Cisco IOS Security Command Reference: Commands A to C, 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

© 2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **aaa authentication banner through aaa group server tacacs+** 1

aaa authentication banner 2

aaa authentication dot1x 4

aaa authentication fail-message 7

aaa authentication login 9

aaa authorization 13

aaa dnis map accounting network 19

aaa dnis map authentication group 22

aaa group server radius 24

aaa group server tacacs+ 27

CHAPTER 2 **aaa nas port extended through address ipv6 (TACACS+)** 31

aaa nas port extended 32

aaa new-model 34

aaa route download 36

aaa server radius dynamic-author 38

access-list (IP standard) 40

address ipv6 (config-radius-server) 44

address ipv6 (TACACS+) 46

CHAPTER 3 **authentication command bounce-port ignore through auth-type** 47

authentication command bounce-port ignore 48

authentication command disable-port ignore 49

authentication control-direction 50

authentication event fail 52

authentication event server alive action reinitialize 54

authentication event server dead action authorize 55

authentication fallback 57

authentication host-mode 58
authentication open 60
authentication order 61
authentication periodic 63
authentication port-control 64
authentication priority 66
authentication timer inactivity 68
authentication timer reauthenticate 70
authentication timer restart 72
authentication violation 74
auth-type 75

CHAPTER 4 **clear dot1x through clear eap** 77
clear dot1x 78
clear eap 80

CHAPTER 5 **client through crl** 83
client 84
crl 86

CHAPTER 6 **crypto ca authenticate through crypto ca trustpoint** 89
crypto ca authenticate 90
crypto ca enroll 92
crypto ca trustpoint 95

CHAPTER 7 **crypto key generate rsa** 99
crypto key generate rsa 100

aaa authentication banner through aaa group server tacacs+

- aaa authentication banner, page 2
- aaa authentication dot1x, page 4
- aaa authentication fail-message, page 7
- aaa authentication login, page 9
- aaa authorization, page 13
- aaa dnis map accounting network, page 19
- aaa dnis map authentication group, page 22
- aaa group server radius, page 24
- aaa group server tacacs+, page 27

aaa authentication banner

To configure a personalized banner that will be displayed at user login, use the **aaa authentication banner** command in global configuration mode. To remove the banner, use the no form of this command.

aaa authentication banner *dstringd*

no aaa authentication banner

Syntax Description

d	Any delimiting character at the beginning and end of the *string* that notifies the system that the *string* is to be displayed as the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.
string	Any group of characters, excluding the one used as the delimiter. The maximum number of characters that you can display is 2996.

Command Default

Not enabled

Command Modes

Global configuration

Command History

Release	Modification
11.3(4)T	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.

Usage Guidelines

Use the **aaa authentication banner** command to create a personalized message that appears when a user logs in to the system. This message or banner will replace the default message for user login.

To create a login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

Note The AAA authentication banner message is not displayed if TACACS+ is the first method in the method list.

Examples

The following example shows the default login message if **aaa authentication banner** is not configured. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication login default group radius
```

This configuration produces the following standard output:

```
User Verification Access
Username:
Password:
```

The following example configures a login banner (in this case, the phrase "Unauthorized use is prohibited.") that will be displayed when a user logs in to the system. In this case, the asterisk (*) symbol is used as the delimiter. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication banner *Unauthorized use is prohibited.*
aaa authentication login default group radius
```

This configuration produces the following login banner:

```
Unauthorized use is prohibited.
Username:
```

Related Commands

Command	Description
aaa authentication fail-message	Configures a personalized banner that will be displayed when a user fails login.

aaa authentication dot1x

To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X, use the **aaa authentication dot1x** command in global configuration mode. To disable authentication, use the **no** form of this command

aaa authentication dot1x {**default**| *listname*} *method1* [*method2* ...]

no aaa authentication dot1x {**default**| *listname*} *method1* [*method2* ...]

Syntax Description

default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
listname	Character string used to name the list of authentication methods tried when a user logs in.
method1 [*method2*...]	At least one of these keywords: • **enable** --Uses the enable password for authentication. • **group radius** --Uses the list of all RADIUS servers for authentication. • **line** --Uses the line password for authentication. • **local** --Uses the local username database for authentication. • **local-case** --Uses the case-sensitive local username database for authentication. • **none** --Uses no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.

Command Default

No authentication is performed.

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced for the Cisco Ethernet switch network module.
12.2(15)ZJ	This command was implemented on the following platforms for the Cisco Ethernet Switch Module: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.

Release	Modification
12.3(2)XA	This command was introduced on the following Cisco router platforms: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Router support was added for the following platforms: Cisco 1751, Cisco 2610XM - Cisco 2611XM, Cisco 2620XM - Cisco 2621XM, Cisco 2650XM - Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.
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 *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence to validate the password provided by the client. The only method that is truly 802.1X-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server. The remaining methods enable AAA to authenticate the client by using locally configured data. For example, the **local** and **local-case** methods use the username and password that are saved in the Cisco IOS configuration file. The **enable** and **line** methods use the **enable** and **line** passwords for authentication.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command. If you are not using a RADIUS server, you can use the **local** or **local-case** methods, which access the local username database to perform authentication. By specifying the **enable** or **line** methods, you can supply the clients with a password to provide access to the switch.

Use the **show running-config** privileged EXEC command to display the configured lists of authentication methods.

Examples

The following example shows how to enable AAA and how to create an authentication list for 802.1X. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is allowed access with no authentication:

```
Router(config)# aaa new model
Router(config)# aaa authentication dot1x default group radius none
```

Related Commands

Command	Description
debug dot1x	Displays 802.1X debugging information.
identity profile default	Creates an identity profile and enters dot1x profile configuration mode.
show dot1x	Displays details for an identity profile.

Command	Description
show dot1x (EtherSwitch)	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

aaa authentication fail-message

To configure a personalized banner that will be displayed when a user fails login, use the **aaa authentication fail-message** command in global configuration mode. To remove the failed login message, use the no form of this command.

aaa authentication fail-message *dstringd*

no aaa authentication fail-message

Syntax Description

d	The delimiting character at the beginning and end of the *string* that notifies the system that the *string* is to be displayed as the banner. The delimiting character can be any character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.
string	Any group of characters, excluding the one used as the delimiter. The maximum number of characters that you can display is 2996.

Command Default

Not enabled

Command Modes

Global configuration

Command History

Release	Modification
11.3(4)T	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.

Usage Guidelines

Use the **aaa authentication fail-message** command to create a personalized message that appears when a user fails login. This message will replace the default message for failed login.

To create a failed-login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any

character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

Examples

The following example shows the default login message and failed login message that is displayed if **aaa authentication banner** and **aaa authentication fail-message** are not configured. (RADIUS is specified as the default login authentication method.)

```
aaa new-model
aaa authentication login default group radius
```

This configuration produces the following standard output:

```
User Verification Access
Username:
Password:
% Authentication failed.
```

The following example configures both a login banner (“Unauthorized use is prohibited.”) and a login-fail message (“Failed login. Try again.”). The login message will be displayed when a user logs in to the system. The failed-login message will display when a user tries to log in to the system and fails. (RADIUS is specified as the default login authentication method.) In this example, the asterisk (*) is used as the delimiting character.

```
aaa new-model
aaa authentication banner *Unauthorized use is prohibited.*
aaa authentication fail-message *Failed login. Try again.*
aaa authentication login default group radius
```

This configuration produces the following login and failed login banner:

```
Unauthorized use is prohibited.
Username:
Password:
Failed login. Try again.
```

Related Commands

Command	Description
aaa authentication banner	Configures a personalized banner that will be displayed at user login.

aaa authentication login

To set authentication, authorization, and accounting (AAA) authentication at login, use the **aaa authentication login** command in global configuration mode. To disable AAA authentication, use the **no** form of this command.

aaa authentication login {**default**| *list-name*} **[passwd-expiry]** *method1* [*method2* ...]

no aaa authentication login {**default**| *list-name*} **[passwd-expiry]** *method1* [*method2* ...]

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in. See the "Usage Guidelines" section for more information.
passwd-expiry	Enables password aging on a local authentication list. **Note** The **radius-server vsa send authentication** command is required to make the **passwd-expiry** keyword work.
method1 [*method2...*]	The list of methods that the authentication algorithm tries in the given sequence. You must enter at least one method; you may enter up to four methods. Method keywords are described in the table below.

Command Default

AAA authentication at login is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	This command was modified. The **group radius**, **group tacacs+**, and **local-case** keywords were added as methods for authentication.
12.4(6)T	This command was modified. The **password-expiry** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB. The **cache** *group-name* keyword and argument were added as a method for authentication.
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.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(1)T	This command was modified. The **group ldap** keyword was added.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

If the **default** keyword is not set, only the local user database is checked. This has the same effect as the following command:

```
aaa authentication login default local
```

Note On the console, login will succeed without any authentication checks if **default** keyword is not set.

The default and optional list names that you create with the **aaa authentication login** command are used with the **login authentication** command.

Create a list by entering the **aaa authentication login** *list-name method*command for a particular protocol. The *list-name* argument is the character string used to name the list of authentication methods activated when a user logs in. The *method* argument identifies the list of methods that the authentication algorithm tries, in the given sequence. The aaa authentication login, on page 9 section lists authentication methods that cannot be used for the *list-name* argument and the table below describes the method keywords.

To create a default list that is used if no list is assigned to a line, use the **login authentication** command with the default argument followed by the methods you want to use in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

If authentication is not specifically set for a line, the default is to deny access and no authentication is performed. Use the **more system:running-config** command to display currently configured lists of authentication methods.

Authentication Methods That Cannot Be Used for the list-name Argument

The authentication methods that cannot be used for the *list-name* argument are as follows:

- **auth-guest**
- **enable**
- **guest**
- **if-authenticated**
- **if-needed**

- **krb5**
- **krb-instance**
- **krb-telnet**
- **line**
- **local**
- **none**
- **radius**
- **rcmd**
- **tacacs**
- **tacacsplus**

Note In the table below, the **group radius**, **group tacacs +**, **group ldap**, and **group***group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius**, **aaa group server ldap**,and **aaa group server tacacs+** commands to create a named group of servers.

The table below describes the method keywords.

Table 1: aaa authentication login Methods Keywords

Keyword	Description
cache *group-name*	Uses a cache server group for authentication.
enable	Uses the enable password for authentication. This keyword cannot be used.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.
group ldap	Uses the list of all Lightweight Directory Access Protocol (LDAP) servers for authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
krb5	Uses Kerberos 5 for authentication.
krb5-telnet	Uses Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router.

Keyword	Description
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
passwd-expiry	Uses the login list to provide password aging support.

Examples

The following example shows how to create an AAA authentication list called *MIS-access*. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

```
aaa authentication login MIS-access group tacacs+ enable none
```

The following example shows how to create the same list, but it sets it as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication login default group tacacs+ enable none
```

The following example shows how to set authentication at login to use the Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router:

```
aaa authentication login default krb5
```

The following example shows how to configure password aging by using AAA with a crypto client:

```
aaa authentication login userauthen passwd-expiry group radius
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
login authentication	Enables AAA authentication for logins.

aaa authorization

To set the parameters that restrict user access to a network, use the **aaa authorization** command in global configuration mode. To remove the parameters, use the **no** form of this command.

aaa authorization {**auth-proxy**| **cache**| **commands** *level*| **config-commands**| **configuration**| **console**| **exec**| **ipmobile**| **multicast**| **network**| **policy-if**| **prepaid**| **radius-proxy**| **reverse-access**| **subscriber-service**| **template**} {**default**| *list-name*} [*method1* [*method2* ...]]

no aaa authorization {**auth-proxy**| **cache**| **commands** *level*| **config-commands**| **configuration**| **console**| **exec**| **ipmobile**| **multicast**| **network**| **policy-if**| **prepaid**| **radius-proxy**| **reverse-access**| **subscriber-service**| **template**} {**default**| *list-name*} [*method1* [*method2* ...]]

Syntax Description

auth-proxy	Runs authorization for authentication proxy services.
cache	Configures the authentication, authorization, and accounting (AAA) server.
commands	Runs authorization for all commands at the specified privilege level.
level	Specific command level that should be authorized. Valid entries are 0 through 15.
config-commands	Runs authorization to determine whether commands entered in configuration mode are authorized.
configuration	Downloads the configuration from the AAA server.
console	Enables the console authorization for the AAA server.
exec	Runs authorization to determine if the user is allowed to run an EXEC shell. This facility returns user profile information such as the autocommand information.
ipmobile	Runs authorization for mobile IP services.
multicast	Downloads the multicast configuration from the AAA server.
network	Runs authorization for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Programs (NCPs), and AppleTalk Remote Access (ARA).
policy-if	Runs authorization for the diameter policy interface application.

prepaid	Runs authorization for diameter prepaid services.
radius-proxy	Runs authorization for proxy services.
reverse-access	Runs authorization for reverse access connections, such as reverse Telnet.
subscriber-service	Runs authorization for iEdge subscriber services such as virtual private dialup network (VPDN).
template	Enables template authorization for the AAA server.
default	Uses the listed authorization methods that follow this keyword as the default list of methods for authorization.
list-name	Character string used to name the list of authorization methods.
method1 [*method2...*]	(Optional) Identifies an authorization method or multiple authorization methods to be used for authorization. A method may be any one of the keywords listed in the table below.

Command Default

Authorization is disabled for all actions (equivalent to the method keyword **none**).

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	This command was modified. The **group radius** and **group tacacs+** keywords were added as methods for authorization.
12.2(28)SB	This command was modified. The **cache** *group-name* keyword and argument were added as a method for authorization.
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.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Release	Modification
15.1(1)T	This command was modified. The **group ldap** keyword was added.

Usage Guidelines

Use the **aaa authorization**command to enable authorization and to create named methods lists, which define authorization methods that can be used when a user accesses the specified function. Method lists for authorization define the ways in which authorization will be performed and the sequence in which these methods will be performed. A method list is a named list that describes the authorization methods (such as RADIUS or TACACS+) that must be used in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or until all the defined methods are exhausted.

Note The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle--meaning that the security server or the local username database responds by denying the user services--the authorization process stops and no other authorization methods are attempted.

If the **aaa authorization** command for a particular authorization type is issued without a specified named method list, the default method list is automatically applied to all interfaces or lines (where this authorization type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no authorization takes place. The default authorization method list must be used to perform outbound authorization, such as authorizing the download of IP pools from the RADIUS server.

Use the **aaa authorization** command to create a list by entering the values for the *list-name*and the *method* arguments, where *list-name* is any character string used to name this list (excluding all method names) and *method*identifies the list of authorization methods tried in the given sequence.

Note In the table below, the **group** *group-name,* **group ldap, group radius**, and **group tacacs +** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius**, **aaa group server ldap**,and **aaa group server tacacs+** commands to create a named group of servers.

The table below describes the method keywords.

Table 2: aaa authorization Methods

Keyword	Description
cache *group-name*	Uses a cache server group for authorization.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the **server group** *group-name* command.

Keyword	Description
group ldap	Uses the list of all Lightweight Directory Access Protocol (LDAP) servers for authentication.
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
if-authenticated	Allows the user to access the requested function if the user is authenticated. **Note** The **if-authenticated** method is a terminating method. Therefore, if it is listed as a method, any methods listed after it will never be evaluated.
local	Uses the local database for authorization.
none	Indicates that no authorization is performed.

Cisco IOS software supports the following methods for authorization:

- Cache Server Groups--The router consults its cache server groups to authorize specific rights for users.
- If-Authenticated --The user is allowed to access the requested function provided the user has been authenticated successfully.
- Local --The router or access server consults its local database, as defined by the **username** command, to authorize specific rights for users. Only a limited set of functions can be controlled through the local database.
- None --The network access server does not request authorization information; authorization is not performed over this line or interface.
- RADIUS --The network access server requests authorization information from the RADIUS security server group. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
- TACACS+ --The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value (AV) pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.

Method lists are specific to the type of authorization being requested. AAA supports five different types of authorization:

- Commands --Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- EXEC --Applies to the attributes associated with a user EXEC terminal session.

- Network --Applies to network connections. The network connections can include a PPP, SLIP, or ARA connection.

Note You must configure the **aaa authorization config-commands** command to authorize global configuration commands, including EXEC commands prepended by the **do** command.

- Reverse Access --Applies to reverse Telnet sessions.
- Configuration --Applies to the configuration downloaded from the AAA server.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, the method lists must be applied to specific lines or interfaces before any of the defined methods are performed.

The authorization command causes a request packet containing a series of AV pairs to be sent to the RADIUS or TACACS daemon as part of the authorization process. The daemon can do one of the following:

- Accept the request as is.
- Make changes to the request.
- Refuse the request and authorization.

For a list of supported RADIUS attributes, see the module RADIUS Attributes. For a list of supported TACACS+ AV pairs, see the module TACACS+ Attribute-Value Pairs.

Note Five commands are associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included in the privilege level command set.

Examples

The following example shows how to define the network authorization method list named mygroup, which specifies that RADIUS authorization will be used on serial lines using PPP. If the RADIUS server fails to respond, local network authorization will be performed.

```
aaa authorization network mygroup group radius local
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.

Command	Description
aaa group server tacacs+	Groups different TACACS+ 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.
tacacs-server host	Specifies a TACACS+ host.
username	Establishes a username-based authentication system.

aaa dnis map accounting network

To map a Dialed Number Information Service (DNIS) number to a particular authentication, authorization, and accounting (AAA) server group that will be used for AAA accounting, use the **aaa dnis map accounting network**command in global configuration mode. To remove DNIS mapping from the named server group, use the **no** form of this command.

aaa dnis map *dnis-number* **accounting network** [**start-stop**| **stop-only**| **none**] **[broadcast] group** *groupname*

no aaa dnis map *dnis-number* **accounting network**

Syntax Description

dnis-number	Number of the DNIS.
start-stop	(Optional) Indicates that the defined security server group will send a “start accounting” notice at the beginning of a process and a “stop accounting” notice at the end of a process. The “start accounting” record is sent in the background. (The requested user process begins regardless of whether the “start accounting” notice was received by the accounting server.)
stop-only	(Optional) Indicates that the defined security server group will send a “stop accounting” notice at the end of the requested user process.
none	(Optional) Indicates that the defined security server group will not send accounting notices.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.
group *groupname*	At least one of the keywords described in the table below.

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.

Release	Modification
12.1(1)T	• The optional **broadcast** keyword was added. • The ability to specify multiple server groups was added. • To accommodate multiple server groups, the name of the command was changed from **aaa dnis map accounting network group** to **aaa dnis map accounting network**.
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

This command lets you assign a DNIS number to a particular AAA server group so that the server group can process accounting requests for users dialing in to the network using that particular DNIS. To use this command, you must first enable AAA, define an AAA server group, and enable DNIS mapping.

The table below contains descriptions of accounting method keywords.

Table 3: AAA Accounting Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius command.**
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
group group-name	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name*.

In the table above, the **group radius**and **group tacacs +** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Examples

The following example maps DNIS number 7777 to the RADIUS server group called group1. Server group group1 will use RADIUS server 172.30.0.0 for accounting requests for users dialing in with DNIS 7777.

```
aaa new-model
```

```
radius-server host 172.30.0.0 acct-port 1646 key cisco1
aaa group server radius group1
 server 172.30.0.0
aaa dnis map enable
aaa dnis map 7777 accounting network group group1
```

Related Commands

Command	Description
aaa dnis map authentication ppp group	Maps a DNIS number to a particular authentication server group.
aaa dnis map enable	Enables AAA server selection based on DNIS.
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.

aaa dnis map authentication group

To map a dialed number identification service (DNIS) number to a particular authentication server group (this server group will be used for authentication, authorization, and accounting [AAA] authentication), use the **aaa dnis map authentication group** command in AAA-server-group configuration mode. To remove the DNIS number from the defined server group, use the **no** form of this command.

aaa dnis map *dnis-number* **authentication** {**ppp**| **login**} **group** *server-group-name*

no aaa dnis map *dnis-number* **authentication** {**ppp**| **login**} **group** *server-group-name*

Syntax Description

dnis-number	Number of the DNIS.
ppp	Enables PPP authentication methods.
login	Enables character-mode authentication.
server-group-name	Character string used to name a group of security servers associated in a server group.

Command Default

A DNIS number is not mapped to a server group.

Command Modes

AAA-server-group configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(3)XL1	This command was modified with the addition of the **login** keyword to include character-mode authentication.
12.2(2)T	Support for the **login** keyword was added into Cisco IOS Release 12.2(2)T and this command was implemented for the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 platforms.
12.2(8)T	This command was implemented on the Cisco 806, Cisco 828, Cisco 1710, Cisco SOHO 78, Cisco 3631, Cisco 3725, Cisco 3745, and Cisco URM for IGX8400 platforms.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
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

Use the **aaa dnis map authentication group** command to assign a DNIS number to a particular AAA server group so that the server group can process authentication requests for users that are dialing in to the network using that particular DNIS. To use the **aaa dnis map authentication group** command, you must first enable AAA, define a AAA server group, and enable DNIS mapping.

Examples

The following example maps DNIS number 7777 to the RADIUS server group called group1. Server group group1 uses RADIUS server 172.30.0.0 for authentication requests for users dialing in with DNIS number 7777.

```
aaa new-model
radius-server host 172.30.0.0 auth-port 1645 key cisco1
aaa group server radius group1
 server 172.30.0.0
 aaa dnis map enable
 aaa dnis map 7777 authentication ppp group group1
 aaa dnis map 7777 authentication login group group1
```

Related Commands

Command	Description
aaa dnis map accounting network group	Maps a DNIS number to a particular accounting server group.
aaa dnis map enable	Enables AAA server selection based on DNIS.
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.

aaa group server radius

To group different RADIUS server hosts into distinct lists and distinct methods, enter the **aaa group server radius**command in global configuration mode. To remove a group server from the configuration list, enter the **no** form of this command.

aaa group server radius *group-name*

no aaa group server radius *group-name*

Syntax Description

group-name	Character string used to name the group of servers. See the table below for a list of words that cannot be used as the *group-name* argument.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	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.

Usage Guidelines

The authentication, authorization, and accounting (AAA) server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

A group server is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts and TACACS+ server hosts. A group server is used in conjunction with a global server host list. The group server lists the IP addresses of the selected server hosts.

The table below lists words that cannot be used as the *group-name* argument.

Table 4: Words That Cannot Be UsedAs the group-nameArgument

Word
auth-guest

Word
enable
guest
if-authenticated
if-needed
krb5
krb-instance
krb-telnet
line
local
none
radius
rcmd
tacacs
tacacsplus

Examples

The following example shows the configuration of an AAA group server named radgroup1 that comprises three member servers:

```
aaa group server radius radgroup1
 server 10.1.1.1 auth-port 1700 acct-port 1701
 server 10.2.2.2 auth-port 1702 acct-port 1703
 server 10.3.3.3 auth-port 1705 acct-port 1706
```

Note If auth-port and acct-port are not specified, the default value of auth-port is 1645 and the default value of acct-port is 1646.

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

Command	Description
aaa authentication login	Set AAA authentication at login.
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

aaa group server tacacs+

To group different TACACS+ server hosts into distinct lists and distinct methods, use the **aaa group server**tacacs+ command in global configuration mode. To remove a server group from the configuration list, use the **no** form of this command.

aaa group server tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

Syntax Description

group-name	Character string used to name the group of servers. See the table below for a list of words that cannot be used as the *group-name* argument.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	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(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.
Cisco IOS XE Release 3.2S	This command was modified. Support for IPv6 was added.

Usage Guidelines

The Authentication, Authorization, and Accounting (AAA) Server-Group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

A server group is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts and TACACS+ server hosts. A server group is used in conjunction with a global server host list. The server group lists the IP addresses of the selected server hosts.

The table below lists the keywords that cannot be used for the *group-name* argument value.

Table 5: Words That Cannot Be UsedAs the group-nameArgument

Word
auth-guest
enable
guest
if-authenticated
if-needed
krb5
krb-instance
krb-telnet
line
local
none
radius
rcmd
tacacs
tacacsplus

Examples

The following example shows the configuration of an AAA server group named tacgroup1 that comprises three member servers:

```
aaa group server tacacs+ tacgroup1
server 10.1.1.1
server 10.2.2.2
server 10.3.3.3
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security.

Command	Description
aaa authentication login	Enables AAA accounting of requested services for billing or security purposes.
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables the AAA access control model.
tacacs-server host	Specifies a TACACS+ host.

aaa nas port extended through address ipv6 (TACACS+)

- aaa nas port extended, page 32
- aaa new-model, page 34
- aaa route download, page 36
- aaa server radius dynamic-author, page 38
- access-list (IP standard), page 40
- address ipv6 (config-radius-server), page 44
- address ipv6 (TACACS+), page 46

aaa nas port extended

To replace the NAS-Port attribute with RADIUS IETF attribute 26 and to display extended field information, use the **aaa nas port extended**command inglobal configuration mode. To display no extended field information, use the **no** form of this command.

aaa nas port extended

no aaa nas port extended

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3	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.

Usage Guidelines

On platforms with multiple interfaces (ports) per slot, the Cisco RADIUS implementation will not provide a unique NAS-Port attribute that permits distinguishing between the interfaces. For example, if a dual PRI interface is in slot 1, calls on both Serial1/0:1 and Serial1/1:1 will appear as NAS-Port = 20101 due to the 16-bit field size limitation associated with RADIUS IETF NAS-Port attribute.

In this case, the solution is to replace the NAS-Port attribute with a vendor-specific attribute (RADIUS IETF Attribute 26). Cisco's vendor ID is 9, and the Cisco-NAS-Port attribute is subtype 2. Vendor-specific attributes (VSAs) can be turned on by entering the **radius-server vsa send** command. The port information in this attribute is provided and configured using the **aaa nas port extended** command.

The standard NAS-Port attribute (RADIUS IETF attribute 5) will continue to be sent. If you do not want this information to be sent, you can suppress it by using the **no radius-server attribute nas-port** command. When this command is configured, the standard NAS-Port attribute will no longer be sent.

Examples

The following example specifies that RADIUS will display extended interface information:

```
radius-server vsa send
aaa nas port extended
```

Related Commands

Command	Description
radius-server extended-portnames	Displays expanded interface information in the NAS-Port attribute.
radius-server vsa send	Configures the network access server to recognize and use vendor-specific attributes.

aaa new-model

To enable the authentication, authorization, and accounting (AAA) access control model, issue the **aaa new-model** command in global configuration mode. To disable the AAA access control model, use the **no** form of this command.

aaa new-model

no aaa new-model

Syntax Description

This command has no arguments or keywords.

Command Default

AAA is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2(33)SXI	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.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command enables the AAA access control system.

Examples

The following example initializes AAA:

```
aaa new-model
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication arap	Enables an AAA authentication method for ARAP using TACACS+.
aaa authentication enable default	Enables AAA authentication to determine if a user can access the privileged command level.
aaa authentication login	Sets AAA authentication at login.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.

aaa route download

To enable the static route download feature and set the amount of time between downloads, use the **aaa route download** command in global configuration mode. To disable this function, use the **no** form of this command.

aaa route download [*time*] [**authorization** *method-list*]

no aaa route download

Syntax Description

time	(Optional) Time between downloads, in minutes. The range is from 1 to 1440 minutes.
authorization *method-list*	(Optional) Specify a named method list to which RADIUS authorization requests for static route downloads are sent. If these attributes are not set, all RADIUS authorization requests will be sent to the servers that are specified by the default method list.

Command Default

The default period between downloads (updates) is 720 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1.
12.2(8)T	The **authorization** keyword was added; the *method-list* argument was added.
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.

Usage Guidelines

This command is used to download static route details from the authorization, authentication, and accounting (AAA) server if the name of the router is *hostname*. The name passed to the AAA server for static routes is *hostname-1*, *hostname-2*... *hostname-n*--the router downloads static routes until it fails an index and no more routes can be downloaded.

Examples

The following example sets the AAA route update period to 100 minutes:

```
aaa route download 100
```

The following example sets the AAA route update period to 10 minutes and sends static route download requests to the servers specified by the method list name “list1”:

```
aaa route download 10 authorization list1
```

Related Commands

Command	Description
aaa authorization configuration default	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
clear ip route download	Clears static routes downloaded from a AAA server.
show ip route	Displays all static IP routes, or those installed using the AAA route download function.

aaa server radius dynamic-author

To configure a device as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server, use the **aaa server radius dynamic-author**command in global configuration mode. To remove this configuration, use the **no** form of this command.

aaa server radius dynamic-author

no aaa server radius dynamic-author

Syntax Description

This command has no arguments or keywords.

Command Default

The device will not function as a server when interacting with external policy servers.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.4	This command was integrated into Cisco IOS Release 12.4.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
12.2(5)SXI	This command was integrated into Cisco IOS Release 12.2(5)SXI.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Dynamic authorization allows an external policy server to dynamically send updates to a device. Once the **aaa server radius dynamic-author** command is configured, dynamic authorization local server configuration mode is entered. Once in this mode, the RADIUS application commands can be configured.

Dynamic Authorization for the Intelligent Services Gateway (ISG)

ISG works with external devices, referred to as policy servers, that store per-subscriber and per-service information. ISG supports two models of interaction between the ISG device and external policy servers: initial authorization and dynamic authorization.

The dynamic authorization model allows an external policy server to dynamically send policies to the ISG. These operations can be initiated in-band by subscribers (through service selection) or through the actions of an administrator, or applications can change policies on the basis of an algorithm (for example, change session quality of service (QoS) at a certain time of day). This model is facilitated by the Change of Authorization (CoA) RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling ISG and the external policy server each to act as a RADIUS client and server.

Examples

The following example configures the ISG to act as a AAA server when interacting with the client at IP address 10.12.12.12:

```
aaa server radius dynamic-author
 client 10.12.12.12 key cisco
 message-authenticator ignore
```

Related Commands

Command	Description
auth-type (ISG)	Specifies the server authorization type.
client	Specifies a RADIUS client from which a device will accept CoA and disconnect requests.
default	Sets a RADIUS application command to its default.
domain	Specifies username domain options.
ignore	Overrides a behavior to ignore certain paremeters.
port	Specifies a port on which local RADIUS server listens.
server-key	Specifies the encryption key shared with RADIUS clients.

access-list (IP standard)

To define a standard IP access list, use the s tandard version of the **access-list** command in global configuration mode. To remove a standard access list, use the **no** form of this command.

access-list *access-list-number* {**deny**| **permit**} *source* [*source-wildcard*] [**log** [*word*]]

no access-list *access-list-number*

Syntax Description

access-list-number	Number of an access list. This is a decimal number from 1 to 99 or from 1300 to 1999.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
source	Number of the network or host from which the packet is being sent. There are two alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
source-wildcard	(Optional) Wildcard bits to be applied to the source. There are two alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The log message includes the access list number, whether the packet was permitted or denied, the source address, the number of packets, and if appropriate, the user-defined cookie or router-generated hash value. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.
word	(Optional) User-defined cookie appended to the log message. The cookie: • cannot be more than characters • cannot start with hexadecimal notation (such as 0x) • cannot be the same as, or a subset of, the following keywords: **reflect**, **fragment**, **time-range** • must contain alphanumeric characters only The user-defined cookie is appended to the access control entry (ACE) syslog entry and uniquely identifies the ACE, within the access control list, that generated the syslog entry.

Command Default

The access list defaults to an implicit deny statement for everything. The access list is always terminated by an implicit deny statement for everything.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
11.3(3)T	The **log** keyword was added.
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.
12.4(22)T	The *word* argument was added to the **log** keyword.

Usage Guidelines

Plan your access conditions carefully and be aware of the implicit deny statement at the end of the access list.

You can use access lists to control the transmission of packets on an interface, control vty access, and restrict the contents of routing updates.

Use the **show access-lists** EXEC command to display the contents of all access lists.

Use the **show ip access-list** EXEC command to display the contents of one access list.

Caution Enhancements to this command are backward compatible; migrating from releases prior to Cisco IOS Release 10.3 will convert your access lists automatically. However, releases prior to Release 10.3 are not upwardly compatible with these enhancements. Therefore, if you save an access list with these images and then use software prior to Release 10.3, the resulting access list will not be interpreted correctly. **This condition could cause you severe security problems**. Save your old configuration file before booting these images.

Examples

The following example of a standard access list allows access for only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the access list statements will be rejected.

```
access-list 1 permit 192.168.34.0 0.0.0.255
access-list 1 permit 10.88.0.0 0.0.255.255
access-list 1 permit 10.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
```

The following example of a standard access list allows access for devices with IP addresses in the range from 10.29.2.64 to 10.29.2.127. All packets with a source address not in this range will be rejected.

```
access-list 1 permit 10.29.2.64 0.0.0.63
! (Note: all other access implicitly denied)
```

To specify a large number of individual addresses more easily, you can omit the wildcard if it is all zeros. Thus, the following two configuration commands are identical in effect:

```
access-list 2 permit 10.48.0.3
access-list 2 permit 10.48.0.3 0.0.0.0
```

The following example of a standard access list allows access for devices with IP addresses in the range from 10.29.2.64 to 10.29.2.127. All packets with a source address not in this range will be rejected.

```
access-list 1 permit 10.29.2.64 0.0.0.63
! (Note: all other access implicitly denied)
```

The following example of a standard access list allows access for devices with IP addresses in the range from 10.29.2.64 to 10.29.2.127. All packets with a source address not in this range will be rejected. In addition, the logging mechanism is enabled and the word SampleUserValue is appended to each syslog entry.

```
Router(config)# access-list 1 permit 10.29.2.64 0.0.0.63 log SampleUserValue
```

Related Commands

Command	Description
access-class	Restricts incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list.
access-list (IP extended)	Defines an extended IP access list.
access-list remark	Writes a helpful comment (remark) for an entry in a numbered IP access list.
deny (IP)	Sets conditions under which a packet does not pass a named access list.
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
ip access-group	Controls access to an interface.
ip access-list logging hash-generation	Enables hash value generation for ACE syslog entries.
permit (IP)	Sets conditions under which a packet passes a named access list.
remark (IP)	Writes a helpful comment (remark) for an entry in a named IP access list.
show access-lists	Displays the contents of current IP and rate-limit access lists.
show ip access-list	Displays the contents of all current IP access lists.

address ipv6 (config-radius-server)

To configure the IPv6 address for the RADIUS server accounting and authentication parameters, use the **address ipv6** command in RADIUS server configuration mode. To remove the specified RADIUS server accounting and authentication parameters, use the **no** form of this command.

address ipv6 {*hostname*| *ipv6address*} [**acct-port** *port*| **alias** {*hostname*| *ipv6address*}| **auth-port** *port* [**acct-port** *port*]]

no address ipv6 {*hostname*| *ipv6address*} [**acct-port** *port*| **alias** {*hostname*| *ipv6address*}| **auth-port** *port* [**acct-port** *port*]]

Syntax Description

hostname	Domain Name System (DNS) name of the RADIUS server host.
ipv6address	RADIUS server IPv6 address.
acct-port *port*	(Optional) Specifies the User Datagram Protocol (UDP) port for the RADIUS accounting server for accounting requests. The default port is 1646.
alias {*hostname* | *ipv6address*}	(Optional) Specifies an alias for this server. The alias can be an IPv6 address or hostname. Up to eight aliases can be configured for this server.
auth-port *port*	(Optional) Specifies the UDP port for the RADIUS authentication server. The default port is 1645.

Command Default

The RADIUS server accounting and authentication parameters are not configured.

Command Modes

RADIUS server configuration (config-radius-server)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

The **aaa new-model** command must be configured before accessing this command.

The Cisco TrustSec (CTS) feature uses Secure RADIUS to prescribe a process of authentication, authorization, session association, encryption, and traffic filtering.

Before an alias can be configured for the RADIUS server, the server's IPv6 address or DNS name must be configured. This is accomplished by using the **address ipv6** command and the *hostname* argument. An alias can then be configured by using the **address ipv6** command, the **alias** keyword, and the *hostname* argument.

Examples

The following example shows how to configure the RADIUS server accounting and authentication parameters:

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv6 2001:DB8:1::1 acct-port 1813 auth-port 1812
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
address ipv4	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.
radius server	Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode.

address ipv6 (TACACS+)

To configure the IPv6 address of the TACACS+ server, use the **address ipv6** command in TACACS+ server configuration mode. To remove the IPv6 address, use the **no** form of this command.

address ipv6 *ipv6-address*

no address ipv6 *ipv6-address*

Syntax Description

ipv6-address	The private TACACS+ server host.

Command Default

No TACACS+ server is configured.

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 address ipv6 (TACACS+) command after you have enabled the TACACS+ server using the **tacacs server** command.

Examples

The following example shows how to specify the IPv6 address on a TACACS+ server named server1:

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# address ipv6 2001:0DB8:3333:4::5
```

Related Commands

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

authentication command bounce-port ignore through auth-type

- authentication command bounce-port ignore, page 48
- authentication command disable-port ignore, page 49
- authentication control-direction, page 50
- authentication event fail, page 52
- authentication event server alive action reinitialize, page 54
- authentication event server dead action authorize, page 55
- authentication fallback, page 57
- authentication host-mode, page 58
- authentication open, page 60
- authentication order, page 61
- authentication periodic, page 63
- authentication port-control, page 64
- authentication priority, page 66
- authentication timer inactivity, page 68
- authentication timer reauthenticate, page 70
- authentication timer restart, page 72
- authentication violation, page 74
- auth-type, page 75

authentication command bounce-port ignore

To configure the router to ignore a RADIUS Change of Authorization (CoA) bounce port command, use the **authentication command bounce-port ignore** command in global configuration mode. To return to the default status, use the **no** form of this command.

authentication command bounce-port ignore

no authentication command bounce-port ignore

Syntax Description

This command has no arguments or keywords.

Command Default

The router accepts a RADIUS CoA bounce port command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

A RADIUS CoA bounce port command sent from a RADIUS server can cause a link flap on an authentication port, which triggers Dynamic Host Configuration Protocol (DHCP) renegotiation from one or more hosts connected to this port. This incident can occur when there is a VLAN change and the endpoint is a device (such as a printer) that does not have a mechanism to detect a change on this authentication port. The **authentication command bounce-port ignore** command configures the router to ignore the RADIUS CoA bounce port command to prevent a link flap from occuring on any hosts that are connected to an authentication port.

Examples

This example shows how to configure the router to ignore a RADIUS CoA bounce port command:

```
Router(config)# aaa new-model
Router(config)# authentication command bounce-port ignore
```

Related Commands

Command	Description
authentication command disable-port ignore	Configures the router to ignore a RADIUS server CoA **disable port** command.

authentication command disable-port ignore

To allow the router to ignore a RADIUS server Change of Authorization (CoA) disable port command, use the **authentication command disable-port ignore** command in global configuration mode. To return to the default status, use the **no** form of this command.

authentication command disable-port ignore

no authentication command disable-port ignore

Syntax Description

This command has no arguments or keywords.

Command Default

The router accepts a RADIUS CoA disable port command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

The RADIUS server CoA disable port command administratively shuts down the authentication port that is hosting a session, resulting in session termination. Use the **authentication command disable-port ignore** command to configure the router to ignore the RADIUS server CoA disable port command so that the authentication port and other hosts on this authentication port are not disconnected.

Examples

This example shows how to configure the router to ignore a CoA **disable port** command:

```
Router(config)# aaa new-model
Router(config)# authentication command disable-port ignore
```

Related Commands

Command	Description
authentication command bounce-port ignore	Configures the router to ignore a RADIUS server CoA bounce port command.

authentication control-direction

To set the direction of authentication control on a port, use the **authentication control-direction**command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication control-direction {**both**| **in**}

no authentication control-direction

Syntax Description

both	Enables bidirectional control on the port.
in	Enables unidirectional control on the port.

Command Default

The port is set to bidirectional mode.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

The IEEE 802.1x standard is implemented to block traffic between the nonauthenticated clients and network resources. This means that nonauthenticated clients cannot communicate with any device on the network except the authenticator. The reverse is true, except for one circumstance--when the port has been configured as a unidirectional controlled port.

Unidirectional State

The IEEE 802.1x standard defines a unidirectional controlled port, which enables a device on the network to "wake up" a client so that it continues to be reauthenticated. When you use the **authentication control-direction in** command to configure the port as unidirectional, the port changes to the spanning-tree forwarding state, thus allowing a device on the network to wake the client, and force it to reauthenticate.

Bidirectional State

When you use the **authentication control-direction both** command to configure a port as bidirectional, access to the port is controlled in both directions. In this state, the port does not receive or send packets.

Examples

The following example shows how to enable unidirectional control:

```
Switch(config-if)# authentication control-direction in
```

The following examples show how to enable bidirectional control:

```
Switch(config-if)# authentication control-direction both
```

authentication event fail

To specify how the Auth Manager handles authentication failures as a result of unrecognized user credentials, use the **authentication event fail**command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication event fail [**retry** *retry-count*] **action** {**authorize vlan** *vlan-id*| **next-method**}

no authentication event fail

Syntax Description

retry *retry-count*	(Optional) Specifies how many times the authentication method is tried after an initial failure.
action	Specifies the action to be taken after an authentication failure as a result of incorrect user credentials.
authorize vlan *vlan-id*	Authorizes a restricted VLAN on a port after a failed authentication attempt.
next-method	Specifies that the next authentication method be invoked after a failed authentication attempt. The order of authentication methods is specified by the **authentication order** command.

Command Default

Authentication is attempted two times after the initial failed attempt.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Only the dot1x authentication method can signal this type of authentication failure.

Examples

The following example specifies that after three failed authentication attempts the port is assigned to a restricted VLAN:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3
```

```
Switch(config-if)# authentication event fail retry 3 action authorize vlan 40
Switch(config-if)# end
```

Related Commands

Command	Description
authentication event no-response action	Specifies the action to be taken when authentication fails due to a nonresponsive host.
authentication order	Specifies the order in which authentication methods are attempted.

authentication event server alive action reinitialize

To reinitialize an authorized Auth Manager session when a previously unreachable authentication, authorization, and accounting (AAA) server becomes available, use the **authentication event server alive action reinitialize** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication event server alive action reinitialize

no authentication event server alive action reinitialize

Syntax Description

This command has no arguments or keywords.

Command Default

The session is not reinitialized .

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use the **authentication event server alive action reinitialize** command to reinitialize authorized sessions when a previously unreachable AAA server becomes available.

Examples

The following example specifies that authorized sessions are reinitialized when a previously unreachable AAA server becomes available:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event server alive action reinitialize
Switch(config-if)# end
```

Related Commands

Command	Description
authentication event server dead action authorize	Specifies how to handle authorized sessions when the AAA server is unreachable.

authentication event server dead action authorize

To authorize Auth Manager sessions when the authentication, authorization, and accounting (AAA) server becomes unreachable, use the **authentication event server dead action authorize** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication event server dead action authorize vlan *vlan-id*

no authentication event server dead action authorize

Syntax Description

vlan *vlan-id*	Authorizes a restricted VLAN on a port after a failed authentication attempt.

Command Default

No session is authorized.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use the **authentication event server dead action authorize** command to authorize sessions even when the AAA server is unavailable.

Examples

The following example specifies that when the AAA server becomes unreachable, the port is assigned to a VLAN:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3

Switch(config-if)# authentication event server dead action authorize vlan 40

Switch(config-if)# end
```

Related Commands

Command	Description
authentication event server alive action reinitialize	Reinitializes an authorized session when a previously unreachable AAA server becomes available.

authentication fallback

To enable a web authentication fallback method, use the **authentication fallback** command in interface configuration mode. To disable web authentication fallback, use the **no** form of this command.

authentication fallback *fallback-profile*

no authentication fallback

Syntax Description

fallback-profile	The name of the fallback profile for web authentication.

Command Default

Web authentication fallback is not enabled.

Command Modes

Interface configuration (config-if)

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 **authentication fallback** command to specify the fallback profile for web authentication. Use the **fallback profile** command to specify the details of the profile.

Examples

The following example shows how to specify a fallback profile on a port:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitethernet1/0/3
Router(config-if)# authentication fallback profile1
Router(config-if)# end
```

Related Commands

Command	Description
fallback profile	Specifies the profile for web authentication.

authentication host-mode

To allow hosts to gain access to a controlled port, use the **authentication host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication host-mode {**single-host**| **multi-auth**| **multi-domain**| **multi-host**} **[open]**

no authentication host-mode

Syntax Description

single-host	Specifies that only one client can be authenticated on a port at any given time. A security violation occurs if more than one client is detected.
multi-auth	Specifies that multiple clients can be authenticated on the port at any given time.
multi-domain	Specifies that only one client per domain (DATA or VOICE) can be authenticated at a time.
multi-host	Specifies that after the first client is authenticated all subsequent clients are allowed access.
open	(Optional) Specifies that the port is open; that is, there are no access restrictions.

Command Default

Access to a port is not allowed.

Command Modes

Interface configuration (config-if)

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

Before you use this command, you must use the **authentication port-control** command with the keyword **auto**.

In **multi-host** mode, only one of the attached hosts has to be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL] logoff message is received), all attached clients are denied access to the network.

Examples

:The following example shows how to enable authentication in **multi-host** mode:

```
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet2/0/1

Switch(config-if)# authentication port-control auto

Switch(config-if)# authentication host-mode multi-host
```

Related Commands

Command	Description
authentication port-control	Displays information about interfaces.

authentication open

To enable open access on this port, use the **authentication open** command in interface configuration mode. To disable open access on this port, use the **no** form of this command.

authentication open

no authentication open

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced.

Usage Guidelines

Open Access allows clients or devices to gain network access before authentication is performed.

You can verify your settings by entering the **show authentication** privileged EXEC command.

This command overrides the **authentication host-mode** *session-type* **open** global configuration mode command for the port only.

Examples

The following example shows how to enable open access to a port:

```
Router(config-if)# authentication open
Router(config-if)#
```

The following example shows how to enable open access to a port:

```
Router(config-if)# no authentication open
Router(config-if)#
```

Related Commands

Command	Description
show authentication	Displays Authentication Manager information.

authentication order

To specify the order in which the Auth Manager attempts to authenticate a client on a port, use the **authentication order** command in interface configuration mode. To return to the default authentication order, use the **no** form of this command.

authentication order {**dot1x** [**mab**| **webauth**] **[webauth]**| **mab** [**dot1x**| **webauth**] **[webauth]**| **webauth**}

no authentication order

Syntax Description

dot1x	Specifies IEEE 802.1X authentication.
mab	Specifies MAC-based authentication(MAB).
webauth	Specifies web-based authentication.

Command Default

The default authentication order is **dot1x**, **mab**, and **webauth**.

Command Modes

Interface configuration (config-if)

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 **authentication order** command to specify explicitly which authentication methods are run and the order in which they are run. Each method may be entered only once in the list and no method can be listed after **webauth**.

Examples

The following example sets the authentication order for a port:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet0/1

Router(config-if)# authentication order mab dot1x
Router(config-if)# end
Router#
```

Related Commands

Command	Description
authentication priority	Specifies the priority of authentication methods on a port.

authentication periodic

To enable automatic reauthentication on a port, use the **authentication periodic** command in interface configuration mode. To disable, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.2(33)SXI, the **authentication periodic** command replaces the **dot1x reauthentication** command.

authentication periodic

no authentication periodic

Syntax Description

This command has no arguments or keywords.

Command Default

Reauthentication is disabled.

Command Modes

Interface configuration (config-if)

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 **authentication periodic** command to enable automatic reauthentication on a port. To configure the interval between reauthentication attempts, use the **authentication timer reauthenticate** command.

Examples

The following example enables reauthentication and sets the interval to 1800 seconds:

```
Switch(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet0/2
Switch(config-if)# authentication periodic
Switch(config-if)# authentication timer reauthenticate 1800
```

Related Commands

Command	Description
authentication timer reauthenticate	Specifies the period of time between attempts to reauthenticate an authorized port.

authentication port-control

To configure the authorization state of a controlled port, use the **authentication port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.2(33)SXI, the **authentication port-control** command replaces the **dot1x port-control** command.

authentication port-control {**auto**| **force-authorized**| **force-unauthorized**}

no authentication port-control

Syntax Description

auto	Enables port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.
force-authorized	Disables IEEE 802.1X on the interface and causes the port to change to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The **force-authorized** keyword is the default.
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

Command Default

Ports are authorized without authentication exchanges.

Command Modes

Interface configuration (config-if)

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

To verify port-control settings, use the **show interfaces** command and check the Status column in the 802.1X Port Summary section of the display. An enabled status means that the port-control value is set to auto or to force-unauthorized.

The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The system requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

Examples

The following example shows the commands used to specify that the authorization status of the client be determined by the authentication process:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface ethernet0/2

Router(config-if)# authentication port-control auto
```

Related Commands

Command	Description
show interfaces	Configures the authorization state of a controlled port.

authentication priority

To specify the priority of authentication methods on a port, use the **authentication priority**command in interface configuration mode. To return to the default, use the **no** form of this command.

authentication priority {**dot1x** [**mab**| **webauth**] **[webauth]**| **mab** [**dot1x**| **webauth**] **[webauth]**| **webauth**}

no authentication priority

Syntax Description

dot1x	Specifies IEEE 802.1X authentication.
mab	Specifies MAC-based authentication.
webauth	Specifies web-based authentication.

Command Default

The default priority order is **dot1x**, **mab**, and **webauth**.

Command Modes

Interface configuration (config-if)

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

The **authentication order** command specifies the order in which authentication methods are attempted. This order is the default priority. To override the default priority and allow higher priority methods to interrupt a running authentication method, use the **authentication priority** command.

Examples

The following example shows the commands used to configure the authentication order and the authentication priority on a port:

```
Router# configure terminal
Router(config)# interface fastethernet0/1

Router(config-if)# authentication order mab dot1x webauth
Router(config-if)# authentication priority dot1x mab
Router(config-if)# end
Router#
```

Related Commands

Command	Description
authentication order	Specifies the order in which the Auth Manager attempts to authenticate a client on a port.

authentication timer inactivity

To configure the time after which an inactive Auth Manager session is terminated, use the **authentication timer inactivity**command in interface configuration mode. To disable the inactivity timer, use the **no** form of this command.

authentication timer inactivity {*seconds*| **server**}

no authentication timer inactivity

Syntax Description

seconds	The period of inactivity, in seconds, allowed before an Auth Manager session is terminated and the port is unauthorized. The range is from 1 to 65535.
server	Specifies that the period of inactivity is defined by the Idle-Timeout value (RADIUS Attribute 28) on the authentication, authorization, and accounting (AAA) server.

Command Default

The inactivity timer is disabled.

Command Modes

Interface configuration (config-if)

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

In order to prevent reauthentication of inactive sessions, use the **authentication timer inactivity**command to set the inactivity timer to an interval shorter than the reauthentication interval set with the **authentication timer reauthenticate** command.

Examples

The following example sets the inactivity interval on a port to 900 seconds:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet6/0

Switch(config-if)# authentication timer inactivity 900

Switch(config-if)# end
```

Related Commands

Command	Description
configuration timer reauthenticate	Specifies the time after which the Auth Manager attempts to reauthenticate an authorized port.
authentication timer restart	Specifies the interval after which the Auth Manager attempts to authenticate an unauthorized port.

authentication timer reauthenticate

To specify the period of time between which the Auth Manager attempts to reauthenticate authorized ports, use the **authentication timer reauthenticate** command in interface configuration mode. To reset the reauthentication interval to the default, use the **no** form of this command.

authentication timer reauthenticate {*seconds*| **server**}

no authentication timer reauthenticate

Syntax Description

seconds	The number of seconds between reauthentication attempts. The default is 3600.
server	Specifies that the interval between reauthentication attempts is defined by the Session-Timeout value (RADIUS Attribute 27) on the authentication, authorization, and accounting (AAA) server.

Command Default

The automatic reauthentication interval is set to 3600 seconds.

Command Modes

Interface configuration (config-if)

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 **authentication timer reauthenticate** command to set the automatic reauthentication interval of an authorized port. If you use the **authentication timer inactivity** command to configure an inactivity interval, configure the reauthentication interval to be longer than the inactivity interval.

Examples

The following example sets the reauthentication interval on a port to 1800 seconds:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet6/0

Switch(config-if)# authentication timer reauthenticate 1800

Switch(config-if)# end
```

Related Commands

Command	Description
authentication periodic	Enables automatic reauthentication.
authentication timer inactivity	Specifies the interval after which the Auth Manager ends an inactive session.
authentication timer restart	Specifies the interval after which the Auth Manager attempts to authenticate an unauthorized port.

authentication timer restart

To specify the period of time after which the Auth Manager attempts to authenticate an unauthorized port, use the **authentication timer restart** command in interface configuration mode. To reset the interval to the default value, use the **no** form of this command.

authentication timer restart *seconds*

no authentication timer restart

Syntax Description

seconds	The number of seconds between attempts to authenticate an unauthorized port. The range is 1 to 65535. The default is 60.

Command Default

No attempt is made to authenticate unauthorized ports.

Command Modes

Interface configuration (config-if)

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 **authentication timer restart** command to specify the interval between attempts to authenticate an unauthorized port. The default interval is 60 seconds.

Examples

The following example sets the authentication timer interval to 120 seconds:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface GigabitEthernet6/0

Router(config-if)# authentication timer restart 120

Router(config-if)# end
```

Related Commands

Command	Description
authentication timer inactivity	Specifies the period of time after which the Auth Manager attempts to authenticate an unauthorized port.
configuration timer reauthenticate	Specifies the time after which the Auth Manager attempts to reauthenticate an authorized port.

authentication violation

To specify the action to be taken when a security violation occurs on a port, use the **authentication violation**command in interface configuration mode. To return to the default action, use the **no** form of this command.

authentication violation {**restrict**| **shutdown**}

no authentication violation

Syntax Description

restrict	Specifies that the port restrict traffic with the domain from which the security violation occurs.
shutdown	Specifies that the port shuts down upon a security violation.

Command Default

Ports are shut down when a security violation occurs.

Command Modes

Interface configuration (config-if)

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 **authentication violation** command to specify the action to be taken when a security violation occurs on a port.

Examples

The following example configures the GigabitEthernet interface to restrict traffic when a security violation occurs:

```
Switch(config)# interface GigabitEthernet6/2

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)# authentication violation restrict

Switch(config-if)# end
```

auth-type

To set policy for devices that are dynamically authenticated or unauthenticated, use the **auth-type** command in identity profile configuration mode. To remove the policy that was specified, use the **no** form of this command.

auth-type {**authorize**| **not-authorize**} **policy** *policy-name*

no auth-type {**authorize**| **not-authorize**} **policy** *policy-name*

Syntax Description

authorize	Policy is specified for all authorized devices.
not-authorize	Policy is specified for all unauthorized devices.
policy *policy-name*	Specifies the name of the identity policy to apply for the associated authentication result.

Command Default

A policy is not set for authorized or unauthorized devices.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

This command is used when a device is dynamically authenticated or unauthenticated by the network access device, and the device requires the name of the policy that should be applied for that authentication result.

Examples

The following example shows that 802.1x authentication applies to the identity policy “grant” for all dynamically authenticated hosts:

```
Router (config)# ip access-list extended allow-acl
Router (config-ext-nacl)# permit ip any any
Router (config-ext-nacl)# exit
Router (config)# identity policy grant
Router (config-identity-policy)# access-group allow-acl
Router (config-identity-policy)# exit
Router (config)# identity profile dot1x

Router (config-identity-prof)# auth-type authorize policy grant
```

Related Commands

Command	Description
identity policy	Creates an identity policy.
identity profile dot1x	Creates an 802.1x identity profile.

clear dot1x through clear eap

- clear dot1x, page 78
- clear eap, page 80

clear dot1x

To clear 802.1X interface information, use the **clear dot1x** command in privileged EXEC mode.

clear dot1x {**all**| **interface interface-name**}

Syntax Description

all	Clears 802.1X information for all interfaces.
interface interface-name	Clears 802.1X information for the specified interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)SEE	This command was integrated into Cisco IOS Release 12.2(25)SEE.
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.

Examples

The following configuration shows that 802.1X information will be cleared for all interfaces:

```
Router# clear dot1x all
```

The following configuration shows that 802.1X information will be cleared for the Ethernet 0 interface:

```
Router# clear dot1x interface ethernet 0
```

You can verify that the information was deleted by entering the **show dot1x** command.

Related Commands

Command	Description
debug dot1x	Displays 802.1X debugging information.
identity profile default	Creates an identity profile and enters identity profile configuration mode.

Command	Description
show dot1x	Displays details for an identity profile.

clear eap

To clear Extensible Authentication Protocol (EAP) information on a switch or for a specified port, use the **clear eap** command in privileged EXEC mode.

clear eap [**sessions** [**credentials** *credentials-name*| **interface** *interface-name*| **method** *method-name*| **transport** *transport-name*]]

Syntax Description

sessions	(Optional) Clears EAP sessions on a switch or a specified port.
credentials *credentials-name*	(Optional) Clears EAP credential information for only the specified profile.
interface *interface-name*	(Optional) Clears EAP credential information for only the specified interface.
method *method-name*	(Optional) Clears EAP credential information for only the specified method.
transport *transport-name*	(Optional) Clears EAP credential information for only the specified lower layer.

Command Default

All active EAP sessions are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEE	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines

You can clear all counters by using the **clear eap** command with the **sessions** keyword, or you can clear only the specified information by using the **credentials**, **interface**, **method**, or **transport** keywords.

Examples

The following example shows how to clear all EAP information:

```
Router# clear eap sessions
```

The following example shows how to clear EAP session information for the specified profile:

```
Router# clear eap sessions credentials type1
```

Related Commands

Command	Description
show eap registrations	Displays EAP registration information.
show eap sessions	Displays active EAP session information.

client through crl

- client, page 84
- crl, page 86

client

To specify a RADIUS client from which a device will accept Change of Authorization (CoA) and disconnect requests, use the **client** command in dynamic authorization local server configuration mode. To remove this specification, use the **no** form of this command.

client {*name*| *ip-address*} [**key** [**0**| **7**] *word*] [**vrf** *vrf-id*]

no client {*name*| *ip-address*} [**key** [**0**| **7**] *word*] [**vrf** *vrf-id*]

Syntax Description

name	Hostname of the RADIUS client.
ip-address	IP address of the RADIUS client.
key	(Optional) Configures the RADIUS key to be shared between a device and a RADIUS client.
0	(Optional) Specifies that an unencrypted key will follow.
7	(Optional) Specifies that a hidden key will follow.
word	(Optional) Unencrypted server key.
vrf *vrf-id*	(Optional) Virtual Routing and Forwarding (VRF) ID of the client.

Command Default

CoA and disconnect requests are dropped.

Command Modes

Dynamic authorization local server configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

A device (such as a router) can be configured to allow an external policy server to dynamically send updates to the router. This functionality is facilitated by the CoA RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling a router and external policy server each to act as a RADIUS client and server. Use the **client** command to specify the RADIUS clients for which the router will act as server.

Examples

The following example configures the router to accept requests from the RADIUS client at IP address 10.0.0.1:

```
aaa server radius dynamic-author
 client 10.0.0.1 key cisco
```

Related Commands

Command	Description
aaa server radius dynamic-author	Configures an ISG as a AAA server to facilitate interaction with an external policy server.

crl

To specify the certificate revocation list (CRL) query and CRL cache options for the public key infrastructure (PKI) trustpool, use the **crl** command in ca-trustpool configuration mode. To return to the default behavior in which the router checks the URL that is embedded in the certificate, use the **no** form of this command.

crl {**cache** {**delete-after** {*minutes*| **none**}| **query** *url*}

no crl {**cache** {**delete-after** {*minutes*| **none**}| **query** *url*}

Syntax Description

cache	Specifies CRL cache options.
delete-after	Removes the CRL from cache after a timeout.
minutes	The number of minutes from 1 to 43200 to wait before deleting CRL from cache.
none	Specifies that CRLs are not cached.
query *url*	Specifies the URL published by the certification authority (CA) server to query the CRL.

Command Default

The CRL is not queried and no CRL cache parameters are configured.

Command Modes

Ca-trustpool configuration (ca-trustpool)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

The **crl query** command is used if the CDP is in Lightweight Directory Access Protocol (LDAP) form, which means that the CDP location in the certificate indicates only where the CRL distribution point (CDP) is located in the directory; that is, the CDP does not indicate the actual query location for the directory.

The Cisco IOS software queries the CRL to ensure that the certificate has not been revoked in order to verify a peer certificate (for example, during Internet Key Exchange (IKE) or Secure Sockets Layer (SSL) handshake). The query looks for the CDP extension in the certificate, which is used to download the CRL. If this query is

unsuccessful, then the Simple Certificate Enrollment Protocol (SCEP) GetCRL mechanism is used to query the CRL from the CA server directly (some CA servers do not support this method).

Cisco IOS software supports the following CDP entries:

- HTTP URL with a hostname. For example: http://myurlname/myca.crl
- HTTP URL with an IPv4 address. For example: http://10.10.10.10:81/myca.crl
- LDAP URL with a hostname. For example: ldap://CN=myca, O=cisco
- LDAP URL with an IPv4 address. For example: ldap://10.10.10.10:3899/CN=myca, O=cisco
- LDAP/X.500 DN. For example: CN=myca, O=cisco

The Cisco IOS needs a complete URL in order to locate the CDP.

Examples

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# crl query http://www.cisco.com/security/pki/crl/crca2048.crl
```

Related Commands

Command	Description
cabundle url	Configures the URL from which the PKI trustpool CA bundle is downloaded.
chain-validation	Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool.
crypto pki trustpool import	Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle.
crypto pki trustpool policy	Configures PKI trustpool policy parameters.
default	Resets the value of a ca-trustpool configuration command to its default.
match	Enables the use of certificate maps for the PKI trustpool.
ocsp	Specifies OCSP settings for the PKI trustpool.
revocation-check	Disables revocation checking when the PKI trustpool policy is being used.

Command	Description
show	Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.
show crypto pki trustpool	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
source interface	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
storage	Specifies a file system location where PKI trustpool certificates are stored on the router.
vrf	Specifies the VRF instance to be used for CRL retrieval.

crypto ca authenticate through crypto ca trustpoint

- crypto ca authenticate, page 90
- crypto ca enroll, page 92
- crypto ca trustpoint, page 95

crypto ca authenticate

Note This command was replaced by the **crypto pki authenticate** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To authenticate the certification authority (by getting the certificate of the CA), use the **crypto ca authenticate** command in global configuration mode.

crypto ca authenticate *name*

Syntax Description

name	Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto ca identity** command .

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command is required when you initially configure CA support at your router.

This command authenticates the CA to your router by obtaining the self-signed certificate of the CA that contains the public key of the CA. Because the CA signs its own certificate, you should manually authenticate the public key of the CA by contacting the CA administrator when you perform this command.

If you are using RA mode (using the **enrollment mode ra** command) when you issue the **crypto ca authenticate** command, then registration authority signing and encryption certificates will be returned from the CA as well as the CA certificate.

This command is not saved to the router configuration. However. the public keys embedded in the received CA (and RA) certificates are saved to the configuration as part of the RSA public key record (called the “RSA public key chain”).

If the CA does not respond by a timeout period after this command is issued, the terminal control will be returned so it will not be tied up. If this happens, you must re-enter the command. Cisco IOS software will not recognize CA certificate expiration dates set for beyond the year 2049. If the validity period of the CA certificate is set to expire after the year 2049, the following error message will be displayed when authentication with the CA server is attempted:

error retrieving certificate :incomplete chain

If you receive an error message similar to this one, check the expiration date of your CA certificate. If the expiration date of your CA certificate is set after the year 2049, you must reduce the expiration date by a year or more.

Examples

In the following example, the router requests the certificate of the CA. The CA sends its certificate and the router prompts the administrator to verify the certificate of the CA by checking the CA certificate's fingerprint. The CA administrator can also view the CA certificate's fingerprint, so you should compare what the CA administrator sees to what the router displays on the screen. If the fingerprint on the router's screen matches the fingerprint viewed by the CA administrator, you should accept the certificate as valid.

```
Router(config)#
crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y
#
```

Related Commands

Command	Description
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.
show crypto pki certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto ca enroll

Note This command was replaced by the **crypto pki enroll** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To obtain the certificate(s) of your router from the certification authority, use the **crypto ca enroll** command in global configuration mode. To delete a current enrollment request, use the **no** form of this command.

crypto ca enroll *name*

no crypto ca enroll *name*

Syntax Description

name	Specifies the name of the CA. Use the same name as when you declared the CA using the **crypto pki trustpoint**command.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command requests certificates from the CA for all of your router's RSA key pairs. This task is also known as enrolling with the CA. (Technically, enrolling and obtaining certificates are two separate events, but they both occur when this command is issued.)

Your router needs a signed certificate from the CA for each RSA key pairs of your router; if you previously generated general purpose keys, this command will obtain the one certificate corresponding to the one general purpose RSA key pair. If you previously generated special usage keys, this command will obtain two certificates corresponding to each of the special usage RSA key pairs.

If you already have a certificate for your keys you will be unable to complete this command; instead, you will be prompted to remove the existing certificate first. (You can remove existing certificates with the **no certificate** command.)

The **crypto ca enroll** command is not saved in the router configuration.

Note If your router reboots after you issue the **crypto ca enroll** command but before you receive the certificate(s), you must reissue the command.

Responding to Prompts

When you issue the **crypto ca enroll** command, you are prompted a number of times.

First, you are prompted to create a challenge password. This password can be up to 80 characters in length. This password is necessary in the event that you ever need to revoke your router's certificate(s). When you ask the CA administrator to revoke your certificate, you must supply this challenge password as a protection against fraudulent or mistaken revocation requests.

Note This password is not stored anywhere, so you need to remember this password.

If you lose the password, the CA administrator may still be able to revoke the router's certificate but will require further manual authentication of the router administrator identity.

You are also prompted to indicate whether or not your router's serial number should be included in the obtained certificate. The serial number is not used by IP Security or Internet Key Exchange but may be used by the CA to either authenticate certificates or to later associate a certificate with a particular router. (Note that the serial number stored is the serial number of the internal board, not the one on the enclosure.) Ask your CA administrator if serial numbers should be included. If you are in doubt, include the serial number.

Normally, you would not include the IP address because the IP address binds the certificate more tightly to a specific entity. Also, if the router is moved, you would need to issue a new certificate. Finally, a router has multiple IP addresses, any of which might be used with IPSec.

If you indicate that the IP address should be included, you will then be prompted to specify the interface of the IP address. This interface should correspond to the interface that you apply your crypto map set to. If you apply crypto map sets to more than one interface, specify the interface that you name in the **crypto map local-address** command.

Examples

In the following example, a router with a general-purpose RSA key pair requests a certificate from the CA. When the router displays the certificate fingerprint, the administrator verifies this number by calling the CA administrator, who checks the number. The fingerprint is correct, so the router administrator accepts the certificate.

There can be a delay between when the router administrator sends the request and when the certificate is actually received by the router. The amount of delay depends on the CA method of operation.

```
Router(config)# crypto ca enroll myca
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password: <mypassword>
Re-enter password: <mypassword>
% The subject name in the certificate will be: myrouter.example.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 03433678
% Include an IP address in the subject name [yes/no]? yes
Interface: ethernet0/0
Request certificate from CA [yes/no]? yes
```

```
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificates' command will also show the fingerprint.
```

Some time later, the router receives the certificate from the CA and displays the following confirmation message:

```
Router(config)#   Fingerprint: 01234567 89ABCDEF FEDCBA98 75543210
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
Router(config)#
```

If necessary, the router administrator can verify the displayed Fingerprint with the CA administrator.

If there is a problem with the certificate request and the certificate is not granted, the following message is displayed on the console instead:

```
%CRYPTO-6-CERTREJ: Certificate enrollment request was rejected by Certificate Authority
```

The subject name in the certificate is automatically assigned to be the same as the RSA key pair's name. In the above example, the RSA key pair was named "myrouter.example.com." (The router assigned this name.)

Requesting certificates for a router with special usage keys would be the same as the previous example, except that two certificates would have been returned by the CA. When the router received the two certificates, the router would have displayed the same confirmation message:

```
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
```

Related Commands

Command	Description
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the router.
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.
show crypto pki certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto ca trustpoint

Note Effective with Cisco IOS Release 12.3(8)T, 12.2(18)SXD, and 12.2(18)SXE, the **crypto ca trustpoint** command is replaced with the **crypto pki trustpoint** command. See the **crypto pki trustpoint** command for more information.

To declare the certification authority (CA) that your router should use, use the **crypto ca trustpoint** command in global configuration mode. To delete all identity information and certificates associated with the CA, use the **no** form of this command.

crypto ca trustpoint *name*

no crypto ca trustpoint *name*

Syntax Description

name	Creates a name for the CA. (If you previously declared the CA and just want to update its characteristics, specify the name you previously created.)

Command Default

Your router does not recognize any CAs until you declare a CA using this command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(15)T	The **match certificate** subcommand was introduced.
12.3(7)T	This command was replaced by the **crypto pki trustpoint** command. You can still enter the **crypto ca trusted-root**or **crypto ca trustpoint** command, but the command will be written in the configuration as “crypto pki trustpoint.”

Usage Guidelines

Use the **crypto ca trustpoint** command to declare a CA, which can be a self-signed root CA or a subordinate CA. Issuing the **crypto ca trustpoint** command puts you in ca-trustpoint configuration mode.

You can specify characteristics for the trustpoint CA using the following subcommands:

- **crl** --Queries the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.

- **default (ca-trustpoint)** --Resets the value of ca-trustpoint configuration mode subcommands to their defaults.
- **enrollment** --Specifies enrollment parameters (optional).
- **enrollment http-proxy** --Accesses the CA by HTTP through the proxy server.
- **match certificate** --Associates a certificate-based access control list (ACL) defined with the **crypto ca certificate map**command.
- **primary** --Assigns a specified trustpoint as the primary trustpoint of the router.
- **root** --Defines the Trivial File Transfer Protocol (TFTP) to get the CA certificate and specifies both a name for the server and a name for the file that will store the CA certificate.

Note Beginning with Cisco IOS Release 12.2(8)T, the **crypto ca trustpoint** command unified the functionality of the **crypto ca identity** and **crypto ca trusted-root** commands, thereby replacing these commands. Although you can still enter the **crypto ca identity** and **crypto ca trusted-root** commands, theconfiguration mode and command will be written in the configuration as **"crypto ca trustpoint**."

Examples

The following example shows how to declare the CA named "ka" and specify enrollment and CRL parameters:

```
crypto ca trustpoint ka
 enrollment url http://kahului:80
```

The following example shows a certificate-based access control list (ACL) with the label "Group" defined in a **crypto ca certificate map** command and included in the **match certificate** subcommand of the **crypto ca | pki trustpoint** command:

```
crypto ca certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
!
crypto ca trustpoint pki
 match certificate Group
```

Related Commands

Command	Description
crl	Queries the CRL to ensure that the certificate of the peer has not been revoked.
default (ca-trustpoint)	Resets the value of a ca-trustpoint configuration subcommand to its default.
enrollment	Specifies the enrollment parameters of your CA.
enrollment http-proxy	Accesses the CA by HTTP through the proxy server.
primary	Assigns a specified trustpoint as the primary trustpoint of the router.

Command	Description
root	Obtains the CA certificate via TFTP.

crypto key generate rsa

- crypto key generate rsa, page 100

crypto key generate rsa

To generate Rivest, Shamir, and Adelman (RSA) key pairs, use the **crypto key generate rsa** commandinglobal configuration mode.

crypto key generate rsa [**general-keys**| **usage-keys**| **signature**| **encryption**] [**label** *key-label*] **[exportable]** [**modulus** *modulus-size*] [**storage** *devicename* **:**] **[redundancy]** [**on** *devicename* **:**]

Syntax Description

general-keys	(Optional) Specifies that a general-purpose key pair will be generated, which is the default.
usage-keys	(Optional) Specifies that two RSA special-usage key pairs, one encryption pair and one signature pair, will be generated.
signature	(Optional) Specifies that the RSA public key generated will be a signature special usage key.
encryption	(Optional) Specifies that the RSA public key generated will be an encryption special usage key.
label *key-label*	(Optional) Specifies the name that is used for an RSA key pair when they are being exported. If a key label is not specified, the fully qualified domain name (FQDN) of the router is used.
exportable	(Optional) Specifies that the RSA key pair can be exported to another Cisco device, such as a router.
modulus *modulus-size*	(Optional) Specifies the IP size of the key modulus. By default, the modulus of a certification authority (CA) key is 1024 bits. The recommended modulus for a CA key is 2048 bits. The range of a CA key modulus is from 350 to 4096 bits. **Note** Effective with Cisco IOS XE Release 2.4 and Cisco IOS Release 15.1(1)T, the maximum key size was expanded to 4096 bits for private key operations. The maximum for private key operations prior to these releases was 2048 bits.
storage *devicename* **:**	(Optional) Specifies the key storage location. The name of the storage device is followed by a colon (:).
redundancy	(Optional) Specifies that the key should be synchronized to the standby CA.

on *devicename* **:**	(Optional) Specifies that the RSA key pair will be created on the specified device, including a Universal Serial Bus (USB) token, local disk, or NVRAM. The name of the device is followed by a colon (:). Keys created on a USB token must be 2048 bits or less.

Command Default

RSA key pairs do not exist.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(8)T	The *key-label* argumentwas added.
12.2(15)T	The **exportable** keyword was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **storage** keyword and *devicename* **:** argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **storage** keyword and *devicename* **:** argument were implemented on the Cisco 7200VXR NPE-G2 platform. The **signature**, **encryption** and **on** keywords and *devicename* **:** argument were added.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.
XE 2.4	The maximum RSA key size was expanded from 2048 to 4096 bits for private key operations.
15.0(1)M	This command was modified. The **redundancy** keyword was introduced.
15.1(1)T	This command was modified. The range value for the **modulus** keyword value is extended from 360 to 2048 bits to 360 to 4096 bits.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Use this command to generate RSA key pairs for your Cisco device (such as a router).

RSA keys are generated in pairs--one public RSA key and one private RSA key.

If your router already has RSA keys when you issue this command, you will be warned and prompted to replace the existing keys with new keys.

Note Before issuing this command, ensure that your router has a hostname and IP domain name configured (with the **hostname** and **ip domain-name** commands). You will be unable to complete the **crypto key generate rsa** command without a hostname and IP domain name. (This situation is not true when you generate only a named key pair.)

Note Secure Shell (SSH) may generate an additional RSA key pair if you generate a key pair on a router having no RSA keys. The additional key pair is used only by SSH and will have a name such as {*router_FQDN*}.server. For example, if a router name is "router1.cisco.com," the key name is "router1.cisco.com.server."

This command is not saved in the router configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.

Note If the configuration is not saved to NVRAM, the generated keys are lost on the next reload of the router.

There are two mutually exclusive types of RSA key pairs: special-usage keys and general-purpose keys. When you generate RSA key pairs, you will be prompted to select either special-usage keys or general-purpose keys.

Special-Usage Keys

If you generate special-usage keys, two pairs of RSA keys will be generated. One pair will be used with any Internet Key Exchange (IKE) policy that specifies RSA signatures as the authentication method, and the other pair will be used with any IKE policy that specifies RSA encrypted keys as the authentication method.

A CA is used only with IKE policies specifying RSA signatures, not with IKE policies specifying RSA-encrypted nonces. (However, you could specify more than one IKE policy and have RSA signatures specified in one policy and RSA-encrypted nonces in another policy.)

If you plan to have both types of RSA authentication methods in your IKE policies, you may prefer to generate special-usage keys. With special-usage keys, each key is not unnecessarily exposed. (Without special-usage keys, one key is used for both authentication methods, increasing the exposure of that key.)

General-Purpose Keys

If you generate general-purpose keys, only one pair of RSA keys will be generated. This pair will be used with IKE policies specifying either RSA signatures or RSA encrypted keys. Therefore, a general-purpose key pair might get used more frequently than a special-usage key pair.

Named Key Pairs

If you generate a named key pair using the *key-label*argument, you must also specify the **usage-keys** keyword or the **general-keys** keyword. Named key pairs allow you to have multiple RSA key pairs, enabling the Cisco IOS software to maintain a different key pair for each identity certificate.

Modulus Length

When you generate RSA keys, you will be prompted to enter a modulus length. The longer the modulus, the stronger the security. However a longer modules takes longer to generate (see the table below for sample times) and takes longer to use.

Table 6: Sample Times by Modulus Length to Generate RSA Keys

Router	360 bits	512 bits	1024 bits	2048 bits (maximum)
Cisco 2500	11 seconds	20 seconds	4 minutes, 38 seconds	More than 1 hour
Cisco 4700	Less than 1 second	1 second	4 seconds	50 seconds

Cisco IOS software does not support a modulus greater than 4096 bits. A length of less than 512 bits is normally not recommended. In certain situations, the shorter modulus may not function properly with IKE, so we recommend using a minimum modulus of 2048 bits.

Note As of Cisco IOS Release 12.4(11)T, peer *public* RSA key modulus values up to 4096 bits are automatically supported. The largest private RSA key modulus is 4096 bits. Therefore, the largest RSA private key a router may generate or import is 4096 bits. However, RFC 2409 restricts the private key size to 2048 bits or less for RSA encryption. The recommended modulus for a CA is 2048 bits; the recommended modulus for a client is 2048 bits.

Additional limitations may apply when RSA keys are generated by cryptographic hardware. For example, when RSA keys are generated by the Cisco VPN Services Port Adapter (VSPA), the RSA key modulus must be a minimum of 384 bits and must be a multiple of 64.

Specifying a Storage Location for RSA Keys

When you issue the **crypto key generate rsa** command with the **storage** *devicename* **:** keyword and argument, the RSA keys will be stored on the specified device. This location will supersede any **crypto key storage** command settings.

Specifying a Device for RSA Key Generation

As of Cisco IOS Release 12.4(11)T and later releases, you may specify the device where RSA keys are generated. Devices supported include NVRAM, local disks, and USB tokens. If your router has a USB token configured and available, the USB token can be used as cryptographic device in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing, and authentication of credentials to be performed on the token. The private key never leaves the USB token and is not exportable. The public key is exportable.

RSA keys may be generated on a configured and available USB token, by the use of the **on** *devicename* **:** keyword and argument. Keys that reside on a USB token are saved to persistent token storage when they are generated. The number of keys that can be generated on a USB token is limited by the space available. If you attempt to generate keys on a USB token and it is full you will receive the following message:

```
% Error in generating keys:no available resources
```

Key deletion will remove the keys stored on the token from persistent storage immediately. (Keys that do not reside on a token are saved to or deleted from nontoken storage locations when the **copy**or similar command is issued.)

For information on configuring a USB token, see " Storing PKI Credentials " chapter in the Cisco IOS Security Configuration Guide, Release 12.4T. For information on using on-token RSA credentials, see the " Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment " chapter in the Cisco IOS Security Configuration Guide , Release 12.4T.

Specifying RSA Key Redundancy Generation on a Device

You can specify redundancy for existing keys only if they are exportable.

Examples

The following example generates a general-usage 1024-bit RSA key pair on a USB token with the label "ms2" with crypto engine debugging messages shown:

```
Router(config)# crypto key generate rsa label ms2 modulus 2048 on usbtoken0:
The name for the keys will be: ms2
% The key modulus size is 2048 bits
% Generating 1024 bit RSA keys, keys will be on-token, non-exportable...
Jan 7 02:41:40.895: crypto_engine: Generate public/private keypair [OK]
Jan 7 02:44:09.623: crypto_engine: Create signature
Jan 7 02:44:10.467: crypto_engine: Verify signature
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_CREATE_PUBKEY(hw)(ipsec)
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_PUB_DECRYPT(hw)(ipsec)
```

Now, the on-token keys labeled "ms2" may be used for enrollment.

The following example generates special-usage RSA keys:

```
Router(config)# crypto key generate rsa usage-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

The following example generates general-purpose RSA keys:

Note You cannot generate both special-usage and general-purpose keys; you can generate only one or the other.

```
Router(config)# crypto key generate rsa general-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

The following example generates the general-purpose RSA key pair “exampleCAkeys”:

```
crypto key generate rsa general-keys label exampleCAkeys
crypto ca trustpoint exampleCAkeys
 enroll url
http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

The following example specifies the RSA key storage location of “usbtoken0:” for “tokenkey1”:

crypto key generate rsa general-keys label tokenkey1 storage usbtoken0:

The following example specifies the **redundancy** keyword:

```
Router(config)# crypto key generate rsa label MYKEYS redundancy
```

The name for the keys will be: MYKEYS

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]:

% Generating 512 bit RSA keys, keys will be non-exportable with redundancy...[OK]

Related Commands

Command	Description
copy	Copies any file from a source to a destination, use the copy command in privileged EXEC mode.
crypto key storage	Sets the default storage location for RSA key pairs.
debug crypto engine	Displays debug messages about crypto engines.
hostname	Specifies or modifies the hostname for the network server.
ip domain-name	Defines a default domain name to complete unqualified hostnames (names without a dotted-decimal domain name).
show crypto key mypubkey rsa	Displays the RSA public keys of your router.
show crypto pki certificates	Displays information about your PKI certificate, certification authority, and any registration authority certificates.

crypto key generate rsa