for this session.
Interface	The type and number of the authentication interface.
Available methods list	Summary information for the authentication methods available on the interface.
Runnable methods list	Summary information for the authentication methods that can run on the interface.

Related Commands

Command	Description
show authentication registrations	Displays information about the authentication methods that are registered with the Auth Manager.
show authentication sessions	Displays information about the current Auth Manager sessions.

show authentication registrations

To display information about the authentication methods that are registered with the Auth Manager, use the **show authentication registrations** command in privileged EXEC mode.

show authentication registrations

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2(33)SXI	This command was introduced.
	15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines Use the **show authentication re gistrations** command to display information about all methods registered with the Auth Manager.

Examples The following is sample output for the show authentication registrations command:

```
Switch# show authentication registrations
Auth Methods registered with the Auth Manager:
  Handle   Priority   Name
    3         0   dot1x
    2         1   mab
    1         2  webauth
```

The table below describes the significant fields shown in the display.

Table 3: show authentication registrations Field Descriptions

Field	Description
Priority	The priority of the method. If the priority for authentication methods has not been configured with the authentication priority command, then the default priority is displayed. The default from highest to lowest is dot1x, mab, and webauth.
Name	The name of the authentication method. The values can be dot1x, mab, or webauth.

Related Commands

Command	Description
show authentication interface	Displays information about the Auth Manager for a given interface.
show authentication sessions	Displays information about current Auth Manager sessions.

show authentication sessions

To display information about current Auth Manager sessions, use the **show authentication sessions** command in privileged EXEC mode.



Note

Effective with Cisco IOS Release 12.2(33)SXI, the **show dot1x** command is supplemented by the **show authentication sessions** command. The **show dot1x** command is reserved for displaying output specific to the use of the 802.1X authentication method. The **show authentication sessions** command displays information for all authentication methods and authorization features.

Cisco IOS XE Release 3SE and Later Releases

show authentication sessions [[**database**]] [**handle** *handle-number*] [**interface** *type number*] [**mac** *mac-address*] [**method** *method-name*] [**interface** *type number*] [**session-id** *session-id*] [**details**]

All Other Releases

show authentication sessions [**handle** *handle-number*] [**interface** *type number*] [**mac** *mac-address*] [**method** *method-name*] [**interface** *type number*] [**session-id** *session-id*]

Syntax Description

database	(Optional) Displays session data stored in the session database. This keyword allows you to see information like the VLAN ID, which is not cached internally. A warning message displays if data stored in the session database does not match the internally cached data.
handle <i>handle-id</i>	(Optional) Specifies the particular handle for which to display Auth Manager information.
interface <i>type number</i>	(Optional) Specifies a particular interface type and number for which Auth Manager information is to be displayed. To display the valid keywords and arguments for interfaces, use the question mark (?) online help function.
mac <i>mac-address</i>	(Optional) Specifies the particular MAC address for which you want to display information.

method <i>method-name</i>	<p>(Optional) Specifies the particular authentication method for which to display Auth Manager information. Valid methods are one of the following:</p> <ul style="list-style-type: none"> • dot1x—IEEE 802.1X authentication method. • mab—MAC authentication bypass (MAB) method. • webauth—Web authentication method. <p>If you specify a method, you can also specify an interface.</p>
session-id <i>session-id</i>	(Optional) Specifies the particular session for which to display Auth Manager information.
details	(Optional) Displays detailed information for each session instead of displaying a single-line summary for sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	Support for this command was introduced.
12.2(33)SXI	This command was changed to add the handle <i>handle</i> keyword and argument and add information to the output.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.
Cisco IOS XE Release 3.2SE	This command was modified. The database and details keywords were added.

Usage Guidelines

Use the **show authentication sessions** command to display information about all current Auth Manager sessions. To display information about specific Auth Manager sessions, use one or more of the keywords.

Examples

The following example shows how to display all authentication sessions on the switch:

```
Device# show authentication sessions
```

Interface	MAC Address	Method	Domain	Status	Session ID
Gi1/48	0015.63b0.f676	dot1x	DATA	Authz Success	0A3462B1000000102983C05C
Gi1/5	000f.23c4.a401	mab	DATA	Authz Success	0A3462B10000000D24F80B58
Gi1/5	0014.bf5d.d26d	dot1x	DATA	Authz Success	0A3462B10000000E29811B94

The following example shows how to display all authentication sessions on an interface:

```
Device# show authentication sessions interface gigabitethernet2/47

Interface: GigabitEthernet2/47
  MAC Address: Unknown
  IP Address: Unknown
  Status: Authz Success
  Domain: DATA
  Oper host mode: multi-host
  Oper control dir: both
  Authorized By: Guest Vlan
  Vlan Policy: 20
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: 0A3462C80000000000002763C
  Acct Session ID: 0x00000002
  Handle: 0x25000000
Runnable methods list:
  Method      State
  mab         Failed over
  dot1x       Failed over
-----
  Interface: GigabitEthernet2/47
  MAC Address: 0005.5e7c.da05
  IP Address: Unknown
  User-Name: 00055e7cda05
  Status: Authz Success
  Domain: VOICE
  Oper host mode: multi-domain
  Oper control dir: both
  Authorized By: Authentication Server
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: 0A3462C80000000010002A238
  Acct Session ID: 0x00000003
  Handle: 0x91000001
Runnable methods list:
  Method      State
  mab         Authc Success
  dot1x       Not run
```

The following example shows how to display the authentication session for a specified session ID:

```
Device# show authentication sessions session-id 0B0101C70000004F2ED55218

  Interface: GigabitEthernet9/2
  MAC Address: 0000.0000.0011
  IP Address: 20.0.0.7
  Username: johndoe
  Status: Authz Success
  Domain: DATA
  Oper host mode: multi-host
  Oper control dir: both
  Authorized By: Critical Auth
  Vlan policy: N/A
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: 0B0101C70000004F2ED55218
  Acct Session ID: 0x00000003
  Handle: 0x91000001
Runnable methods list:
  Method      State
  mab         Authc Success
  dot1x       Not run
```

The following examples show how to display all clients authorized by the specified authentication method:

```
Device# show authentication sessions method mab

No Auth Manager contexts match supplied criteria
```

Device# **show authentication sessions method dot1x**

```
Interface  MAC Address      Domain   Status      Session ID
Gi9/2      0000.0000.0011  DATA   Authz Success  0B0101C70000004F2ED55218
```

The table below describes the significant fields shown in the displays.

Table 4: show authentication sessions Field Descriptions

Field	Description
Interface	The type and number of the authentication interface.
MAC Address	The MAC address of the client.
Domain	The name of the domain, either DATA or VOICE.
Status	<p>The status of the authentication session. The possible values are:</p> <ul style="list-style-type: none"> • Authc Failed—An authentication method has run for this session and authentication failed. • Authc Success—An authentication method has run for this session and authentication was successful. • Authz Failed—A feature has failed and the session has terminated. • Authz Success—All features have been applied to the session and the session is active. • Idle—This session has been initialized but no authentication methods have run. This is an intermediate state. • No methods—No authentication method has provided a result for this session. • Running—An authentication method is running for this session.
Handle	The context handle.

Field	Description
State	<p>The operating states for the reported authentication sessions. The possible values are:</p> <ul style="list-style-type: none">• Not run—The method has not run for this session.• Running—The method is running for this session.• Failed over—The method has failed and the next method is expected to provide a result.• Success—The method has provided a successful authentication result for the session.• Authc Failed—The method has provided a failed authentication result for the session.

Related Commands

Command	Description
show access-sessions	Displays information about session aware networking sessions.
show authentication registrations	Displays information about the authentication methods that are registered with the Auth Manager.
show authentication statistics	Displays statistics for Auth Manager sessions.
show dot1x	Displays details for an identity profile specific to the use of the 802.1X authentication method.



show diameter peer through show object-group

- [show dot1x, page 46](#)
- [show ip access-lists, page 50](#)
- [show ip admission, page 54](#)
- [show ip ssh, page 60](#)
- [show ipv6 access-list, page 61](#)
- [show mab, page 65](#)
- [show mac-address-table, page 67](#)

show dot1x

To display details for an identity profile, use the **show dot1x** command in privileged EXEC mode.



Note

Effective with Cisco IOS Release 12.2(33)SXI, the **show dot1x** command is supplemented by the **show authentication** command. The **show dot1x** command is reserved for displaying output specific to the use of the 802.1X authentication method. The **show authentication sessions** command has a wider remit of displaying information for all authentication methods and authorization features. See the **show authentication sessions** command for more information.

show dot1x [**all** [**summary**]] **interface** *interface-name* [**details**|**statistics**]

Syntax Description

all	(Optional) Displays 802.1X status for all interfaces.
summary	(Optional) Displays summary of 802.1X status for all interfaces.
interface <i>interface-name</i>	(Optional) Specifies the interface name and number.
details	(Optional) Displays the interface configuration as well as the authenticator instances on the interface.
statistics	(Optional) Displays 802.1X statistics for all the interfaces.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(11)AX	This command was introduced.
12.1(14)EA1	The all keyword was added.
12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)SED	The output display was expanded to include auth-fail-vlan information in the authorization state machine state and port status fields.
12.2(25)SEE	The details and statistics keywords were added.

Release	Modification
12.3(11)T	The PAE, HeldPeriod, StartPeriod, and MaxStart fields were added to the show dot1x command output.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you do not specify a port, global parameters and a summary appear. If you specify a port, details for that port appear in the output.



Note

In some IOS versions, the **show dot1x** command may not display the AUTHORIZED or UNAUTHORIZED value in the Port Status command output field if authentication methods other than the 802.1X authentication method are used. If the Port Status field does not contain a value, then use the **show authentication sessions** command to display the Authz Success or Authz Failed port status authentication value.

Examples

The following is sample output from the **show dot1x** command using both the **interface** and **details** keywords. The clients are successfully authenticated in this example.

```
Router# show dot1x interface ethernet1/0 details
Dot1x Info for Ethernet1/0
-----
PAE                               = AUTHENTICATOR
PortControl                       = AUTO
ControlDirection                  = Both
HostMode                          = MULTI_HOST
QuietPeriod                       = 60
ServerTimeout                     = 0
SuppTimeout                       = 30
ReAuthMax                         = 2
MaxReq                            = 1
TxPeriod                          = 30
Dot1x Authenticator Client List
-----
Supplicant                        = aabb.cc00.c901
Session ID                       = 0A3462800000000000000009F8
  Auth SM State                   = AUTHENTICATED
  Auth BEND SM State              = IDLE
```

The following is sample output from the **show dot1x** command using both the **interface** and **details** keywords. The clients are unsuccessful at authenticating in this example.

```
Router# show dot1x interface ethernet1/0 details
Dot1x Info for Ethernet1/0
-----
PAE                               = AUTHENTICATOR
PortControl                       = AUTO
ControlDirection                  = Both
HostMode                          = MULTI_HOST
QuietPeriod                       = 60
ServerTimeout                     = 0
SuppTimeout                       = 30
ReAuthMax                         = 2
MaxReq                            = 1
```

```
TxPeriod                = 30
Dot1x Authenticator Client List Empty
```

The table below describes the significant fields shown in the displays.

Table 5: show dot1x Field Descriptions

Field	Description
PAE	Port Access Entity. Defines the role of an interface (as a supplicant, as an authenticator, or as an authenticator and supplicant).
PortControl	Port control value. <ul style="list-style-type: none"> • AUTO--The authentication status of the client PC is being determined by the authentication process. • Force-authorize--All the client PCs on the interface are being authorized. • Force-unauthorized--All the client PCs on the interface are being unauthorized.
ControlDirection	Indicates whether control for an IEEE 802.1X controlled port is applied to both directions (ingress and egress), or inbound direction only (ingress). See 'dot1x control-direction', or effective from Cisco IOS Release 12.2(33)SXI onwards, authentication control-direction for more detail.
HostMode	Indicates whether the host-mode is single-host or multi-host, and effective from Cisco IOS Release 12.2(33)SXI onwards, multi-auth or multi-domain as well. See 'dot1x host-mode', or effective from Cisco IOS Release 12.2(33)SXI onwards, 'authentication host-mode' for more detail.
QuietPeriod	If authentication fails for a client, the authentication gets restarted after the quiet period shown in seconds.
ServerTimeout	Timeout that has been set for RADIUS retries. If an 802.1X packet is sent to the server and the server does not send a response, the packet will be sent again after the number of seconds that are shown.
SuppTimeout	Time that has been set for supplicant (client PC) retries. If an 802.1X packet is sent to the supplicant and the supplicant does not send a response, the packet will be sent again after the number of seconds that are shown.

Field	Description
ReAuthMax	The maximum amount of time in seconds after which an automatic reauthentication of a client PC is initiated.
MaxReq	Maximum number of times that the router sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client PC before concluding that the client PC does not support 802.1X.
TxPeriod	Timeout for supplicant retries, that is the timeout for EAP Identity Requests. See 'dot1x timeout tx-period' for more detail.
Supplicant	MAC address of the client PC or any 802.1X client.
Session ID	The ID of the network session.
Auth SM State	Describes the state of the client PC as either AUTHENTICATED or UNAUTHENTICATED.
Auth BEND SM State	The state of the IEEE 802.1X authenticator backend state machine.

Related Commands

Command	Description
clear dot1x	Clears 802.1X interface information.
debug dot1x	Displays 802.1X debugging information.
dot1x default	Resets the global 802.1X parameters to their default values.
identity profile	Creates an identity profile.
show authentication sessions	Displays information about current Authentication Manager sessions.

show ip access-lists

To display the contents of all current IP access lists, use the **show ip access-lists** command in user EXEC or privileged EXEC modes.

show ip access-lists [*access-list-number*| *access-list-number-expanded-range*| *access-list-name*| **dynamic** [*dynamic-access-list-name*]| **interface** *name number* [**in**| **out**]]

Syntax Description

<i>access-list-number</i>	(Optional) Number of the IP access list to display.
<i>access-list-number-expanded-range</i>	(Optional) Expanded range of the IP access list to display.
<i>access-list-name</i>	(Optional) Name of the IP access list to display.
dynamic <i>dynamic-access-list-name</i>	(Optional) Displays the specified dynamic IP access lists.
interface <i>name number</i>	(Optional) Displays the access list for the specified interface.
in	(Optional) Displays input interface statistics.
out	(Optional) Displays output interface statistics.

Command Default

All standard and expanded IP access lists are displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.3(7)T	The dynamic keyword was added.
12.4(6)T	The interface <i>name</i> and <i>number</i> keyword and argument pair was added. The in and out keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was modified. Example output from the dynamic keyword was added.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. The output of this command was extended to display access lists that contain object groups.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The **show ip access-lists** command provides output identical to the **show access-lists** command, except that it is IP-specific and allows you to specify a particular access list.

Examples

The following is sample output from the **show ip access-lists** command when all access lists are requested:

```
Router# show ip access-lists
Extended IP access list 101
  deny udp any any eq nntp
  permit tcp any any
  permit udp any any eq tftp
  permit icmp any any
  permit udp any any eq domain
```

The table below describes the significant fields shown in the display.

Table 6: show ip access-lists Field Descriptions

Field	Description
Extended IP access list	Extended IP access-list number.
deny	Packets to reject.
udp	User Datagram Protocol.
any	Source host or destination host.
eq	Packets on a given port number.
nntp	Network News Transport Protocol.
permit	Packets to forward.
tcp	Transmission Control Protocol.
tftp	Trivial File Transfer Protocol.
icmp	Internet Control Message Protocol.
domain	Domain name service.

The following is sample output from the **show ip access-lists** command when the name of a specific access list is requested:

```
Router# show ip access-lists Internetfilter
Extended IP access list Internetfilter
  permit tcp any 192.0.2.0 255.255.255.255 eq telnet
  deny tcp any any
  deny udp any 192.0.2.0 255.255.255.255 lt 1024
  deny ip any any log
```

The following is sample output from the **show ip access-lists** command when the name of a specific access list that contains an object group is requested:

```
Router# show ip access-lists my-ogacl-policy
Extended IP access list my-ogacl-policy
  10 permit object-group eng-service any any
```

The following sample output from the **show ip access-lists** command shows input statistics for Fast Ethernet interface 0/0:

```
Router#
show ip access-lists interface FastEthernet0/0 in

Extended IP access list 150 in
  10 permit ip host 10.1.1.1 any
  30 permit ip host 10.2.2.2 any (15 matches)
```

The following is sample output from the **show ip access-lists** command using the **dynamic** keyword:

```
Router#
show ip access-lists dynamic CM_SF#1
Extended IP access list CM_SF#1
  10 permit udp any any eq 5060 (650 matches)
  20 permit tcp any any eq 5060
  30 permit udp any any dscp ef (806184 matches)
```

To check your configuration, use the **show run interfaces cable** command:

```
Router#
show run interfaces cable 0/1/0
Building configuration...
Current configuration : 144 bytes
!
interface cable-modem0/1/0
 ip address dhcp
 load-interval 30
 no keepalive
 service-flow primary upstream
 service-policy output llq
end
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
ip access-group	Applies an ACL or OGACL to an interface or a service policy map.
ip access-list	Defines an IP access list or OGACL by name or number.

Command	Description
object-group network	Defines network object groups for use in OGACLs.
object-group service	Defines service object groups for use in OGACLs.
permit	Sets conditions in a named IP access list or OGACL that will permit packets.
show object-group	Displays information about object groups that are configured.
show run interfaces cable	Displays statistics on the cable modem.

show ip admission

To display the network admission cache entries and information about web authentication sessions, use the **show ip admission** command in user EXEC or privileged EXEC mode.

Cisco IOS XE Release 3SE and Later Releases

show ip admission {cache| statistics [brief| details| httpd| input-feature]} status [banners| custom-pages| httpd| parameter-map [*parameter-map-name*]]| watch-list}

All Other Releases

show ip admission {cache [consent| eapoudp| ip-addr *ip-address*| username *username*]} configuration| httpd| statistics| [brief| details| httpd]| status [httpd]| watch-list}

Syntax Description

cache	Displays the current list of network admission entries.
statistics	Displays statistics for web authentication.
brief	(Optional) Displays a statistics summary for web authentication.
details	(Optional) Displays detailed statistics for web authentication.
httpd	(Optional) Displays information about web authentication HTTP processes
input-feature	Displays statistics about web authentication packets.
status	Displays status information about configured web authentication features including banners, custom pages, HTTP processes, and parameter maps.
banners	Displays information about configured banners for web authentication.
custom-pages	Displays information about custom pages configured for web authentication. Custom files are read into a local cache and served from the cache. A background process periodically checks if the files need to be re-cached.
parameter-map <i>parameter-map-name</i>	Displays information about configured banners and custom pages for all parameter maps or only for the specified parameter map.
watch-list	Displays the list of IP addresses in the watch list.

consent	(Optional) Displays the consent web page cache entries.
eapoudp	(Optional) Displays the Extensible Authentication Protocol over UDP (EAPoUDP) network admission cache entries. Includes the host IP addresses, session timeout, and posture state.
ip-addr <i>ip-address</i>	(Optional) Displays information for a client IP address.
username <i>username</i>	(Optional) Display information for a client username.
configuration	(Optional) Displays the NAC configuration. Note This keyword is not supported in Cisco IOS XE Release 3.2SE and later releases. Use the show running-config all command to see the running web authentication configuration and the commands configured with default parameters.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)T	This command was modified. The output of this command was enhanced to display whether the AAA timeout policy is configured.
12.4(15)T	This command was modified. The consent keyword was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.3(1)T	This command was modified. The statistics , brief , details , httpd , and status keywords were added.
Cisco IOS XE Release 3.2SE	This command was modified. The input-feature , banners , custom-pages , and parameter-map keywords were added. The configuration keyword was removed.

Usage Guidelines

Use the **show ip admission** command to display information about network admission entries and information about web authentication sessions.

Examples

The following is sample output from the **show ip admission cache** command:

Device# **show ip admission cache**

Authentication Proxy Cache

Total Sessions: 1 Init Sessions: 1

Client MAC 5cf3.fc25.7e3d Client IP 1.150.128.2 IPv6 :: Port 0, State INIT, Method Webauth

The following is sample output from the **show ip admission statistics** command:

Device# **show ip admission statistics**

Webauth input-feature statistics:

	IPv4	IPv6
Total packets received	46	0
Delivered to TCP	46	0
Forwarded	0	0
Dropped	0	0
TCP new connection limit reached	0	0

Webauth HTTPd statistics:

HTTPd process 1	
Intercepted HTTP requests:	8
IO Read events:	9
Received HTTP messages:	7
IO write events:	11
Sent HTTP replies:	7
IO AAA messages:	4
SSL OK:	0
SSL Read would block:	0
SSL Write would block:	0
HTTPd process scheduled count:	23

The following is sample output from the **show ip admission status** command:

Device# **show ip admission status**

IP admission status:

Enabled interfaces	1		
Total sessions	1		
Init sessions	1	Max init sessions allowed	100
Limit reached	0	Hi watermark	1
TCP half-open connections	0	Hi watermark	0
TCP new connections	0	Hi watermark	0
TCP half-open + new	0	Hi watermark	0
HTTPD1 Contexts	0	Hi watermark	1

Parameter Map: Global

Custom Pages

Custom pages not configured

Banner

Banner not configured

Parameter Map: PMAP_WEBAUTH

Custom Pages

Custom pages not configured

Banner

Type: text

Banner

" <H2>Login Page Banner</H2> "

Html

" <H2>Login Page Banner</H2> ";

Length

48

Parameter Map: PMAP_CONSENT

Custom Pages

Custom pages not configured

Banner

Banner not configured

Parameter Map: PMAP_WEBCONSENT

Custom Pages

Custom pages not configured


```

Parameter Map: PMAP_WEBAUTH
Type: file
  Banner                                <h2>Cisco Systems</h2>
<h3>Webauth Banner from file</h3>

Length                                60
File                                  flash:webauth_banner1.html
File status                           Ok - File cached
File mod time                         2012-07-24T07:07:09.000Z
File needs re-cached                  No
Cache                                 0x3AF6CEE4
Cache len                             60
Cache time                           2012-09-19T10:13:59.000Z
Cache access                          0 reads, 1 write

```

The following is sample output from the **show ip admission status custom pages** command:

Device# **show ip admission status custom pages**

```

IP admission status:
Parameter Map: Global
Custom pages not configured
Parameter Map: PMAP_WEBAUTH
Type: "login"
  File                                  flash:webauth_login.html
  File status                           Ok - File cached
  File mod time                         2012-07-20T02:29:36.000Z
  File needs re-cached                  No
  Cache                                 0x3B0DCEB4
  Cache len                             246582
  Cache time                           2012-09-18T16:26:13.000Z
  Cache access                          0 reads, 1 write
Type: "success"
  File                                  flash:webauth_success.html
  File status                           Ok - File cached
  File mod time                         2012-02-21T06:57:28.000Z
  File needs re-cached                  No
  Cache                                 0x3A2E9090
  Cache len                             70
  Cache time                           2012-09-18T16:26:13.000Z
  Cache access                          0 reads, 1 write
Type: "failure"
  File                                  flash:webauth_fail.html
  File status                           Ok - File cached
  File mod time                         2012-02-21T06:55:49.000Z
  File needs re-cached                  No
  Cache                                 0x3AF6D1A4
  Cache len                             67
  Cache time                           2012-09-18T16:26:13.000Z
  Cache access                          0 reads, 1 write
Type: "login expired"
  File                                  flash:webauth_expire.html
  File status                           Ok - File cached
  File mod time                         2012-02-21T06:55:25.000Z
  File needs re-cached                  No
  Cache                                 0x3A2E8284
  Cache len                             69
  Cache time                           2012-09-18T16:26:13.000Z
  Cache access                          0 reads, 1 write
Parameter Map: PMAP_CONSENT
Custom pages not configured

```

The following table describes the significant fields shown in the above display.

Table 7: show ip admission Field Descriptions

File mod time	Time stamp when the file was changed on the file system.
Cache time	Time stamp when the file was last read into cache.

The following output displays all the IP admission control rules that are configured on a router:

Device# **show ip admission configuration**

```
Authentication Proxy Banner not configured
Consent Banner is not configured
Authentication Proxy webpage
  Login page           : flash:test1.htm
  Success page         : flash:test1.htm
  Fail page            : flash:test1.htm
  Login Expire page    : flash:test1.htm
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 5 minutes
Authentication Proxy Watch-list is disabled
```

```
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

The following output displays the host IP addresses, the session timeout, and the posture states. If the posture statue is POSTURE ESTAB, the host validation was successful.

Device# **show ip admission cache eapoudp**

```
Posture Validation Proxy Cache
Total Sessions: 3 Init Sessions: 1
  Client IP 10.0.0.112, timeout 60, posture state POSTURE ESTAB
  Client IP 10.0.0.142, timeout 60, posture state POSTURE INIT
  Client IP 10.0.0.205, timeout 60, posture state POSTURE ESTAB
```

The fields in the displays are self-explanatory.

Related Commands

Command	Description
banner (parameter-map webauth)	Displays a banner on the web-authentication login web page.
clear ip admission cache	Clears IP admission cache entries from the router.
custom-page	Displays custom web pages during web authentication login.
ip admission name	Creates a Layer 3 network admission control rule.

show ip ssh

To display the version and configuration data for Secure Shell (SSH), use the **show ip ssh** command in privileged EXEC mode.

show ip ssh

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1 T.
12.1(5)T	This command was modified to display the SSH status--enabled or disabled.
12.2(17a)SX	This command was integrated into Cisco IOS Release 12.2(17a)SX.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use the **show ip ssh** command to view the status of configured options such as retries and timeouts. This command allows you to see if SSH is enabled or disabled.

Examples

The following is sample output from the **show ip ssh** command when SSH has been enabled:

```
Router# show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
The following is sample output from the show ip ssh
command when SSH has been disabled:
Router# show ip ssh
%SSH has not been enabled
```

Related Commands

Command	Description
show ssh	Displays the status of SSH server connections.

show ipv6 access-list

To display the contents of all current IPv6 access lists, use the **show ipv6 access-list** command in user EXEC or privileged EXEC mode.

show ipv6 access-list [*access-list-name*]

Syntax Description

<i>access-list-name</i>	(Optional) Name of access list.
-------------------------	---------------------------------

Command Default

All IPv6 access lists are displayed.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	The priority field was changed to sequence and Layer 4 protocol information (extended IPv6 access list functionality) was added to the display output.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(50)SY	This command was modified. Information about IPv4 and IPv6 hardware statistics is displayed.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **show ipv6 access-list** command provides output similar to the **show ip access-list** command, except that it is IPv6-specific.

Examples

The following output from the **show ipv6 access-list** command shows IPv6 access lists named inbound, tcptraffic, and outbound:

```
Router# show ipv6 access-list
IPv6 access list inbound
  permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
  permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
  permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
  permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
    left 243) sequence 1
  permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
    (time left 296) sequence 2
IPv6 access list outbound
  evaluate udptraffic
  evaluate tcptraffic
```

The following sample output shows IPv6 access list information for use with IPsec:

```
Router# show ipv6 access-list
IPv6 access list Tunnel0-head-0-ACL (crypto)
  permit ipv6 any any (34 matches) sequence 1
IPv6 access list Ethernet2/0-ipsecv6-ACL (crypto)
  permit 89 FE80::/10 any (85 matches) sequence 1
```

The table below describes the significant fields shown in the display.

Table 8: show ipv6 access-list Field Descriptions

Field	Description
ipv6 access list inbound	Name of the IPv6 access list, for example, inbound.
permit	Permits any packet that matches the specified protocol type.
tcp	Transmission Control Protocol. The higher-level (Layer 4) protocol type that the packet must match.
any	Equal to ::/0.
eq	An equal operand that compares the source or destination ports of TCP or UDP packets.
bgp	Border Gateway Protocol. The lower-level (Layer 3) protocol type that the packet must be equal to.
reflect	Indicates a reflexive IPv6 access list.

Field	Description
tcptraffic (8 matches)	The name of the reflexive IPv6 access list and the number of matches for the access list. The clear ipv6 access-list privileged EXEC command resets the IPv6 access list match counters.
sequence 10	Sequence in which an incoming packet is compared to lines in an access list. Lines in an access list are ordered from first priority (lowest number, for example, 10) to last priority (highest number, for example, 80).
host 2001:0DB8:1::1	The source IPv6 host address that the source address of the packet must match.
host 2001:0DB8:1::2	The destination IPv6 host address that the destination address of the packet must match.
11000	The ephemeral source port number for the outgoing connection.
timeout 300	The total interval of idle time (in seconds) after which the temporary IPv6 reflexive access list named tcptraffic will time out for the indicated session.
(time left 243)	The amount of idle time (in seconds) remaining before the temporary IPv6 reflexive access list named tcptraffic is deleted for the indicated session. Additional received traffic that matches the indicated session resets this value to 300 seconds.
evaluate udptraffic	Indicates the IPv6 reflexive access list named udptraffic is nested in the IPv6 access list named outbound.

Related Commands

Command	Description
clear ipv6 access-list	Resets the IPv6 access list match counters.
hardware statistics	Enables the collection of hardware statistics.
show ip access-list	Displays the contents of all current IP access lists.
show ip prefix-list	Displays information about a prefix list or prefix list entries.

Command	Description
show ipv6 prefix-list	Displays information about an IPv6 prefix list or IPv6 prefix list entries.

show mab

To display MAC Authentication Bypass (MAB) information, use the **show mab** command in privileged EXEC mode.

show mab [**all**| **interface** *type number*] [**detail**]

Syntax Description

all	Specifies all interfaces.
interface <i>type number</i>	Specifies a particular interface for which to display MAB information.
detail	(Optional) Displays detailed information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.
15.2(3)T	This command was modified. The authorization status of the authentication result is displayed as SUCCESS or FAIL instead of AUTHORIZED or UNAUTHORIZED in the command output.

Usage Guidelines

Use the **show mab** command to display information about MAB ports and MAB sessions.

Examples

The following is sample output from the **show mab interface detail** command where a MAB session has been authorized:

```
Switch# show mab interface
FastEthernet1/0/1
detail
MAB details for FastEthernet1/0/1
-----
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None
MAB Client List
-----
Client MAC                 = 000f.23c4.a401
MAB SM state               = TERMINATE
Auth Status                = SUCCESS
```

The table below describes the significant fields shown in the display.

Table 9: show mab Field Descriptions

Field	Description
Mac-Auth-Bypass	Specifies whether MAB is enabled or disabled.
Inactivity Timeout	The period of time of no activity after which the session is ended.
Client MAC	The MAC address of the client.
MAB SM state	<p>The state of the MAB state machine. The possible values, from start to finish, are:</p> <ul style="list-style-type: none"> • INITIALIZE--the state of the session when it is being initialized. • ACQUIRING--the state of the session when the MAC address is being obtained from the client. • AUTHORIZING--the state of the session when the MAC address is being authorized. • TERMINATE--the state of the session once an authorization result has been obtained.
Auth Status	<p>The authorization status of the MAB session. The possible values are:</p> <ul style="list-style-type: none"> • SUCCESS--the session has been successfully authorized. • FAIL--the session failed to be authorized.

Related Commands

Command	Description
show authentication interface	Displays information about the Auth Manager for a given interface.
show authentication registrations	Displays information about authentication methods registered with the Auth Manager.
show authentication sessions	Displays information about Auth Manager sessions.

show mac-address-table

To display the MAC address table, use the **show mac-address-table** command in privileged EXEC mode.

Cisco 2600, 3600, and 3700 Series Routers

```
show mac-address-table [secure| self| count][address macaddress][interface type/number] {fa |
gi slot/port} [atm slot/port] [atm slot/port] [vlan vlan-id]
```

Catalyst 4500 Series Switches

```
show mac-address-table {assigned| ip| ipx| other}
```

Catalyst 6000/6500 Series Switches and 7600 Series Routers

```
show mac-address-table [ address mac-addr [all | interface type/number | module number | vlan
vlan-id ] | aging-time [vlan vlan-id ] | count [module number | vlan vlan-id ] | interface type/number | limit
[vlan vlan-id | module number | interface type] | module number | multicast [ count ] [igmp-snooping
|mld-snooping | user ][vlan vlan-id ] | notification {mac-move [counter [vlan]] | threshold | change} [interface
[number]] | synchronize statistics | unicast-flood | vlan vlan-id [all | module number]]
```

Syntax Description

secure	(Optional) Displays only the secure addresses.
self	(Optional) Displays only addresses added by the switch itself.
count	(Optional) Displays the number of entries that are currently in the MAC address table.
address mac-addr	(Optional) Displays information about the MAC address table for a specific MAC address. See the Usage Guidelines section for formatting information.
interface type / number	(Optional) Displays addresses for a specific interface. For the Catalyst 6500 and 6000 series switches, valid values are atm , fastethernet , gigabitethernet , and port-channel . For the Cisco 7600 series, valid values are atm , ethernet , fastethernet , ge-wan , gigabitethernet , tengigabitethernet , and pos .
fa	(Optional) Specifies the Fast Ethernet interface.
gi	(Optional) Specifies the Gigabit Ethernet interface.
slot / port	(Optional) Adds dynamic addresses to the module in slot 1 or 2. The slash mark is required.

atm <i>slot /port</i>	(Optional) Adds dynamic addresses to ATM module <i>slot /port</i> . Use 1 or 2 for the slot number. Use 0 as the port number. The slash mark is required.
vlan <i>vlan -id</i>	(Optional) Displays addresses for a specific VLAN. For the Cisco 2600, 3600, and 3700 series, valid values are from 1 to 1005; do not enter leading zeroes. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094. For the Catalyst 6500 and 6000 series switches and 7600 series, valid values are from 1 to 4094.
assigned	Specifies the assigned protocol entries.
ip	Specifies the IP protocol entries.
ipx	Specifies the IPX protocol entries.
other	Specifies the other protocol entries.
all	(Optional) Displays every instance of the specified MAC address in the forwarding table.
<i>type / number</i>	(Optional) Module and interface number.
module <i>number</i>	(Optional) Displays information about the MAC address table for a specific Distributed Forwarding Card (DFC) module.
aging-time	(Optional) Displays the aging time for the VLANs.
limit	Displays MAC-usage information.
multicast	Displays information about the multicast MAC address table entries only.
igmp-snooping	Displays the addresses learned by Internet Group Management Protocol (IGMP) snooping.
mld-snooping	Displays the addresses learned by Multicast Listener Discover version 2 (MLDv2) snooping.
user	Displays the manually entered (static) addresses.
notification mac-move	Displays the MAC-move notification status.
notification mac-move counter	(Optional) Displays the number of times a MAC has moved and the number of these instances that have occurred in the system.

<i>vlan</i>	(Optional) Specifies a VLAN to display. For the Catalyst 6500 and 6000 series switches and 7600 series, valid values are from 1 to 4094.
notification threshold	Displays the Counter-Addressable Memory (CAM) table utilization notification status.
notification change	Displays the MAC notification parameters and history table.
synchronize statistics	Displays information about the statistics collected on the switch processor or DFC.
unicast-flood	Displays unicast-flood information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2(8)SA	This command was introduced.
11.2(8)SA3	This command was modified. The aging-time ,, count , self , and vlan vlan-id keywords and arguments were added.
11.2(8)SA5	This command was modified. The atmslot/port keyword-argument pair was added.
12.2(2)XT	This command was modified. This command was implemented on Cisco 2600, 3600, and 3700 series routers.
12.1(8a)EW	This command was modified. This command was implemented on Catalyst 4500 series switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on Cisco 2600, 3600, and 3700 series routers.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(14)SX	This command was modified. This command was implemented on the Supervisor Engine 720.

Release	Modification
12.2(17a)SX	<p>This command was modified. For the Catalyst 6500 and 6000 series switches and 7600 series, this command was changed to support the following optional keywords and arguments:</p> <ul style="list-style-type: none"> • count <i>module number</i> • limit [<i>vlan vlan-id</i> <i>port number</i> <i>interface interface-type</i>] • notification threshold • unicast-flood
12.2(17d)SXB	This command was modified. Support for this command was added for the Supervisor Engine 2.
12.2(18)SXE	This command was modified. For the Catalyst 6500 and 6000 series switches and Cisco 7600 series, support was added for the mld-snooping keyword on the Supervisor Engine 720 only.
12.2(18)SXF	This command was modified. For the Catalyst 6500 and 6000 series switches and Cisco 7600 series, support was added for the synchronizestatistics keywords on the Supervisor Engine 720 only.
12.2(33)SRA	This command was modified. This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	This command was modified to extend the range of valid VLAN IDs to 1 to 4094 for specified platforms.
12.2(33)SXH	This command was modified. The change keyword was added.
12.2(33)SXI	This command was modified to add the counter keyword.

Usage Guidelines

Cisco 2600, 3600, and 3700 Series Routers

The **show mac-address-table** command displays the MAC address table for the switch. Specific views can be defined by using the optional keywords and arguments. If more than one optional keyword is used, then all the conditions must be true for that entry to be displayed.

Catalyst 4500 Series Switches

For the MAC address table entries that are used by the routed ports, the routed port name, rather than the internal VLAN number, is displayed in the □vlan□ column.

Catalyst 6000 and 6500 Series Switches and Cisco 7600 Series Routers

If you do not specify a module number, the output of the **show mac-address-table** command displays information about the supervisor engine. To display information about the MAC address table of the DFCs, you must enter the module number or the **all** keyword.

The *mac-addr* value is a 48-bit MAC address. The valid format is H.H.H.

The interface *number* argument designates the module and port number. Valid values depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The optional **module number** keyword-argument pair is supported only on DFC modules. The **module number** keyword-argument pair designate the module number.

Valid values for the *mac-group-address* argument are from 1 to 9.

The optional **count** keyword displays the number of multicast entries.

The optional **multicast** keyword displays the multicast MAC addresses (groups) in a VLAN or displays all statically installed or IGMP snooping-learned entries in the Layer 2 table.

The information that is displayed in the show mac-address-table unicast-flood command output is as follows:

- Up to 50 flood entries, shared across all the VLANs that are not configured to use the filter mode, can be recorded.
- The output field displays are defined as follows:
 - ALERT--Information is updated approximately every 3 seconds.
 - SHUTDOWN--Information is updated approximately every 3 seconds.



Note

The information displayed on the destination MAC addresses is deleted as soon as the floods stop after the port shuts down.

- Information is updated each time that you install the filter. The information lasts until you remove the filter.

The dynamic entries that are displayed in the Learn field are always set to Yes.

The **show mac-address-table limit** command output displays the following information:

- The current number of MAC addresses.
- The maximum number of MAC entries that are allowed.
- The percentage of usage.

The show mac-address-table synchronize statistics command output displays the following information:

- Number of messages processed at each time interval.
- Number of active entries sent for synchronization.
- Number of entries updated, created, ignored, or failed.

Examples

The following is sample output from the **show mac-address-table** command:

```
Switch# show mac-address-table
Dynamic Addresses Count:          9
Secure Addresses (User-defined) Count: 0
```

show mac-address-table

```

Static Addresses (User-defined) Count: 0
System Self Addresses Count:         41
Total MAC addresses:                  50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-----
0010.0de0.e289      Dynamic      1     FastEthernet0/1
0010.7b00.1540      Dynamic      2     FastEthernet0/5
0010.7b00.1545      Dynamic      2     FastEthernet0/5
0060.5cf4.0076      Dynamic      1     FastEthernet0/1
0060.5cf4.0077      Dynamic      1     FastEthernet0/1
0060.5cf4.1315      Dynamic      1     FastEthernet0/1
0060.70cb.f301      Dynamic      1     FastEthernet0/1
00e0.1e42.9978      Dynamic      1     FastEthernet0/1
00e0.1e9f.3900      Dynamic      1     FastEthernet0/1

```

Examples

The following example shows how to display the MAC address table entries that have a specific protocol type (in this case, “assigned”):

```
Switch# show mac-address-table protocol assigned
```

vlan	mac address	type	protocol	qos	ports
200	0050.3e8d.6400	static	assigned	--	Switch
100	0050.3e8d.6400	static	assigned	--	Switch
5	0050.3e8d.6400	static	assigned	--	Switch
4092	0000.0000.0000	dynamic	assigned	--	Switch
1	0050.3e8d.6400	static	assigned	--	Switch
4	0050.3e8d.6400	static	assigned	--	Switch
4092	0050.f0ac.3058	static	assigned	--	Switch
4092	0050.f0ac.3059	dynamic	assigned	--	Switch
1	0010.7b3b.0978	dynamic	assigned	--	Fa5/9

The following example shows the “other” output for the previous example:

```
Switch# show mac-address-table protocol other
```

```

Unicast Entries
vlan  mac address  type  protocols  port
-----
1      0000.0000.0201   dynamic other      FastEthernet6/15
1      0000.0000.0202   dynamic other      FastEthernet6/15
1      0000.0000.0203   dynamic other      FastEthernet6/15
1      0000.0000.0204   dynamic other      FastEthernet6/15
1      0030.94fc.0dff   static ip,ipx,assigned,other Switch
2      0000.0000.0101   dynamic other      FastEthernet6/16
2      0000.0000.0102   dynamic other      FastEthernet6/16
2      0000.0000.0103   dynamic other      FastEthernet6/16
2      0000.0000.0104   dynamic other      FastEthernet6/16
Fa6/1  0030.94fc.0dff   static ip,ipx,assigned,other Switch
Fa6/2  0030.94fc.0dff   static ip,ipx,assigned,other Switch

Multicast Entries
vlan  mac address  type  ports
-----
1      ffff.ffff.ffff   system Switch,Fa6/15
2      ffff.ffff.ffff   system Fa6/16
1002   ffff.ffff.ffff   system
1003   ffff.ffff.ffff   system
1004   ffff.ffff.ffff   system
1005   ffff.ffff.ffff   system
Fa6/1  ffff.ffff.ffff   system Switch,Fa6/1
Fa6/2  ffff.ffff.ffff   system Switch,Fa6/2

```

Examples

The following is sample output from the **show mac-address-table** command:

```
Switch# show mac-address-table

Dynamic Addresses Count:          9
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count:     41
Total MAC addresses:             50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-----
0010.0de0.e289      Dynamic      1     FastEthernet0/1
0010.7b00.1540      Dynamic      2     FastEthernet0/5
0010.7b00.1545      Dynamic      2     FastEthernet0/5
0060.5cf4.0076      Dynamic      1     FastEthernet0/1
0060.5cf4.0077      Dynamic      1     FastEthernet0/1
0060.5cf4.1315      Dynamic      1     FastEthernet0/1
0060.70cb.f301      Dynamic      1     FastEthernet0/1
00e0.1e42.9978      Dynamic      1     FastEthernet0/1
00e0.1e9f.3900      Dynamic      1     FastEthernet0/1
```



Note

In a distributed Encoded Address Recognition Logic (EARL) switch, the asterisk (*) indicates a MAC address that is learned on a port that is associated with this EARL.

The following example shows how to display the information about the MAC address table for a specific MAC address with a Supervisor Engine 720:

```
Switch# show mac-address-table address 001.6441.60ca

Codes: * - primary entry
       vlan  mac address  type  learn qos  ports
-----+-----+-----+-----+-----+-----
Supervisor:
* --- 0001.6441.60ca  static No  -- Router
The following example shows how to display MAC address table information for a specific MAC address with a Supervisor Engine 720:
```

```
Router# show mac-address-table address 0100.5e00.0128

Legend: * - primary entry
       age - seconds since last seen
       n/a - not available
       vlan  mac address  type  learn  age  ports
-----+-----+-----+-----+-----+-----
Supervisor:
* 44 0100.5e00.0128  static Yes  - Fa6/44,Router
* 1  0100.5e00.0128  static Yes  - Router
Module 9:
* 44 0100.5e00.0128  static Yes  - Fa6/44,Router
* 1  0100.5e00.0128  static Yes  - Router
```

The following example shows how to display the currently configured aging time for all VLANs:

```
Switch# show mac-address-table aging-time

Vlan  Aging Time
----  -
*100   300
200    1000
```

The following example shows how to display the entry count for a specific slot:

```
Switch# show mac-address-table count module 1

MAC Entries on slot 1 :
Dynamic Address Count:          4
Static Address (User-defined) Count: 25
Total MAC Addresses In Use:      29
Total MAC Addresses Available:   131072
```

The following example shows how to display the information about the MAC address table for a specific interface with a Supervisor Engine 720:

```
Switch# show mac-address-table interface fastethernet 6/45

Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address      type    learn    age    ports
-----+-----+-----+-----+-----+-----
*  45    00e0.f74c.842d    dynamic Yes         5    Fa6/45
```



Note

A leading asterisk (*) indicates entries from a MAC address that was learned from a packet coming from an outside device to a specific module.

The following example shows how to display the limit information for a specific slot:

```
Switch# show mac-address-table limit vlan 1 module 1

vlan   switch   module   action    maximum   Total entries   flooding
-----+-----+-----+-----+-----+-----+-----
1       1         7       warning    500        0              enabled
1       1        11       warning    500        0              enabled
1       1        12       warning    500        0              enabled

Router#show mac-address-table limit vlan 1 module 2

vlan   switch   module   action    maximum   Total entries   flooding
-----+-----+-----+-----+-----+-----+-----
1       2         7       warning    500        0              enabled
1       2         9       warning    500        0              enabled
```

The following example shows how to display the MAC-move notification status:

```
Switch# show mac-address-table notification mac-move

MAC Move Notification: Enabled
```

The following example shows how to display the MAC move statistics:

```
Router# show mac-address-table notification mac-move counter

-----
Vlan Mac Address From Mod/Port To Mod/Port Count
-----+-----+-----+-----+-----+-----
1 00-01-02-03-04-01 2/3 3/1 10
20 00-01-05-03-02-01 5/3 5/1 20
```

The following example shows how to display the CAM-table utilization-notification status:

```
Router# show mac-address-table notification threshold
```

```
Status limit Interval
-----+-----
enabled 1 120
```

The following example shows how to display the MAC notification parameters and history table:

```
Switch# show mac-address-table notification change

MAC Notification Feature is Disabled on the switch
MAC Notification Flags For All Ethernet Interfaces :
-----
Interface                               MAC Added Trap  MAC Removed Trap
-----
```

The following example shows how to display the MAC notification parameters and history table for a specific interface:

```
Switch# show mac-address-table notification change interface gigabitethernet5/2

MAC Notification Feature is Disabled on the switch
Interface                               MAC Added Trap  MAC Removed Trap
-----
GigabitEthernet5/2                     Disabled        Disabled
```

The following example shows how to display unicast-flood information:

```
Switch# show mac-address-table unicast-flood

> > Unicast Flood Protection status: enabled
> >
> > Configuration:
> > vlan Kfps action timeout
> > -----+-----+-----+-----
> > 2 2 alert none
> >
> > Mac filters:
> > No. vlan source mac addr. installed
> > on time left (mm:ss)
> >
> > -----+-----+-----+-----+-----+-----
> >
> > Flood details:
> > Vlan source mac addr. destination mac addr.
> >
> > -----+-----+-----+-----+-----+-----
> > 2 0000.0000.cafe 0000.0000.bad0, 0000.0000.babe,
> > 0000.0000.bac0
> > 0000.0000.bac2, 0000.0000.bac4,
> > 0000.0000.bac6
> > 0000.0000.bac8
> > 2 0000.0000.caff 0000.0000.bad1, 0000.0000.babf,
> > 0000.0000.bac1
> > 0000.0000.bac3, 0000.0000.bac5,
> > 0000.0000.bac7
> > 0000.0000.bac9
```

The following example shows how to display the information about the MAC-address table for a specific VLAN:

```
Switch#show mac-address-table vlan 100

vlan    mac address      type    protocol  qos    ports
-----+-----+-----+-----+-----+-----
100     0050.3e8d.6400      static  assigned  --     Router
100     0050.7312.0cff      dynamic ip       --     Fa5/9
100     0080.1c93.8040      dynamic ip       --     Fa5/9
100     0050.3e8d.6400      static  ipx      --     Router
100     0050.3e8d.6400      static  other    --     Router
```

```

100 0100.0cdd.dddd static other -- Fa5/9,Router,Switch
100 00d0.5870.a4ff dynamic ip -- Fa5/9
100 00e0.4fac.b400 dynamic ip -- Fa5/9
100 0100.5e00.0001 static ip -- Fa5/9,Switch
100 0050.3e8d.6400 static ip -- Router

```

The following example shows how to display the information about the MAC address table for MLDv2 snooping:

```
Switch# show mac-address-table multicast mld-snooping
```

```

vlan mac address type learn qos ports
-----+-----+-----+-----+-----+-----
--- 3333.0000.0001 static Yes - Switch,Stby-Switch
--- 3333.0000.000d static Yes - Fa2/1,Fa4/1,Router,Switch
--- 3333.0000.0016 static Yes - Switch,Stby-Switch

```

The table below describes the significant fields shown in the displays.

Table 10: show mac-address-table Field Descriptions

Field	Description
Dynamic Addresses Count	Total number of dynamic addresses in the MAC address table.
Secure Addresses (User-defined) Count	Total number of secure addresses in the MAC address table.
Static Addresses (User-defined) Count	Total number of static addresses in the MAC address table.
System Self Addresses Count	Total number of addresses in the MAC address table.
Total MAC addresses	Total MAC addresses in the MAC address table.
Destination Address	Destination addresses present in the MAC address table.
Address Type	Address type: static or dynamic.
VLAN	VLAN number.
Destination Port	Destination port information present in the MAC address table.
mac address	The MAC address of the entry.
protocol	Protocol present in the MAC address table.
qos	Quality of service associated with the MAC address table.
ports	Port type.

Field	Description
age	The time in seconds since last occurrence of the interface.
Aging Time	Aging time for entries.
module	Module number.
action	Type of action.
flooding	Status of the flooding.

Related Commands

Command	Description
clear mac-address-table	Deletes entries from the MAC address table.
mac-address-table aging-time	Configures the aging time for entries in the Layer 2 table.
mac-address-table limit	Enables MAC limiting.
mac-address-table notification mac-move	Enables MAC-move notification.
mac-address-table static	Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.
mac-address-table synchronize	Synchronizes the Layer 2 MAC address table entries across the PFC and all the DFCs.
show mac-address-table static	Displays only static MAC address table entries.



show parameter-map type consent through show users

- [show port-security, page 80](#)
- [show privilege, page 82](#)
- [show radius statistics, page 83](#)
- [show ssh, page 89](#)

show port-security

To display information about the port-security setting in EXEC command mode, use the **show port-security** command.

show port-security [**interface** *interface interface-number*]

show port-security [**interface** *interface interface-number*] {**address**| **vlan**}

Syntax Description

interface <i>interface</i>	(Optional) Specifies the interface type; possible valid values are ethernet , fastethernet , gigabitethernet , and longreachethernet .
<i>interface-number</i>	Interface number. Valid values are 1 to 6.
address	Displays all the secure MAC addresses that are configured on all the switch interfaces or on a specified interface with aging information for each address.
vlan	Virtual LAN.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	The address keyword was added to display the maximum number of MAC addresses configured per VLAN on a trunk port on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

The **vlan** keyword is supported on trunk ports only and displays per-Vlan maximums set on a trunk port.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Examples

This example shows the output from the **show port-security** command when you do not enter any options:

```
Router# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action                                     (Count)      (Count)        (Count)
-----
Fa5/1            11             11           0                  Shutdown
Fa5/5            15             5            0                  Restrict
Fa5/11           5              4            0                  Protect
-----
```

```
Total Addresses in System: 21
Max Addresses limit in System: 128
Router#
```

This example shows how to display port-security information for a specified interface:

```
Router# show port-security interface fastethernet 5/1
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
Router#
```

This example show how to display all the secure MAC addresses that are configured on all the switch interfaces or on a specified interface with aging information for each address:

```
Router# show port-security address
Default maximum: 10
VLAN Maximum Current
1      5          3
2      4          4
3      6          4
Router#
```

Related Commands

Command	Description
clear port-security	Deletes configured secure MAC addresses and sticky MAC addresses from the MAC address table.

show privilege

To display your current level of privilege, use the **show privilege** command in EXEC mode.

show privilege

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows sample output from the **show privilege** command. The current privilege level is 15.

```
Router# show privilege
Current privilege level is 15
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the enable password command.

show radius statistics

To display the RADIUS statistics for accounting and authentication packets, use the **show radius statistics** command in user EXEC or privileged EXEC mode.

show radius statistics

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC (>) Privileged EXEC (#)

Command History	Release	Modification
	12.1(3)T	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S. Support for the CISCO-RADIUS-EXT-MIB was added.
	15.1(4)M	This command was modified. Support for the CISCO-RADIUS-EXT-MIB was added.

Examples The following is sample output from the **show radius statistics** command:

```
Router# show radius statistics
Auth.      Acct.      Both
Maximum inQ length:      NA      NA      1
Maximum waitQ length:    NA      NA      2
Maximum doneQ length:    NA      NA      1
Total responses seen:     33      67     100
Packets with responses:   33      67     100
Packets without responses: 0       0       0
Access Rejects           : 0
Average response delay(ms) : 1331    124    523
Maximum response delay(ms): 5720    4800   5720
Number of Radius timeouts: 8        2      10
Duplicate ID detects:     0        0       0
Buffer Allocation Failures: 0        0       0
Maximum Buffer Size (bytes): 156     327    327
Malformed Responses      : 0        0       0
Bad Authenticators       : 0        0       0
Source Port Range: (2 ports only)
1645 - 1646
Last used Source Port/Identifier:
1645/33
1646/69
```

The table below describes significant fields shown in the display.

Table 11: show radius statistics Field Descriptions

Field	Description
Auth.	Statistics for authentication packets.
Acct.	Statistics for accounting packets.
Both	Combined statistics for authentication and accounting packets.
Maximum inQ length	Maximum number of entries allowed in the queue that holds the RADIUS messages not yet sent.
Maximum waitQ length	Maximum number of entries allowed in the queue that holds the RADIUS messages that have been sent and are waiting for a response.
Maximum doneQ length	Maximum number of entries allowed in the queue that holds the messages that have received a response and will be forwarded to the code that is waiting for the messages.
Total responses seen	Number of RADIUS responses seen from the server. In addition to the expected packets, the number includes repeated packets and packets that do not have a matching message in the waitQ.
Packets with responses	Number of packets that received a response from the RADIUS server.
Packets without responses	Number of packets that never received a response from any RADIUS server.
Access Rejects	Number of times access requests have been rejected by a RADIUS server.
Average response delay	Average time, in milliseconds (ms), from when the packet was first transmitted to when it received a response. If the response timed out and the packet was sent again, this value includes the timeout. If the packet never received a response, this value is not included in the average.
Maximum response delay	Maximum delay, in ms, observed while gathering the average response delay information.
Number of RADIUS timeouts	Number of times a server did not respond and the RADIUS server re-sent the packet.

Field	Description
Duplicate ID detects	RADIUS has a maximum of 255 unique IDs. In some instances, there can be more than 255 outstanding packets. When a packet is received, the doneQ is searched from the oldest entry to the youngest. If the IDs are the same, further techniques are used to see if this response matches this entry. If this response does not match, the duplicate ID detect counter is increased.
Buffer Allocation Failures	Number of times the buffer failed to get allocated.
Maximum Buffer Size (bytes)	Displays the maximum size of the buffer.
Malformed Responses	Number of corrupted responses, mostly due to bad authenticators.
Bad Authenticators	Number of authentication failures due to shared secret mismatches.
Source Port Range: (2 ports only)	Displays the port numbers.
Last used Source Port/Identifier	Ports that were last used by the RADIUS server for authentication.

The fields in the output are mapped to Simple Network Management Protocol (SNMP) objects in the CISCO-RADIUS-EXT-MIB and are used in SNMP reporting. The first line of the report is mapped to the CISCO-RADIUS-EXT-MIB as follows:

- Maximum inQ length maps to creClientTotalMaxInQLength
- Maximum waitQ length maps to creClientTotalMaxWaitQLength
- Maximum doneQ length maps to creClientTotalMaxDoneQLength

The field "Both" in the output can be derived from the authentication and accounting MIB objects. The calculation formula for each field, as displayed in the output, is given in the table below.

Table 12: Calculation Formula for the Both field in show radius statistics Command Output

show radius statistics Command Output Data	Calculation Formula for the Both Field
Maximum inQ length	creClientTotalMaxInQLength
Maximum waitQ length	creClientTotalWaitQLength
Maximum doneQ length	creClientDoneQLength
Total responses seen	creAuthClientTotalResponses + creAcctClientTotalResponses

show radius statistics Command Output Data	Calculation Formula for the Both Field
Packets with responses	creAuthClientTotalPacketsWithResponses + creAcctClientTotalPacketsWithResponses
Packets without responses	creAuthClientTotalPacketsWithoutResponses + creAcctClientTotalPacketsWithoutResponses
Access Rejects	creClientTotalAccessRejects
Average response delay	creClientAverageResponseDelay
Maximum response delay	MAX(creAuthClientMaxResponseDelay, creAcctClientMaxResponseDelay)
Number of RADIUS timeouts	creAuthClientTimeouts + creAcctClientTimeouts
Duplicate ID detects	creAuthClientDupIDs + creAcctClientDupIDs
Buffer Allocation Failures	creAuthClientBufferAllocFailures + creAcctClientBufferAllocFailures
Maximum Buffer Size (bytes)	MAX(creAuthClientMaxBufferSize, creAcctClientMaxBufferSize)
Malformed Responses	creAuthClientMalformedResponses + creAcctClientMalformedResponses
Bad Authenticators	creAuthClientBadAuthenticators + creAcctClientBadAuthenticators

Mapping the following set of objects listed in the CISCO-RADIUS-EXT-MIB map to fields displayed by the **show radius statistics** command is straightforward. For example, the creClientLastUsedSourcePort field corresponds to the Last used Source Port/Identifier portion of the report, creAuthClientBufferAllocFailures corresponds to the Buffer Allocation Failures for authentication packets, creAcctClientBufferAllocFailure corresponds to the Buffer Allocation Failures for accounting packets, and so on.

- creClientTotalMaxInQLength
- creClientTotalMaxWaitQLength
- creClientTotalMaxDoneQLength
- creClientTotalAccessRejects
- creClientTotalAverageResponseDelay
- creClientSourcePortRangeStart
- creClientSourcePortRangeEnd
- creClientLastUsedSourcePort
- creClientLastUsedSourceId

- creAuthClientBadAuthenticators
- creAuthClientUnknownResponses
- creAuthClientTotalPacketsWithResponses
- creAuthClientBufferAllocFailures
- creAuthClientTotalResponses
- creAuthClientTotalPacketsWithoutResponses
- creAuthClientAverageResponseDelay
- creAuthClientMaxResponseDelay
- creAuthClientMaxBufferSize
- creAuthClientTimeouts
- creAuthClientDupIDs
- creAuthClientMalformedResponses
- creAuthClientLastUsedSourceId
- creAcctClientBadAuthenticators
- creAcctClientUnknownResponses
- creAcctClientTotalPacketsWithResponses
- creAcctClientBufferAllocFailures
- creAcctClientTotalResponses
- creAcctClientTotalPacketsWithoutResponses
- creAcctClientAverageResponseDelay
- creAcctClientMaxResponseDelay
- creAcctClientMaxBufferSize
- creAcctClientTimeouts
- creAcctClientDupIDs
- creAcctClientMalformedResponses
- creAcctClientLastUsedSourceId

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <http://www.cisco.com/go/mibs> .

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.

Command	Description
radius-server retransmit	Specifies how many times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval for which a router waits for a server host to reply.

show ssh

To display the status of Secure Shell (SSH) server connections on the router, use the **show ssh** command in user EXEC or privileged EXEC mode.

show ssh vty [*ssh-number*]

Syntax Description

vty	Displays virtual terminal line (VTY) connection details.
<i>ssh-number</i>	(Optional) The number of SSH server connections on the router. Range is from 0 to 1510. The default value is 0.

Command Modes

User Exec (>) Privileged EXEC (#)

Command History

Release	Modification
12.1(15)T	This command was introduced.
12.2(33)SRA	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was modified. It was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **show ssh** command to display the status of the SSH connections on your router. This command does not display any SSH configuration data. Use the **show ip ssh** command for SSH configuration information such as timeouts and retries.

Examples

The following is sample output from the **show ssh** command with SSH enabled:

```
Router# show ssh
Connection    Version    Encryption    State          Username
0             1.5        3DES          Session Started guest
```

The table below describes the significant fields shown in the display.

Table 13: show ssh Field Descriptions

Field	Description
Connection	Number of SSH connections on the router.
Version	Version number of the SSH terminal.
Encryption	Type of transport encryption.
State	The status of SSH connection to indicate if the session has started or stopped.
Username	Username to log in to the SSH.

Related Commands

Command	Description
show ip ssh	Displays version and configuration data for SSH.



showvlanthroughswitchportport-security violation

- [single-connection](#), page 92
- [source](#), page 93
- [ssh](#), page 95
- [switchport port-security](#), page 100

single-connection

To enable all TACACS packets to be sent to the same server using a single TCP connection, use the **single-connection** command in TACACS+ server configuration mode. To disable this feature, use the **no** form of this command.

single-connection

no single-connection

Syntax Description This command has no arguments or keywords.

Command Default TACACS packets are not sent on a single TCP connection.

Command Modes TACACS+ server configuration (config-server-tacacs)

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines Use the **single-connection** command to multiplex all TACACS packets to the same server over a single TCP connection.

Examples The following example shows how to multiplex all TACACS packets over a single TCP connection to the TACACS server:

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# single-connection
```

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters config server tacacs mode.

source

To sequentially number the source address, use the **source** command in IKEv2 FlexVPN client profile configuration mode. To remove the sequence, use the **no** form of this command.

source *sequence* *interface* **track** *track-number*

no source *sequence*

Syntax Description

<i>sequence</i>	Assigns a sequence number.
<i>interface</i>	Interface type and number.
track <i>track-number</i>	Tracks the source address with a track number.

Command Default

The track status is always up.

Command Modes

IKEv2 FlexVPN client profile configuration (config-ikev2-flexvpn)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

Before you enable this command, you must configure the **crypto ikev2 client flexvpn** command.

The source address is the one with the lowest sequence number for which track object is in the UP state only if the source IP address is available in the tunnel VRF of the tunnel interface. If a session is UP for a source, the source is said to be a "Current active source".



Note

Any changes to this command terminates the active session.

Examples

The following example shows how to define a static peer:

```
Router(config)# crypto ikev2 client flexvpn client1  
Router(config-ikev2-flexvpn)# source 1 Ethernet 0/1 track 11
```

Related Commands

Command	Description
crypto ikev2 client flexvpn	Defines an IKEv2 FlexVPN client profile.

ssh

To start an encrypted session with a remote networking device, use the **ssh** command in privileged EXEC or user EXEC mode.

ssh [-v {1| 2}] [-c {3des| aes128-cbc| aes192-cbc| aes256-cbc}] [-l *userid*] [-l *userid:vrfname number ip-address ip-address*] [-l *userid:rotary number ip-address*] [-m {hmac-md5| hmac-md5-96| hmac-sha1| hmac-sha1-96}] [-o *numberofpasswordprompts n*] [-p *port-num*] [*ip-addr*] [*hostname*] [*command*] [-vrf]

Syntax Description

-v	(Optional) Specifies the version of Secure Shell (SSH) to use to connect to the server. <ul style="list-style-type: none"> • 1 --Connects using SSH Version 1. • 2 --Connects using SSH Version 2.
-c { 3des aes128-cbc aes192-cbc aes256-cbc }	(Optional) Specifies the crypto algorithms Data Encryption Standard (DES), Triple DES (3DES), or Advanced Encryption Standard (AES) to use for encrypting data. AES algorithms supported are aes128-cbc, aes192-cbc, and aes256-cbc. <ul style="list-style-type: none"> • To use SSH Version 1, you must have an encryption image running on the router. Cisco software images that include encryption have the designators "k8" (DES) or "k9" (3DES). • SSH Version 2 supports only the following crypto algorithms: aes128-cbc, aes192-cbc, aes256-cbc, and 3des-cbc. SSH Version 2 is supported only in 3DES images. • If you do not specify the -c keyword, during negotiation the remote networking device sends all the supported crypto algorithms. • If you configure the -c keyword and the server does not support the argument that you have shown (des, 3des, aes128-cbc, aes192-cbc, or aes256-cbc), the remote networking device closes the connection.
-l <i>userid</i>	(Optional) Specifies the user ID to use when logging in on the remote networking device running the SSH server. If no user ID is specified, the default is the current user ID.

<p>-l <i>userid</i> : <i>vrfname</i> <i>number</i> <i>ip-address</i></p>	<p>(Optional) Specifies the user ID when configuring reverse SSH by including port information in the <i>userid</i> field.</p> <ul style="list-style-type: none"> • --Signifies that a port number and terminal IP address will follow the user ID. • <i>vrfname</i> -- User specific VRF. • <i>number</i> --Terminal or auxiliary line number. • <i>ip-address</i> --IP address of the terminal server. <p>Note The <i>userid</i> argument and : <i>number ip-address</i> delimiter and arguments must be used if you are configuring reverse SSH by including port information in the <i>userid</i> field (a method that is easier than the longer method of listing each terminal or auxiliary line on a separate command configuration line). The <i>vrfname</i> allows SSH to establish sessions with hosts whose addresses are in a VRF instance.</p>
<p>-l <i>userid</i> :rotary <i>number</i> <i>ip-address</i></p>	<p>(Optional) Specifies that the terminal lines are to be grouped under the rotary group for reverse SSH.</p> <ul style="list-style-type: none"> • --Signifies that a rotary group number and terminal IP address will follow. • <i>number</i> --Terminal or auxiliary line number. • <i>ip-address</i> --IP address of the terminal server. <p>Note The <i>userid</i> argument and :rotary{ <i>number</i> } {<i>ip-address</i>} delimiter and arguments must be used if you are configuring reverse SSH by including rotary information in the <i>userid</i> field (a process that is easier than the longer process of listing each terminal or auxiliary line on a separate command configuration line).</p>
<p>-m {hmac-md5 hmac-md5-96 hmac-sha1 hmac-sha1-96</p>	<p>(Optional) Specifies a Hashed Message Authentication Code (HMAC) algorithm.</p> <ul style="list-style-type: none"> • SSH Version 1 does not support HMACs. • If you do not specify the -m keyword, the remote device sends all the supported HMAC algorithms during negotiation. If you specify the -m keyword and the server does not support the argument that you have shown (hmac-md5, hmac-md5-96, hmac-sha1, and hmac-sha1-96), the remote device closes the connection.

-o numberofpasswordprompts <i>n</i>	(Optional) Specifies the number of password prompts that the software generates before ending the session. The SSH server may also apply a limit to the number of attempts. If the limit set by the server is less than the value specified by the -o numberofpasswordprompts keyword, the limit set by the server takes precedence. The default is 3 attempts, which is also the Cisco IOS SSH server default. The range of values is from 1 to 5.
-p <i>port-num</i>	(Optional) Indicates the desired port number for the remote host. The default port number is 22.
<i>ip-addr</i> <i>hostname</i>	Specifies the IPv4 or IPv6 address or host name of the remote networking device.
<i>command</i>	(Optional) Specifies the Cisco IOS command that you want to run on the remote networking device. If the remote host is not running Cisco IOS software, this may be any command recognized by the remote host. If the command includes spaces, you must enclose the command in quotation marks.
-vrf	(Optional) Adds VRF awareness to SSH client side functionality. VRF instance name in the client is provided with the IP address to lookup the correct routing table and establish a connection.

Command Default No encrypted session exists if the command is not used.

Command Modes User EXEC (>) Privileged EXEC (#)

Command History	Release	Modification
	12.1(3)T	This command was introduced.
	12.2(8)T	Support for IPv6 addresses was added.
	12.0(21)ST	IPv6 address support was integrated into Cisco IOS Release 12.0(21)ST.
	12.0(22)S	IPv6 address support was integrated into Cisco IOS Release 12.0(22)S.
	12.2(14)S	IPv6 address support was integrated into Cisco IOS Release 12.2(14)S.
	12.2(17a)SX	This command was integrated into Cisco IOS Release 12.2(17a)SX.

Release	Modification
12.3(7)T	This command was expanded to include Secure Shell Version 2 support. The -c keyword was expanded to include support for the following cryptic algorithms: aes128-cbc, aes192-cbc, and aes256-cbc. The -m keyword was added, with the following algorithms: hmac-md5, hmac-md5-96, hmac-sha1, and hmac-sha1-96. The -v keyword and arguments 1 and 2 were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	The -I userid : number ip-address and -I userid : rotary number ip-address keyword and argument options were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.3(7)JA	This command was integrated into Cisco IOS Release 12.3(7)JA.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	The -I userid : vrfname number ip-address keyword and argument and -vrf keyword were added.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The **ssh** command enables a Cisco router to make a secure, encrypted connection to another Cisco router or device running an SSH Version 1 or Version 2 server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.



Note

SSH Version 1 is supported on DES (56-bit) and 3DES (168-bit) data encryption software images only. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.

- SSH Version 2 supports only the following crypto algorithms: aes128-cbc, aes192-cbc, and aes256-cbc. SSH Version 2 is supported only in 3DES images.
- SSH Version 1 does not support HMAC algorithms.

The following example illustrates the initiation of a secure session between the local router and the remote host HQhost to run the **show users** command. The result of the **show users** command is a list of valid users who are logged in to HQhost. The remote host will prompt for the adminHQ password to authenticate the

user adminHQ. If the authentication step is successful, the remote host will return the result of the **show users** command to the local router and will then close the session.

```
ssh -l adminHQ HQhost "show users"
```

The following example illustrates the initiation of a secure session between the local router and the edge router HQedge to run the **show ip route** command. In this example, the edge router prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the edge router will return the result of the **show ip route** command to the local router.

```
ssh -l adminHQ HQedge "show ip route"
```

The following example shows the SSH client using 3DES to initiate a secure remote command connection with the HQedge router. The SSH server running on HQedge authenticates the session for the admin7 user on the HQedge router using standard authentication methods. The HQedge router must have SSH enabled for authentication to work.

```
ssh -l admin7 -c 3des -o numberofpasswordprompts 5 HQedge
```

The following example shows a secure session between the local router and a remote IPv6 router with the address 3ffe:1111:2222:1044::72 to run the **show running-config** command. In this example, the remote IPv6 router prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the remote IPv6 router will return the result of the **show running-config** command to the local router and will then close the session.

```
ssh -l adminHQ 3ffe:1111:2222:1044::72 "show running-config"
```



Note

A hostname that maps to the IPv6 address 3ffe:1111:2222:1044::72 could have been used in the last example.

The following example shows a SSH Version 2 session using the crypto algorithm aes256-cbc and an HMAC of hmac-sha1-96. The user ID is user2, and the IP address is 10.76.82.24.

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-96 -l user2 10.76.82.24
```

The following example shows that reverse SSH has been configured on the SSH client:

```
ssh -l lab:1 router.example.com
```

The following command shows that Reverse SSH will connect to the first free line in the rotary group:

```
ssh -l lab:rotary1 router.example.com
```

Related Commands

Command	Description
ip ssh	Configures SSH server control parameters on the router.
show ip ssh	Displays the version and configuration data for SSH.
show ssh	Displays the status of SSH server connections.

switchport port-security

To enable port security on an interface, use the **switchport port-security** command in interface configuration mode. To disable port security, use the **no** form of this command.

switchport port-security

no switchport port-security

Syntax Description This command has no keywords or arguments.

Command Default Disabled

Command Modes Interface configuration

Command History	Release	Modification
	12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
	12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
	12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: <ul style="list-style-type: none"> • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines Follow these guidelines when configuring port security:

- With Release 12.2(18)SXE and later releases, port security is supported on trunks.
- With releases earlier than Release 12.2(18)SXE, port security is not supported on trunks.
- With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
- With releases earlier than Release 12.2(18)SXE, port security is not supported on 802.1Q tunnel ports.
- A secure port cannot be a destination port for a Switch Port Analyzer (SPAN).
- A secure port cannot belong to an EtherChannel.
- A secure port cannot be a trunk port.

- A secure port cannot be an 802.1X port. If you try to enable 802.1X on a secure port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to a secure port, an error message appears, and the security settings are not changed.

Examples

This example shows how to enable port security:

```
Router(config-if) #  
switchport port-security
```

This example shows how to disable port security:

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.



tacacs-server administration through title-color

- [tacacs server, page 104](#)
- [tacacs-server host, page 106](#)
- [telnet, page 109](#)
- [test aaa group, page 115](#)
- [timeout \(TACACS+\), page 119](#)

tacacs server

To configure the TACACS+ server for IPv6 or IPv4 and enter TACACS+ server configuration mode, use the **tacacs server** command in global configuration mode. To remove the configuration, use the **no** form of this command.

tacacs server *name*

no tacacs server

Syntax Description

name	Name of the private TACACS+ server host.
------	--

Command Default

No TACACS+ server is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **tacacs server** command configures the TACACS server using the *name* argument and enters TACACS+ server configuration mode. The configuration is applied once you have finished configuration and exited TACACS+ server configuration mode.

Examples

The following example shows how to configure the TACACS server using the name server1 and enter TACACS+ server configuration mode to perform further configuration:

```
Router(config)# tacacs server server1
Router(config-server-tacacs)#
```

Related Commands

Command	Description
address ipv6 (TACACS+)	Configures the IPv6 address of the TACACS+ server.
key (TACACS+)	Configures the per-server encryption key on the TACACS+ server.
port (TACACS+)	Specifies the TCP port to be used for TACACS+ connections.

Command	Description
send-nat-address (TACACS+)	Sends a client's post-NAT address to the TACACS+ server.
single-connection (TACACS+)	Enables all TACACS packets to be sent to the same server using a single TCP connection.
timeout (TACACS+)	Configures the time to wait for a reply from the specified TACACS server.

tacacs-server host

To specify a TACACS+ host, use the **tacacs-server host** command in global configuration mode. To delete the specified name or address, use the **no** form of this command.

```
tacacs-server host {host-name|  
host-ip-address} [keystring] [nat] [port integer ] [single-connection] [timeout integer ]]  
no tacacs-server host {host-name | host-ip-address}
```

Syntax Description

<i>host-name</i>	Name of the host.
<i>host-ip-address</i>	IP address of the host.
key	(Optional) Specifies an authentication and encryption key. This must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global command tacacs-server key for this server only.
<i>string</i>	(Optional) Character string specifying authentication and encryption key.
nat	(Optional) Port Network Address Translation (NAT) address of the client is sent to the TACACS+ server.
port	(Optional) Specifies a TACACS+ server port number. This option overrides the default, which is port 49.
<i>integer</i>	(Optional) Port number of the server. Valid port numbers range from 1 through 65535.
single-connection	(Optional) Maintains a single open connection between the router and the TACACS+ server.
timeout	(Optional) Specifies a timeout value. This overrides the global timeout value set with the tacacs-server timeout command for this server only.
<i>integer</i>	(Optional) Integer value, in seconds, of the timeout interval. The value is from 1 through 1000.

Command Default No TACACS+ host is specified.

Command Modes Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(11), 12.2(6)	The nat keyword was added.
12.2(8)T	The nat keyword was integrated into Cisco IOS Release 12.2(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can use multiple **tacacs-server host** commands to specify additional hosts. The Cisco IOS software searches for hosts in the order in which you specify them. Use the **port**, **timeout**, **key**, **single-connection**, and **nat** keywords only when running a AAA/TACACS+ server.

Because some of the parameters of the **tacacs-server host** command override global settings made by the **tacacs-server timeout** and **tacacs-server key** commands, you can use this command to enhance security on your network by uniquely configuring individual routers.

The **single-connection** keyword specifies a single connection (only valid with CiscoSecure Release 1.0.1 or later). Rather than have the router open and close a TCP connection to the server each time it must communicate, the single-connection option maintains a single open connection between the router and the server. The single connection is more efficient because it allows the server to handle a higher number of TACACS operations.

Examples

The following example specifies a TACACS+ host named Sea_Change:

```
tacacs-server host Sea_Change
```

The following example specifies that, for authentication, authorization, and accounting (AAA) confirmation, the router consults the TACACS+ server host named Sea_Cure on port number 51. The timeout value for requests on this connection is three seconds; the encryption key is a_secret.

```
tacacs-server host Sea_Cure port 51 timeout 3 key a_secret
```

Related Commands

Command	Description
aaa authentication	Specifies or enables AAA authentication.
aaa authorization	Sets parameters that restrict user access to a network.
aaa accounting	Enables AAA accounting of requested services for billing or security.
ppp	Starts an asynchronous connection using PPP.

Command	Description
slip	Starts a serial connection to a remote host using SLIP.
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.

telnet

To log in to a host that supports Telnet, use the **telnet** command in user EXEC or privileged EXEC mode.

telnet *host* [*port*] [*keyword*]

Syntax Description

<i>host</i>	A hostname or an IP address.
<i>port</i>	(Optional) A decimal TCP port number, or port name; the default is the Telnet router port (decimal 23) on the host.
<i>keyword</i>	(Optional) One of the keywords listed in the table below.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(21)ST	The /ipv4 and /ipv6 keywords were added.
12.1	The /quiet keyword was added.
12.2(2)T	The /ipv4 and /ipv6 keywords were added.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The table below lists the optional **telnet** command keywords.

Table 14: telnet Keyword Options

Option	Description
/debug	Enables Telnet debugging mode.
/encrypt kerberos	<p>Enables an encrypted Telnet session. This keyword is available only if you have the Kerberized Telnet subsystem.</p> <p>If you authenticate using Kerberos Credentials, the use of this keyword initiates an encryption negotiation with the remote server. If the encryption negotiation fails, the Telnet connection will be reset. If the encryption negotiation is successful, the Telnet connection will be established, and the Telnet session will continue in encrypted mode (all Telnet traffic for the session will be encrypted).</p>
/ipv4	Specifies version 4 of the IP protocol. If a version of the IP protocol is not specified in a network that supports both the IPv4 and IPv6 protocol stacks, IPv6 is attempted first and is followed by IPv4.
/ipv6	Specifies version 6 of the IP protocol. If a version of the IP protocol is not specified in a network that supports both the IPv4 and IPv6 protocol stacks, IPv6 is attempted first and is followed by IPv4.
/line	Enables Telnet line mode. In this mode, the Cisco IOS software sends no data to the host until you press the Enter key. You can edit the line using the standard Cisco IOS software command-editing characters. The /line keyword is a local switch; the remote router is not notified of the mode change.
/noecho	Disables local echo.
/quiet	Prevents onscreen display of all messages from the Cisco IOS software.
/route: path	Specifies loose source routing. The <i>path</i> argument is a list of hostnames or IP addresses that specify network nodes and ends with the final destination.
/source-interface	Specifies the source interface.

Option	Description
/stream	Turns on <i>stream</i> processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
<i>port-number</i>	Port number.
bgp	Border Gateway Protocol.
chargen	Character generator.
cmd <i>rcmd</i>	Remote commands.
daytime	Daytime.
discard	Discard.
domain	Domain Name Service.
echo	Echo.
exec	EXEC.
finger	Finger.
ftp	File Transfer Protocol.
ftp-data	FTP data connections (used infrequently).
gopher	Gopher.
hostname	Hostname server.
ident	Ident Protocol.
irc	Internet Relay Chat.
klogin	Kerberos login.
kshell	Kerberos shell.
login	Login (rlogin).
lpd	Printer service.
nntp	Network News Transport Protocol.

Option	Description
pim-auto-rp	Protocol Independent Multicast (PIM) auto-rendezvous point (RP).
node	Connect to a specific Local-Area Transport (LAT) node.
pop2	Post Office Protocol v2.
pop3	Post Office Protocol v3.
port	Destination local-area transport (LAT) port name.
smtp	Simple Mail Transfer Protocol.
sunrpc	Sun Remote Procedure Call.
syslog	Syslog.
tacacs	Specifies TACACS security.
talk	Talk (517).
telnet	Telnet (23).
time	Time (37).
uucp	UNIX-to-UNIX Copy Program (540).
whois	Nickname (43).
www	World Wide Web (HTTP, 80).

With the Cisco IOS implementation of TCP/IP, you are not required to enter the **connect** or **telnet** command to establish a terminal connection. You can enter only the learned hostname--as long as the following conditions are met:

- The hostname is different from a command word for the router.
- The preferred transport protocol is set to **telnet**.

To display a list of the available hosts, use the **show hosts** command. To display the status of all TCP connections, use the **show tcp** command.

The Cisco IOS software assigns a logical name to each connection, and several commands use these names to identify connections. The logical name is the same as the hostname, unless that name is already in use, or you change the connection name with the **name-connection EXEC** command. If the name is already in use, the Cisco IOS software assigns a null name to the connection.

The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter the escape sequence and then a command character. The default escape sequence is Ctrl-^ (press and hold the Ctrl and Shift keys and the 6 key). You can enter the command character as you hold down Ctrl or with Ctrl released; you can use either uppercase or lowercase letters. The table below lists the special Telnet escape sequences.

Table 15: Special Telnet Escape Sequences

Escape Sequence ¹	Purpose
Ctrl-^ b	Break
Ctrl-^ c	Interrupt Process (IP and IPv6)
Ctrl-^ h	Erase Character (EC)
Ctrl-^ o	Abort Output (AO)
Ctrl-^ t	Are You There? (AYT)
Ctrl-^ u	Erase Line (EL)

¹ The caret (^) symbol refers to Shift-6 on your keyboard.

At any time during an active Telnet session, you can list the Telnet commands by pressing the escape sequence keys followed by a question mark at the system prompt: **Ctrl-^ ?**

A sample of this list follows. In this sample output, the first caret (^) symbol represents the Ctrl key, and the second caret represents Shift-6 on your keyboard:

```
router> ^^?
[Special telnet escape help]
^^B  sends telnet BREAK
^^C  sends telnet IP
^^H  sends telnet EC
^^O  sends telnet AO
^^T  sends telnet AYT
^^U  sends telnet EL
```

You can have several concurrent Telnet sessions open and switch among them. To open a subsequent session, first suspend the current connection by pressing the escape sequence (Ctrl-Shift-6 then x [Ctrl^x] by default) to return to the system command prompt. Then open a new connection with the **telnet** command.

To terminate an active Telnet session, enter any of the following commands at the prompt of the device to which you are connecting:

- **close**
- **disconnect**
- **exit**
- **logout**
- **quit**

Examples

The following example establishes an encrypted Telnet session from a router to a remote host named host1:

```
router>
```

```
telnet host1 /encrypt kerberos
```

The following example routes packets from the source system host1 to example.com, then to 10.1.0.11, and finally back to *host1* :

```
router>
```

```
telnet host1 /route:example.com 10.1.0.11 host1
```

The following example connects to a host with the logical name host1:

```
router>
```

```
host1
```

The following example suppresses all onscreen messages from the Cisco IOS software during login and logout:

```
router>
```

```
telnet host2 /quiet
```

The following example shows the limited messages displayed when connection is made using the optional **/quiet** keyword:

```
login:User2
```

```
Password:
```

```
    Welcome to OpenVMS VAX version V6.1 on node CRAW
```

```
    Last interactive login on Tuesday, 15-DEC-1998 11:01
```

```
    Last non-interactive login on Sunday,  3-JAN-1999 22:32
```

```
Server3) logout
```

```
    User2          logged out at  16-FEB-2000 09:38:27.85
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
kerberos clients mandatory	Causes the rsh , rcp , rlogin , and telnet commands to fail if they cannot negotiate the Kerberos Protocol with the remote server.
name connection	Assigns a logical name to a connection.
rlogin	Logs in to a UNIX host using rlogin.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.
show tcp	Displays the status of TCP connections.

test aaa group

To associate a dialed number identification service (DNIS) or calling line identification (CLID) user profile with the record that is sent to the RADIUS server or to manually test load-balancing server status, use the **test aaa group** command in privileged EXEC mode.

DNIS and CLID User Profile

test aaa group {*group-name*| **radius**} *username password new-code* [**profile** *profile-name*]

RADIUS Server Load Balancing Manual Testing

test aaa group *group-name* [**server** *ip-address*] [**auth-port** *port-number*] [**acct-port** *port-number*] *username password new-code* [**count** *requests*] [**rate** *requests-per-second*] [**blocked** {*yes*| *no*}]

Syntax Description

<i>group-name</i>	Subset of RADIUS servers that are used, as defined by the server group <i>group-name</i> .
radius	Uses RADIUS servers for authentication.
<i>username</i>	Name for the test user. Caution If you use this command to manually test RADIUS load-balancing server state, it is recommended that a test user, one that is not defined on the RADIUS server, be used to protect against security issues that may arise if the test user is not correctly configured.
<i>password</i>	Password.
new-code	Code path through the new code, which supports a CLID or DNIS user profile association with a RADIUS server.
profile <i>profile-name</i>	(Optional) Identifies the user profile specified in the aaa user profile command. To associate a user profile with the RADIUS server, you must identify the user profile name.
server <i>ip-address</i>	(Optional) For RADIUS server load balancing, specifies to which server in the server group the test packets will be sent.
auth-port	(Optional) User Datagram Protocol (UDP) destination port for authentication requests.

<i>port-number</i>	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1646.
acct-port	(Optional) UDP destination port for accounting requests.
<i>port-number</i>	(Optional) Port number for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 1646.
count <i>requests</i>	(Optional) Number of authentication and accounting requests that are to be sent to the server for each port. Range: 1 to 50000. Default: 1.
rate <i>requests-per-second</i>	(Optional) Number of requests per second that are to be sent to the server. Range: 1 to 1000. Default: 10.
blocked { yes no }	(Optional) Specifies whether the request is sent in blocking or nonblocking mode. If the blocked keyword is not used and one request is sent, the default is yes ; if more than one request is sent, the default is no .

Command Default

DNIS or CLID attribute values are not sent to the RADIUS server.

RADIUS Server Load Balancing Manual Testing

RADIUS server load-balancing server status manual testing does not occur.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	The following keywords and arguments were added for configuring RADIUS load balancing manual testing functionality: server <i>ip-address</i> , auth-port <i>port-number</i> , acct-port <i>port-number</i> , count <i>request</i> , rate <i>requests-per-second</i> , blocked .
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)ZV1	This command was enhanced to show user attributes returned from RADIUS authentication when authentication is successful.

Release	Modification
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Usage Guidelines

The **test aaa group** command can be used to

- Associate a DNIS or CLID named user profile with the record that is sent to the RADIUS server, which can then access DNIS or CLID information when the server receives a RADIUS record.
- Verify RADIUS load-balancing server status.



Note

The **test aaa group** command does not work with TACACS+.

Examples

The following example shows how to configure a dnis = dnisvalue user profile named prfl1 and associate it with a **test aaa group** command:

```
aaa user profile prfl1
  aaa attribute dnis
  aaa attribute dnis dnisvalue
  no aaa attribute clid
! Attribute not found.
  aaa attribute clid clidvalue
  no aaa attribute clid
exit
!
! Associate the dnis user profile with the test aaa group command.
test aaa group radius user1 pass new-code profile prfl1
```

The following example shows the response from a load-balanced RADIUS server that is alive when the username "test" does not match a user profile. The server is verified alive when it issues an Access-Reject response to a AAA packet generated by the **test aaa group** command.

```
Router# test aaa group SG1 test lab new-code

00:06:07: RADIUS/ENCODE(00000000):Orig. component type = INVALID
00:06:07: RADIUS/ENCODE(00000000): dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:06:07: RADIUS(00000000): Config NAS IP: 192.0.2.4
00:06:07: RADIUS(00000000): sending
00:06:07: RADIUS/ENCODE: Best Local IP-Address 192.0.2.141 for Radius-Server 192.0.2.176
00:06:07: RADIUS(00000000): Send Access-Request to 192.0.2.176:1645 id 1645/1, len 50
00:06:07: RADIUS: authenticator CA DB F4 9B 7B 66 C8 A9 - D1 99 4E 8E A4 46 99 B4
00:06:07: RADIUS: User-Password [2] 18 *
00:06:07: RADIUS: User-Name [1] 6 "test"
00:06:07: RADIUS: NAS-IP-Address [4] 6 192.0.2.141
00:06:07: RADIUS: Received from id 1645/1 192.0.2.176:1645, Access-Reject, len 44
00:06:07: RADIUS: authenticator 2F 69 84 3E F0 4E F1 62 - AB B8 75 5B 38 82 49 C3
00:06:07: RADIUS: Reply-Message [18] 24
00:06:07: RADIUS: 41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E 20 66 [Authentication ]
00:06:07: RADIUS: 61 69 6C 75 72 65 [failure]
00:06:07: RADIUS(00000000): Received from id 1645/1
00:06:07: RADIUS/DECODE: Reply-Message fragments, 22, total 22 bytes
```

Examples

The following example shows the user attribute list that the RADIUS server returns when you issue the test aaa command and authentication is successful:

```
Router# test aaa group radius viral viral new-code blocked no
AAA/SG/TEST: Sending 1 Access-Requests @ 10/sec, 0 Accounting-Requests @ 10/sec
CLI-1#
AAA/SG/TEST: Testing Status
AAA/SG/TEST:   Authen Requests to Send      : 1
AAA/SG/TEST:   Authen Requests Processed   : 1
AAA/SG/TEST:   Authen Requests Sent       : 1
AAA/SG/TEST:   Authen Requests Replied    : 1
AAA/SG/TEST:   Authen Requests Successful : 1
AAA/SG/TEST:   Authen Requests Failed     : 0
AAA/SG/TEST:   Authen Requests Error      : 0
AAA/SG/TEST:   Authen Response Received   : 1
AAA/SG/TEST:   Authen No Response Received: 0
AAA/SG/TEST: Testing Status
AAA/SG/TEST:   Account Requests to Send    : 0
AAA/SG/TEST:   Account Requests Processed   : 0
AAA/SG/TEST:   Account Requests Sent       : 0
AAA/SG/TEST:   Account Requests Replied    : 0
AAA/SG/TEST:   Account Requests Successful : 0
AAA/SG/TEST:   Account Requests Failed     : 0
AAA/SG/TEST:   Account Requests Error      : 0
AAA/SG/TEST:   Account Response Received   : 0
AAA/SG/TEST:   Account No Response Received: 0
USER ATTRIBUTES
username           "Username:viral"
nas-ip-address     3.1.1.1
interface          "210"
service-type       1 [Login]
Framed-Protocol    3 [ARAP]
ssg-account-info   "S20.5.0.2"
ssg-command-code   0B 4C 32 54 50 53 55 52 46
Router
```

Related Commands

Command	Description
aaa attribute	Adds DNIS or CLID attribute values to a user profile.
aaa user profile	Creates a AAA user profile.
load-balance	Enables RADIUS server load-balancing for RADIUS-named server groups.
radius-server host	Enables RADIUS automated testing for load balancing.
radius-server load-balance	Enables RADIUS server load-balancing for the global RADIUS server group.

timeout (TACACS+)

To configure the time to wait for a reply from the specified TACACS server, use the **timeout** command in TACACS+ server configuration mode. To return to the command default, use the **no** form of this command.

timeout *seconds*

no timeout *seconds*

Syntax Description

seconds	(Optional) Amount of time, in seconds.
---------	--

Command Default

Time to wait is 5 seconds.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use the **timeout** command to set the time, in seconds, to wait for a reply from the TACACS server. If the **timeout** command is configured, the specified number of seconds overrides the default time of 5 seconds.

Examples

The following example shows how to configure the wait time to 10 seconds:

```
Router(config)# tacacs server server1
Router(config-server-tacacs)# timeout 10
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS server configuration mode.

■ timeout (TACACS+)



traffic-export through zone security

- [username](#), page 122
- [username secret](#), page 129

username

To establish a username-based authentication system, use the **username** command in global configuration mode. To remove an established username-based authentication, use the **no** form of this command.

```

username name [aaa attribute list aaa-list-name]
username name [access-class access-list-number]
username name [autocommand command]
username name [callback-dialstring telephone-number]
username name [callback-line [tty] line-number [ ending-line-number ]]
username name [callback-rotary rotary-group-number]
username name [dnis]
username name [mac]
username name [nocallback-verify]
username name [noescape]
username name [nohangup]
username name [nopassword | password password] password encryption-type encrypted-password]
username name [one-time {password {0| 7| password}| secret {0| 5| password}}]
username name [password secret]
username name [privilege level]
username name [secret {0| 5| password}]
username name [user-maxlinks number]
username [lawful-intercept] name [privilege privilege-level] view view-name] password password
no username name

```

Syntax Description

<i>name</i>	Hostname, server name, user ID, or command name. The <i>name</i> argument can be only one word. Blank spaces and quotation marks are not allowed.
aaa attribute list <i>aaa-list-name</i>	Uses the specified authentication, authorization, and accounting (AAA) method list.
access-class <i>access-list-number</i>	(Optional) Specifies an outgoing access list that overrides the access list specified in the access-class command available in line configuration mode. It is used for the duration of the user's session.

autocommand <i>command</i>	(Optional) Causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and can contain embedded spaces, commands using the autocommand keyword must be the last option on the line.
callback-dialstring <i>telephone-number</i>	(Optional) For asynchronous callback only: permits you to specify a telephone number to pass to the DCE device.
callback-line <i>line-number</i>	(Optional) For asynchronous callback only: relative number of the terminal line (or the first line in a contiguous group) on which you enable a specific username for callback. Numbering begins with zero.
<i>ending-line-number</i>	(Optional) Relative number of the last line in a contiguous group on which you want to enable a specific username for callback. If you omit the keyword (such as tty), then line-number and ending-line-number are absolute rather than relative line numbers.
tty	(Optional) For asynchronous callback only: standard asynchronous line.
callback-rotary <i>rotary-group-number</i>	(Optional) For asynchronous callback only: permits you to specify a rotary group number on which you want to enable a specific username for callback. The next available line in the rotary group is selected. Range: 1 to 100.
dnis	Does not require a password when obtained via Dialed Number Identification Service (DNIS).
mac	Allows a MAC address to be used as the username for MAC filtering done locally.
nocallback-verify	(Optional) Specifies that the authentication is not required for EXEC callback on the specified line.
noescape	(Optional) Prevents a user from using an escape character on the host to which that user is connected.
nohangup	(Optional) Prevents Cisco IOS software from disconnecting the user after an automatic command (set up with the autocommand keyword) has completed. Instead, the user gets another EXEC prompt.

nopassword	No password is required for this user to log in. This is usually the most useful keyword to use in combination with the autocommand keyword.
password	Specifies the password to access the <i>name</i> argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the username command.
<i>password</i>	Password that a user enters.
<i>encryption-type</i>	Single-digit number that defines whether the text immediately following is encrypted and if so, what type of encryption is used. Defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using a Cisco-defined encryption algorithm.
<i>encrypted-password</i>	Encrypted password that a user enters.
one-time	Specifies that the username and password is valid for only one time. This configuration is used to prevent default credentials from remaining in user configurations.
0	Specifies that an unencrypted password or secret (depending on the configuration) follows.
7	Specifies that a hidden password follows.
5	Specifies that a hidden secret follows.
secret	Specifies a secret for the user.
<i>secret</i>	For Challenge Handshake Authentication Protocol (CHAP) authentication: specifies the secret for the local router or the remote device. The secret is encrypted when it is stored on the local router. The secret can consist of any string of up to 11 ASCII characters. There is no limit to the number of username and password combinations that can be specified, allowing any number of remote devices to be authenticated.
privilege <i>privilege-level</i>	(Optional) Sets the privilege level for the user. Range: 1 to 15.
user-maxlinks <i>number</i>	Maximum number of inbound links allowed for a user.

lawful-intercept	(Optional) Configures lawful intercept users on a Cisco device.
<i>name</i>	Hostname, server name, user ID, or command name. The <i>name</i> argument can be only one word. Blank spaces and quotation marks are not allowed.
view <i>view-name</i>	(Optional) For CLI view only: associates a CLI view name, which is specified with the parser view command, with the local AAA database.
password <i>password</i>	Password to access the CLI view.

Command Default

No username-based authentication system is established.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
11.1	This command was modified. The following keywords and arguments were added: <ul style="list-style-type: none"> • callback-dialstring <i>telephone-number</i> • callback-rotary <i>rotary-group-number</i> • callback-line [tty] <i>line-number</i> [<i>ending-line-number</i>] • nocallback-verify
12.3(7)T	This command was modified. The following keywords and arguments were added: <ul style="list-style-type: none"> • lawful-intercept • view • <i>view-name</i>
12.2(33)SRB	This command was modified. The following keywords and arguments were integrated into Cisco IOS Release 12.2(33)SRB: <ul style="list-style-type: none"> • lawful-intercept • view • <i>view-name</i>

Release	Modification
12.2(33)SB	This command was modified. The following keywords and arguments were integrated into Cisco IOS Release 12.2(33)SB: <ul style="list-style-type: none"> • lawful-intercept • view • <i>view-name</i>
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.4	This command was modified. The following keywords were integrated into Cisco IOS Release 12.4: <ul style="list-style-type: none"> • one-time • secret • 0, 5, 7
15.1(1)S	This command was modified. Support for the nohangup keyword was removed from Secure Shell (SSH).
Cisco IOS XE Release 3.2SE	This command was modified. The mac keyword was added.

Usage Guidelines

The **username** command provides username or password authentication, or both, for login purposes only.

Multiple **username** commands can be used to specify options for a single user.

Add a username entry for each remote system with which the local router communicates and from which it requires authentication. The remote device must have a username entry for the local router. This entry must have the same password as the local router's entry for that remote device.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an "info" username that does not require a password but connects the user to a general purpose information service.

The **username** command is required as part of the configuration for CHAP. Add a username entry for each remote system from which the local router requires authentication.



Note

To enable the local router to respond to remote CHAP challenges, one **username name** entry must be the same as the **hostname** entry that has already been assigned to the other router.

- To avoid the situation of a privilege level 1 user entering into a higher privilege level, configure a per-user privilege level other than 1 (for example, 0 or 2 through 15).

- Per-user privilege levels override virtual terminal privilege levels.

In Cisco IOS Release 15.1(1)S and later releases, the **nohangup** keyword is not supported with SSH. If the **username user autocommand command-name** command is configured and SSH is used, the session disconnects after executing the configured command once. This behavior with SSH is opposite to the Telnet behavior, where Telnet continuously asks for authentication and keeps executing the command until the user exits Telnet manually.

CLI and Lawful Intercept Views

Both CLI views and lawful intercept views restrict access to specified commands and configuration information. A lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of Simple Network Management Protocol (SNMP) commands that stores information about calls and users.

Users who are specified via the **lawful-intercept** keyword are placed in the lawful-intercept view, by default, if no other privilege level or view name has been explicitly specified.

If no value is specified for the *secret* argument and the **debug serial-interface** command is enabled, an error is displayed when a link is established and the CHAP challenge is not implemented. The CHAP debugging information is available using the **debug ppp negotiation**, **debug serial-interface**, and **debug serial-packet** commands. For more information about **debug** commands, refer to the *Cisco IOS Debug Command Reference*.

Examples

The following example shows how to implement a service similar to the UNIX **who** command, which can be entered at the login prompt and lists the current users of the router:

```
username who nopassword nohangup autocommand show users
```

The following example shows how to implement an information service that does not require a password to be used. The command takes the following form:

```
username info nopassword noescape autocommand telnet nic.ddn.mil
```

The following example shows how to implement an ID that works even if all the TACACS+ servers break. The command takes the following form:

```
username superuser password superpassword
```

The following example shows how to enable CHAP on interface serial 0 of "server_1." It also defines a password for a remote server named "server_r."

```
hostname server_1
username server_r password theirsystem
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

The following is output from the **show running-config** command displaying the passwords that are encrypted:

```
hostname server_1
username server_r password 7 121F0A18
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

In the following example, a privilege level 1 user is denied access to privilege levels higher than 1:

```
username user privilege 0 password 0 cisco
username user2 privilege 2 password 0 cisco
```

The following example shows how to remove the username-based authentication for user2:

```
no username user2
```

Related Commands

Command	Description
arap callback	Enables an ARA client to request a callback from an ARA client.
callback forced-wait	Forces the Cisco IOS software to wait before initiating a callback to a requesting client.
debug ppp negotiation	Displays PPP packets sent during PPP startup, where PPP options are negotiated.
debug serial-interface	Displays information about a serial connection failure.
debug serial-packet	Displays more detailed serial interface debugging information than you can obtain using debug serial interface command.
ppp callback (DDR)	Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.
ppp callback (PPP client)	Enables a PPP client to dial into an asynchronous interface and request a callback.
show users	Displays information about the active lines on the router.

username secret

To encrypt a user password with irreversible encryption, use the **username secret** command in global configuration mode.

username *name* **secret** {**0** *password*| **5** *secret-string*| **4** *secret-string*}

Syntax Description

<i>name</i>	Username.
0	Specifies an unencrypted secret.
<i>password</i>	Clear-text password.
5 <i>secret-string</i>	message digest algorithm5 (MD5) encrypted secret text string, which is stored as the encrypted user password.
4 <i>secret-string</i>	SHA256 encrypted secret text string, which is stored as the encrypted user password.

Command Default

No username-based authentication system is established.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(18)S	This command was introduced.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S. Encryption types 0 , 4 , and 5 were added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **username secret** command to configure a username and MD5-encrypted user password. MD5 encryption is a strong encryption method that is not retrievable; thus, you cannot use MD5 encryption with protocols that require clear-text passwords, such as Challenge Handshake Authentication Protocol (CHAP).

The **username secret** command provides an additional layer of security over the username password. It also provides better security by encrypting the password using non reversible MD5 encryption and storing the encrypted text. The added layer of MD5 encryption is useful in environments in which the password crosses the network or is stored on a TFTP server.

Use MD5 as the encryption type if you paste into this command an encrypted password that you copied from a router configuration file.

Use this command to enable Enhanced Password Security for the specified, un retrievable username. This command enables MD5 encryption on the password. MD5 encryption is a strong encryption method. You cannot use MD5 encryption with protocols, such as CHAP, that require clear-text passwords.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an "info" username that does not require a password but connects the user to a general-purpose information service.

The **username** command provides username or secret authentication for login purposes only. The *name* argument can be one word only. Spaces and quotation marks are not allowed. You can use multiple **username** commands to specify options for a single user.

Examples

The following example shows how to configure username "abc" and enable MD5 encryption on the clear-text password "xyz":

```
username abc secret 0 xyz
```

The following example shows how to configure username "cde" and enter an MD5 encrypted text string that is stored as the username password:

```
username cde secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

The following example shows how to configure username "xyz" and enter an MD5 encrypted text string that is stored as the username password:

```
username xyz secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the enable password command.
username	Establishes a username-based authentication system.