aaa accounting through aaa local authentication attempts max-fail

aaa accounting (IKEv2 profile)

To enable AAA accounting for IPsec sessions, use the **aaa accounting** command in IKEv2 profile configuration mode. To disable AAA accounting, use the **no** form of this command.

aaa accounting {**psk**| **cert**| **eap**} *list-name*

no aaa accounting {**psk**| **cert**| **eap**} *list-name*

Syntax Description

psk	Specifies a method list if the authentication method preshared key.
cert	Specifies a method list if the authentication method is certificate based.
eap	Specifies a method list if the authentication method is Extensible Authentication Protocol (EAP).
list-name	Name of the AAA list.

Command Default

AAA accounting is disabled.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use the **aaa accounting** command to enable and specify the method list for AAA accounting for IPsec sessions. The **aaa accounting** command can be specific to an authentication method or common to all authentication methods, but not both at the same time. If no method list is specified, the list is common across authentication methods.

Examples

The following example defines an AAA accounting configuration common to all authentication methods:

```
Router(config-ikev2-profile)# aaa accounting common-list1
```

The following example configures an AAA accounting for each authentication method:

```
Router(config-ikev2-profile)# aaa accounting psk psk-list1
Router(config-ikev2-profile)# aaa accounting cert cert-list1
Router(config-ikev2-profile)# aaa accounting eap eap-list1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.

aaa accounting connection h323

To define the accounting method list H.323 using RADIUS as a method with either **stop-only** or **start-stop** accounting options, use the **aaa accounting connection h323** command in global configuration mode. To disable the use of this accounting method list, use the **no** form of this command.

aaa accounting connection h323 {**stop-only**| **start-stop**| **none**} **[broadcast] group groupname**

no aaa accounting connection h323 {**stop-only**| **start-stop**| **none**} **[broadcast] group groupname**

Syntax Description

stop-only	Sends a “stop” accounting notice at the end of the requested user process.
start-stop	Sends 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.
none	Disables accounting services on this line or interface.
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*	Specifies the server group to be used for accounting services. The following are valid server group names: • *string* : Character string used to name a server group. • **radius** : Uses list of all RADIUS hosts. • **tacacs+** : Uses list of all TACACS+ hosts.

Command Default

No accounting method list is defined.

Command Modes

Global configuration

Command History

Release	Modification
11.3(6)NA2	This command was introduced.
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 creates a method list called h323 and is applied by default to all voice interfaces if the **gw-accounting h323** command is also activated.

Examples

The following example enables authentication, authorization, and accounting (AAA) services, gateway accounting services, and defines a connection accounting method list (h323). The h323 accounting method lists specifies that RADIUS is the security protocol that will provide the accounting services, and that the RADIUS service will track start-stop records.

```
aaa new model
gw-accounting h323
aaa accounting connection h323 start-stop group radius
```

Related Commands

Command	Description
gw-accounting	Enables the accounting method for collecting call detail records.

aaa accounting delay-start

To delay the generation of accounting start records until the user IP address is established, use the **aaa accounting delay-start** command in global configuration mode. To disable this functionality, use the **no** form of this command.

aaa accounting delay-start [all] [**vrf** *vrf-name*] [**extended-time** *delay-value*]

no aaa accounting delay-start [all] [**vrf** *vrf-name*] [**extended-time** *delay-value*]

Syntax Description

all	(Optional) Extends the delay of sending accounting start records to all Virtual Route Forwarding (VRF) and non-VRF users.
vrf *vrf-name*	(Optional) Extends the delay of sending accounting start records to the specified VRF user.
extended-time *delay-value*	(Optional) Delays the sending of accounting start records by a configured delay value (in seconds) when the Internet Protocol Control Protocol Version 6 (IPCPv6) address is initialized before the IPCPv4 address is sent to the RADIUS server. The valid values are 1 and 2.

Command Default

Accounting records are not delayed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1	This command was introduced.
12.2(1)DX	This command was modified. The **vrf** keyword and *vrf-name* argument were introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were integrated into Cisco IOS Release 12.2(13)T.
12.3(1)	This command was modified. The **all** keyword was added.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.2(4)S	This command was modified. The **extended-time** keyword and *delay-value* argument were added.

Usage Guidelines

Use the **aaa accounting delay-start** command to delay the generation of accounting start records until the IP address of the user has been established. Use the **vrf** *vrf-name* keyword and argument to delay accounting start records for individual VPN routing and forwarding (VRF) users or use the **all** keyword for all VRF and non-VRF users.

Note The **aaa accounting delay-start** command applies only to non-VRF users. If you have a mix of VRF and non-VRF users, configure the **aaa accounting delay-start** (for non-VRF users), **aaa accounting delay-start vrf** *vrf-name* (for VRF users), or **aaa accounting delay-start all** (for all VRF and non-VRF users) command.

Use the **aaa accounting delay-start extended-time** *delay-value* command in the following two scenarios:

- The user is a dual-stack (IPv4 or IPv6) subscriber.
- The IP address is from a local pool and not from the RADIUS server.

In both scenarios, the IPCPv6 address is initialized first and the IPCPv4 address is initialized after a few milliseconds. Use the **aaa accounting delay-start extended-time** *delay-value* command to delay the accounting start records for the configured time (in seconds) after the IPCPv6 address is sent to the RADIUS server. During this configured delay time, the IPCPv4 address is sent and the Framed-IP-Address attribute is added to the accounting start record. If the IPCPv4 address is not sent in the configured delay time, the accounting start record is sent without the Framed-IP-Address attribute.

Examples

The following example shows how to delay accounting start records until the IP address of the user is established:

```
aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop group radius
aaa accounting delay-start
radius-server host 192.0.2.1 non-standard
radius-server key rad123
```

The following example shows that accounting start records are to be delayed to all VRF and non-VRF users:

```
aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop group radius
aaa accounting delay-start all
radius-server host 192.0.2.1 non-standard
radius-server key rad123
```

The following example shows how to delay accounting start records for 2 seconds when the user is a dual-stack subscriber:

```
aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop group radius
aaa accounting delay-start extended-time 2
radius-server host 192.0.2.1 non-standard
radius-server key rad123
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
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.
tacacs-server host	Specifies a TACACS+ server host.

aaa accounting gigawords

To enable authentication, authorization, and accounting (AAA) 64-bit, high-capacity counters, use the **aaa accounting gigawords** command in global configuration mode. To disable the counters, use the **no** form of this command. (Note that gigaword support is automatically configured unless you unconfigure it using the **no** form of the command.)

aaa accounting gigawords

no aaa accounting gigawords

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not configured, the 64-bit, high-capacity counters that support RADIUS attributes 52 and 53 are automatically enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13.7)T	This command was introduced.

Usage Guidelines

The AAA high-capacity counter process takes approximately 8 percent CPU memory for 24,000 (24 K) sessions running under steady state.

If you have entered the **no** form of this command to turn off the 64-bit counters and you want to reenable them, you will need to enter the **aaa accounting gigawords**command. Also, once you have entered the **no form of the command**, it takes a reload of the router to actually disable the use of the 64-bit counters.

Note The **aaa accounting gigawords** command does not show up in the running configuration unless the **no** form of the command is used in the configuration.

Examples

The following example shows that the AAA 64-bit counters have been disabled:

```
no aaa accounting gigawords
```

aaa accounting include auth-profile

To include authorization profile attributes for the AAA accounting records, use the **aaa accounting include auth-profile**command in global configuration mode. To disable the authorization profile, use the **no** form of this command.

aaa accounting include auth-profile {**delegated-ipv6-prefix| framed-ip-address| framed-ipv6-prefix**}

no aaa accounting include auth-profile {**delegated-ipv6-prefix| framed-ip-address| framed-ipv6-prefix**}

Syntax Description

delegated-ipv6-prefix	Includes the delegated-IPv6-Prefix profile in accounting records.
framed-ip-address	Includes the Framed-IP-Address profile in accounting records.
framed-ipv6-prefix	Includes the Framed-IPv6-Prefix profile in accounting records.

Command Default

authorization profile is included in the aaa accounting records.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced in a release earlier than Cisco IOS Release 15.1(1)T.

Usage Guidelines

The **aaa accounting include auth-profile**command can also be used for a dual-stack session if the negotiation between IPv4 and IPv6 is successful.

Examples

The following example shows how to include the delegated-IPv6-Prefix profile in the AAA accounting records:

```
Router(config)# aaa accounting include auth-profile delegated-ipv6-prefix
```

Related Commands

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

aaa accounting-list

To enable authentication, authorization, and accounting (AAA) accounting when you are using RADIUS for Secure Socket Layer Virtual Private Network (SSL VPN) sessions, use the **aaa accounting-list**command in global configuration mode. To disable the AAA accounting, use the **no** form of this command.

aaa accounting-list *aaa-list*

no aaa accounting-list *aaa-list*

Syntax Description

aaa-list	Name of the AAA accounting list that has been configured under global configuration.

Command Default

AAA accounting is not enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Before configuring this command, ensure that the AAA accounting list has already been configured under global configuration.

Examples

The following example shows that AAA accounting has been configured for an SSL VPN session:

```
Router (config)# aaa accounting-list aaalist1
```

Related Commands

Command	Description
aaa accounting network SSLVPN start-stop group radius	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.

aaa accounting jitter maximum

To provide an interval of time between records so that the AAA server does not get overwhelmed by a constant stream of records, use the **aaa accounting jitter maximum**command in global configuration mode. To return to the default interval, use the **no** form of this command.

aaa accounting jitter maximum max-value

no aaa accounting jitter

Syntax Description

jitter-value	Allows the maximum jitter value from 0 to 2147483 seconds to be set in periodic accounting. The value 0 turns off jitter.

Command Default

Jitter is set to 300 seconds (5 minutes) by default.

Command Modes

Global configuration

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

If certain applications require that periodic records be sent at exact intervals, disable jitter by setting it to 0.

Examples

The following example sets the maximum jitter value to 20 seconds:

```
aaa accounting jitter maximum 20
```

Related Commands

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

aaa accounting nested

To specify that NETWORK records be generated, or nested, within EXEC “start” and “stop” records for PPP users who start EXEC terminal sessions, use the **aaa accounting nested** command in global configuration mode. To allow the sending of records for users with a NULL username, use the **no** form of this command.

aaa accounting nested [**suppress stop**]

no aaa accounting nested [**suppress stop**]

Syntax Description

suppress stop	(Optional) Prevents sending a multiple set of records (one from EXEC and one from PPP) for the same client.

Command Default

Disabled

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.
12.4(11)T	The **suppress** and **stop** keywords were added.
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 accounting nested**command when you want to specify that NETWORK records be nested within EXEC “start” and “stop” records, such as for PPP users who start EXEC terminal sessions. In some cases, such as billing customers for specific services, it can be desirable to keep NETWORK “start” and “stop” records together, essentially nesting them within the framework of the EXEC “start” and “stop” messages. For example, if you dial in using PPP, you can create the following records: EXEC-start, NETWORK-start, EXEC-stop, and NETWORK-stop. By using the **aaa accounting nested command to**generate accounting records, NETWORK-stop records follow NETWORK-start messages: EXEC-start, NETWORK-start, NETWORK-stop, EXEC-stop.

Use the **aaa accounting nested suppress stop** command to suppress the sending of EXEC-stop accounting records and to send only PPP accounting records.

Examples

The following example enables nesting of NETWORK accounting records for user sessions:

```
Router(config)# aaa accounting nested
```

The following example disables nesting of EXEC accounting records for user sessions:

```
Router(config)# aaa accounting nested suppress stop
```

aaa accounting redundancy

To set the Accounting, Authorization, and Authentication (AAA) platform redundancy accounting behavior, use the **aaa accounting redundancy** command in global configuration mode. To disable the accounting behavior, use the **no** form of this command.

aaa accounting redundancy {**best-effort-reuse [send-interim]| new-session| suppress system-records**}

no aaa accounting redundancy {**best-effort-reuse [send-interim]| new-session| suppress system-records**}

Syntax Description

best-effort-reuse	Tracks redundant accounting sessions as existing sessions after switchover.
send-interim	(Optional) Sends an interim accounting update after switchover.
new-session	Tracks redundant accounting sessions as new sessions after switchover.
suppress	Suppresses specific records upon switchover.
system-records	Suppresses system records upon switchover.

Command Default

A redundant session is set as a new session upon switchover.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
Cisco IOS XE Release 3.5S	This command was modified. The **send-interim** keyword was added.

Usage Guidelines

Use the **aaa accounting redundancy** command to specify the AAA platform redundancy accounting behavior. This command also enables you to track the redundant sessions or existing sessions upon switchover.

Use the **send-interim** keyword to send the interim accounting record first after a switchover. The router sends the interim update for all sessions that survived the switchover as soon as the standby processor becomes active.

Examples

The following example shows how to set the AAA platform redundancy accounting behavior to track redundant sessions as existing sessions upon switchover:

```
Router(config)# aaa accounting redundancy best-effort-reuse
```

The following example shows how to enable the router to send the interim accounting record first after a switchover:

```
Router(config)# aaa accounting redundancy best-effort-reuse send-interim
```

Related Commands

Command	Description
aaa accounting delay-start	Specifies delay generation of accounting “start” records until the user IP address is established.
aaa authentication dot1x	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.

aaa accounting resource start-stop group

To enable full r esource accounting, which will generate both a “start” record at call setup and a “stop” record at call termination, use the aaa accounting resource start-stop group command in global configuration mode. To disable full resource accounting, use the no form of this command.

aaa accounting resource *method-list* **start-stop [broadcast] group** *groupname*

no aaa accounting resource *method-list* **start-stop [broadcast] group** *groupname*

Syntax Description

method-list	Method used for accounting services. Use one of the following options: • **default** : Uses the listed accounting methods that follow this argument as the default list of methods for accounting services. • *string* : Character string used to name the list of accounting methods.
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.
groupname	Specifies the server group to be used for accounting services. The following are valid server group names: • *string* : Character string used to name a server group. • **radius** : Uses list of all RADIUS hosts. • **tacacs+** : Uses list of all TACACS+ hosts.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA

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

Usage Guidelines

Use the aaa accounting resource start-stop group command to send a “start” record at each call setup followed with a corresponding “stop” record at the call disconnect. There is a separate “call setup-call disconnect “start-stop” accounting record tracking the progress of the resource connection to the device, and a separate “user authentication start-stop accounting” record tracking the user management progress. These two sets of accounting records are interlinked by using a unique session ID for the call.

You may want to use this command to manage and monitor wholesale customers from one source of data reporting, such as accounting records.

Note Sending “start-stop” records for resource allocation along with user “start-stop” records during user authentication can lead to serious performance issues and is discouraged unless absolutely required.

All existing AAA accounting method list and server group options are made available to this command.

Examples

The following example shows how to configure resource accounting for “start-stop” records:

```
aaa new-model
aaa authentication login AOL group radius local
aaa authentication ppp default group radius local
aaa authorization exec AOL group radius if-authenticated
aaa authorization network default group radius if-authenticated
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting resource default start-stop group radius
```

Related Commands

Command	Description
aaa accounting start-stop failure	Enables resource failure stop accounting support, which will only generate a stop record at any point prior to user authentication if a call is terminated.

aaa accounting resource stop-failure group

To enable re source failure stop accounting support, which will generate a “stop” record at any point prior to user authentication only if a call is terminated, use the aaa accounting resource stop-failure group command in global configuration mode. To disable resource failure stop accounting, use the no form of this command.

aaa accounting resource *method-list* **stop-failure [broadcast] group** *groupname*

no aaa accounting resource *method-list* **stop-failure [broadcast] group** *groupname*

Syntax Description

method-list	Method used for accounting services. Use one of the following options: • **default** : Uses the listed accounting methods that follow this argument as the default list of methods for accounting services. • *string* : Character string used to name the list of accounting methods.
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.
groupname	Group to be used for accounting services. Use one of the following options: • *string* : Character string used to name a server group. • **radius** : Uses list of all RADIUS hosts. • **tacacs+** : Uses list of all TACACS+ hosts.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA

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

Usage Guidelines

Use the aaa accounting resource stop-failure group command to generate a “stop” record for any calls that do not reach user authentication; this function creates “stop” accounting records for the moment of call setup. All calls that pass user authentication will behave as before; that is, no additional accounting records will be seen.

All existing authentication, authorization, and accounting (AAA) accounting method list and server group options are made available to this command.

Examples

The following example shows how to configure “stop” accounting records from the moment of call setup:

```
aaa new-model
aaa authentication login AOL group radius local
aaa authentication ppp default group radius local
aaa authorization exec AOL group radius if-authenticated
aaa authorization network default group radius if-authenticated
aaa accounting exec default start-stop group radius
aaa accounting network default start-stop group radius
aaa accounting resource default stop-failure group radius
```

Related Commands

Command	Description
aaa accounting resource start-stop group	Enables full resource accounting, which will generate both a “start” record at call setup and a “stop” record at call termination.

aaa accounting send counters ipv6

To send IPv6 counters in the stop record to the accounting server, use the **aaa accounting send counters ipv6**command in global configuration mode. To stop sending IPv6 counters, use the **no** form of this command.

aaa accounting send counters ipv6

no aaa accounting send counters ipv6

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 counters in the stop records are not sent to the accounting server.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

The **aaa accounting send counters ipv6**command sends IPv6 counters in the stop record to the accounting server.

Examples

The following example shows how enable the router to send IPv6 counters in the stop record to the accounting server:

```
Router(config)# aaa accounting send counters ipv6
```

aaa accounting send stop-record always

To send a stop record whether or not a start record was sent, use the **aaa accounting send stop-record always** command in global configuration mode. To disable sending a stop record, use the **no** form of this command.

aaa accounting send stop-record always

no aaa accounting send stop-record always

Syntax Description

This command has no arguments or keywords.

Command Default

A stop record is not sent.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

When the **aaa accounting send stop-record always** command is enabled, accounting stop records are sent, even if their corresponding accounting starts were not sent out previously. This command enables stop records to be sent whether local authentication, or other authentication, is configured.

When a session is terminated on a Network Control Protocol (NCP) timeout, a stop record needs to be sent, even if a start record was not sent.

Examples

The following example shows how to enable stop records to be sent always when an NCP timeout occurs, whether or not a start record was sent:

```
Router(config)# aaa accounting send stop-record always
```

aaa accounting send stop-record authentication

To refine generation of authentication, authorization, and accounting (AAA) accounting “stop” records, use the **aaa accounting send stop-record authentication** command in global configuration mode. To end generation of accounting stop records, use the **no** form of this command that is appropriate.

aaa accounting send stop-record authentication {**failure**| **success remote-server**} [**vrf** *vrf-name*]

Failed Calls: End Accounting Stop Record Generation

no aaa accounting send stop-record authentication failure [**vrf** *vrf-name*]

Successful Calls: End Accounting Stop Record Generation

no aaa accounting send stop-record authentication success remote-server [**vrf** *vrf-name*]

Syntax Description

failure	Used to generate accounting “stop” records for calls that fail to authenticate at login or during session negotiation.

success	• Used to generate accounting “stop” records for calls that have been authenticated by the remote AAA server. A “stop” record will be sent after the call is terminated.
	• Used to generate accounting "stop" records for calls that have *not* been authenticated by the remote AAA server. A“stop” record will be sent if one of the following states is true:
	  • The start record has been sent.
	  • The call is successfully established and is terminated with the “stop-only” configuration.

remote-server	Used to specify that the remote server is to be used.
vrf *vrf-name*	(Optional) Used to enable this feature for a particular Virtual Private Network (VPN) routing and forwarding configuration.

Command Default

Accounting “stop” records are sent only if one of the following is true:

- A start record has been sent.

- The call is successfully established with the “stop-only” configuration and is terminated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(1)DX	The vrf keyword and *vrf-name* argument were introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	The vrf keyword and *vrf-name* argument were added.
12.4(2)T	The **success** and **remote-server** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
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.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

When the **aaa accounting** command is activated, by default the Cisco IOS software does not generate accounting records for system users who fail login authentication or who succeed in login authentication but fail PPP negotiation for some reason. The **aaa accounting** command can be configured to sent a “stop” record using either the **start-stop** keyword or the **stop-only** keyword.

When the **aaa accounting** command is issued with either the **start-stop** keyword or the **stop-only** keyword, the “stop” records can be further configured with the **aaa accounting send stop-record authentication**command. The failure and success keywords are mutually exclusive. If you have the **aaa accounting send stop-record authentication** command enabled with the **failure** keyword and then enable the same command with the **success** keyword, accounting stop records will no longer be generated for failed calls. Accounting stop records are sent for successful calls only until you issue either of the following commands:

- **no aaa accounting send stop-record authentication success remote-server**
- **aaa accounting send stop-record authentication failure**

When using the **failure** keyword, a “stop” record will be sent for calls that are rejected during authentication.

When using the **success** keyword, a “stop” record will be sent for calls that meet one of the following criteria:

- Calls that are authenticated by a remote AAA server when the call is terminated.
- Calls that are not authenticated by a remote AAA server and the start record has been sent.
- Calls that are successfully established and then terminated with the "stop-only" **aaa accounting** configuration.

Use the **vrf**vrf-name keyword and argument to generate accounting "stop" records per VPN routing and forwarding configuration.

Note The **success** and **remote-server** keywords are not available in Cisco IOS Release 12.2SX.

Examples

The following example shows how to generate "stop" records for users who fail to authenticate at login or during session negotiation:

aaa accounting send stop-record authentication failure

The following example shows "start" and "stop" records being sent for a successful call when the **aaa accounting send stop-record authentication**command is issued with the **failure** keyword:

```
Router# show running-config | include aaa

.
.
.
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group radius
.
.
.
*Jul  7 03:28:31.543: AAA/BIND(00000018): Bind i/f Virtual-Template2
*Jul  7 03:28:31.547: ppp14 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:28:33.555: AAA/AUTHOR (0x18): Pick method list 'default'
*Jul  7 03:28:33.555: AAA/BIND(00000019): Bind i/f
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ
*Jul  7 03:28:33.555:  Tnl 5192 L2TP: O SCCRQ, flg TLS, ver 2, len 141, tnl 0,
ns 0, nr 0
         C8 02 00 8D 00 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 10 00 00 00 07 4C 41 43 2D 74 75
         6E 6E 65 6C 00 19 00 00 00 08 43 69 73 63 6F 20
         53 79 73 74 65 6D 73 ...
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 0, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse SCCRP
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 2, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Protocol Ver 256
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 3, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Framing Cap 0x0
*Jul  7 03:28:33.563:  Tnl 5192 L2TP: Parse  AVP 4, len 10, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Bearer Cap 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 6, len 8, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Firmware Ver 0x1120
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 7, len 16, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Hostname LNS-tunnel
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 8, len 25, flag 0x0
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Vendor Name Cisco Systems, Inc.
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 9, len 8, flag 0x8000 (M)
```

```
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Assigned Tunnel ID 6897
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 10, len 8, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Rx Window Size 20050
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 11, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng
         81 13 03 F6 A8 E4 1D DD 25 18 25 6E 67 8C 7C 39
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Parse  AVP 13, len 22, flag 0x8000 (M)
*Jul  7 03:28:33.567:  Tnl 5192 L2TP: Chlng Resp
         4D 52 91 DC 1A 43 B3 31 B4 F5 B8 E1 88 22 4F 41
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: No missing AVPs in SCCRP
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP, flg TLS, ver 2, len 157, tnl
5192, ns 0, nr 1
contiguous pak, size 157
         C8 02 00 9D 14 48 00 00 00 00 00 01 80 08 00 00
         00 00 00 02 80 08 00 00 00 02 01 00 80 0A 00 00
         00 03 00 00 00 00 80 0A 00 00 00 04 00 00 00 00
         00 08 00 00 00 06 11 20 80 10 00 00 00 07 4C 4E
         53 2D 74 75 6E 6E 65 6C ...
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: I SCCRP from LNS-tunnel
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN  to LNS-tunnel tnlid 6897
*Jul  7 03:28:33.571:  Tnl 5192 L2TP: O SCCCN, flg TLS, ver 2, len 42, tnl
6897, ns 1, nr 1
         C8 02 00 2A 1A F1 00 00 00 01 00 01 80 08 00 00
         00 00 00 03 80 16 00 00 00 0D 32 24 17 BC 6A 19
         B1 79 F3 F9 A9 D4 67 7D 9A DB
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ to LNS-tunnel 6897/0
*Jul  7 03:28:33.571: uid:14 Tnl/Sn 5192/11 L2TP: O ICRQ, flg TLS, ver 2, len
63, tnl 6897, lsid 11, rsid 0, ns 2, nr 1
         C8 02 00 3F 1A F1 00 00 00 02 00 01 80 08 00 00
         00 00 00 0A 80 0A 00 00 00 0F C8 14 B4 03 80 08
         00 00 00 0E 00 0B 80 0A 00 00 00 12 00 00 00 00
         00 0F 00 09 00 64 0F 10 09 02 02 00 1B 00 00
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 0, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Parse  AVP 14, len 8, flag
0x8000 (M)
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: Assigned Call ID 5
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: No missing AVPs in ICRP
*Jul  7 03:28:33.575: uid:14 Tnl/Sn 5192/11 L2TP: I ICRP, flg TLS, ver 2, len
28, tnl 5192, lsid 11, rsid 0, ns 1, nr 3
contiguous pak, size 28
         C8 02 00 1C 14 48 00 0B 00 01 00 03 80 08 00 00
         00 00 00 0B 80 08 00 00 00 0E 00 05
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN to LNS-tunnel 6897/5
*Jul  7 03:28:33.579: uid:14 Tnl/Sn 5192/11 L2TP: O ICCN, flg TLS, ver 2, len
167, tnl 6897, lsid 11, rsid 5, ns 3, nr 2
         C8 02 00 A7 1A F1 00 05 00 03 00 02 80 08 00 00
         00 00 00 0C 80 0A 00 00 00 18 06 1A 80 00 00 0A
         00 00 00 26 06 1A 80 00 80 0A 00 00 00 13 00 00
         00 01 00 15 00 00 00 1B 01 04 05 D4 03 05 C2 23
         05 05 06 0A 0B E2 7A ...
*Jul  7 03:28:33.579: RADIUS/ENCODE(00000018):Orig. component type = PPoE
*Jul  7 03:28:33.579: RADIUS(00000018): Config NAS IP: 0.0.0.0
*Jul  7 03:28:33.579: RADIUS(00000018): sending
*Jul  7 03:28:33.579: RADIUS/ENCODE: Best Local IP-Address 192.168.202.169 for
Radius-Server 192.168.202.169
*Jul  7 03:28:33.579: RADIUS(00000018): Send Accounting-Request to
172.19.192.238:2196 id 1646/23, len 176
*Jul  7 03:28:33.579: RADIUS:  authenticator 3C 81 D6 C5 2B 6D 21 8E - 19 FF
43 B5 41 86 A8 A5
*Jul  7 03:28:33.579: RADIUS:  Acct-Session-Id     [44]  10  "00000023"
*Jul  7 03:28:33.579: RADIUS:  Framed-Protocol     [7]   6
PPP                      [1]
*Jul  7 03:28:33.579: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                  [1]
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Endpoi[66]  10  "192.168.202.169"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Endpoi[67]  10  "192.168.202.169"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Assignment-Id[82]  5   "lac"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                  [3]
*Jul  7 03:28:33.583: RADIUS:  Acct-Tunnel-Connecti[68]  12  "3356800003"
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Client-Auth-I[90]  12  "LAC-tunnel"
```

```
*Jul  7 03:28:33.583: RADIUS:  Tunnel-Server-Auth-I[91]  12  "LNS-tunnel"
*Jul  7 03:28:33.583: RADIUS:  User-Name           [1]   16  "user@domain.com"
*Jul  7 03:28:33.583: RADIUS:  Acct-Authentic      [45]  6
Local                     [2]
*Jul  7 03:28:33.583: RADIUS:  Acct-Status-Type    [40]  6
Start                     [1]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:28:33.583: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:28:33.583: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:28:33.583: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:28:33.583: RADIUS:  NAS-IP-Address      [4]   6
192.168.202.169
*Jul  7 03:28:33.583: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:28:33.683: RADIUS: Received from id 1646/23 192.168.202.169:2196,
Accounting-response, len 20
*Jul  7 03:28:33.683: RADIUS:  authenticator 1C E9 53 42 A2 8A 58 9A - C3 CC
1D 79 9F A4 6F 3A
```

The following example shows the “stop” record being sent when the call is rejected during authentication when the **aaa accounting send stop-record authentication**command is issued with the **success** keyword.

```
Router# show running-config | include aaa
,
,
,
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting send stop-record authentication success remote-server
aaa accounting network default start-stop group radius
Router#
*Jul  7 03:39:40.199: AAA/BIND(00000026): Bind i/f Virtual-Template2
*Jul  7 03:39:40.199: ppp21 AAA/AUTHOR/LCP: Authorization succeeds trivially
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:42.199: RADIUS:  AAA Unsupported     [156] 7
*Jul  7 03:39:42.199: RADIUS:   30 2F 30 2F
30                                  [0/0/0]
*Jul  7 03:39:42.199: RADIUS(00000026): Config NAS IP: 0.0.0.0
*Jul  7 03:39:42.199: RADIUS/ENCODE(00000026): acct_session_id: 55
*Jul  7 03:39:42.199: RADIUS(00000026): sending
*Jul  7 03:39:42.199: RADIUS/ENCODE: Best Local IP-Address 192.168.202.169 for
Radius-Server 192.168.202.169
*Jul  7 03:39:42.199: RADIUS(00000026): Send Access-Request to
172.19.192.238:2195 id 1645/14, len 94
*Jul  7 03:39:42.199: RADIUS:  authenticator A6 D1 6B A4 76 9D 52 CF - 33 5D
16 BE AC 7E 5F A6
*Jul  7 03:39:42.199: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:42.199: RADIUS:  User-Name           [1]   16  "user@domain.com"
*Jul  7 03:39:42.199: RADIUS:  CHAP-Password       [3]   19  *
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:39:42.199: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:42.199: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:42.199: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:42.199: RADIUS:  NAS-IP-Address      [4]   6
192.168.202.169
*Jul  7 03:39:42.271: RADIUS: Received from id 1645/14 192.168.202.169:2195,
Access-Accept, len 194
*Jul  7 03:39:42.271: RADIUS:  authenticator 30 AD FF 8E 59 0C E4 6C - BA 11
23 63 81 DE 6F D7
*Jul  7 03:39:42.271: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  26
```

```
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   20  "vpdn:tunnel-
id=lac"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  29
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   23  "vpdn:tunnel-
type=l2tp"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  30
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   24  "vpdn:gw-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  31
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   25  "vpdn:nas-
password=cisco"
*Jul  7 03:39:42.275: RADIUS:  Vendor, Cisco       [26]  34
*Jul  7 03:39:42.275: RADIUS:   Cisco AVpair       [1]   28  "vpdn:ip-
addresses=192.168.202.169"
*Jul  7 03:39:42.275: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:42.275: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:42.275: RADIUS(00000026): Received from id 1645/14
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-id
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: tunnel-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: gw-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: nas-password
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: ip-addresses
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: service-type
*Jul  7 03:39:42.275: ppp21 PPP/AAA: Check Attr: Framed-Protocol
*Jul  7 03:39:42.279: AAA/BIND(00000027): Bind i/f
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ
*Jul  7 03:39:42.279:  Tnl 21407 L2TP: O SCCRQ, flg TLS, ver 2, len 134, tnl
0, ns 0, nr 0
         C8 02 00 86 00 00 00 00 00 00 00 80 08 00 00
         00 00 00 01 80 08 00 00 00 02 01 00 00 08 00 00
         00 06 11 30 80 09 00 00 00 07 6C 61 63 00 19 00
         00 00 08 43 69 73 63 6F 20 53 79 73 74 65 6D 73
         2C 20 49 6E 63 2E 80 ...
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN
*Jul  7 03:39:49.279:  Tnl 21407 L2TP: O StopCCN, flg TLS, ver 2, len 66, tnl
0, ns 1, nr 0
         C8 02 00 42 00 00 00 00 00 01 00 00 80 08 00 00
         00 00 00 04 80 1E 00 00 00 01 00 02 00 06 54 6F
         6F 20 6D 61 6E 79 20 72 65 74 72 61 6E 73 6D 69
         74 73 00 08 00 09 00 69 00 01 80 08 00 00 00 09
         53 9F
*Jul  7 03:39:49.279: RADIUS/ENCODE(00000026):Orig. component type = PPoE
*Jul  7 03:39:49.279: RADIUS(00000026): Config NAS IP: 0.0.0.0
*Jul  7 03:39:49.279: RADIUS(00000026): sending
*Jul  7 03:39:49.279: RADIUS/ENCODE: Best Local IP-Address 192.168.202.169 for
Radius-Server 192.168.202.169
*Jul  7 03:39:49.279: RADIUS(00000026): Send Accounting-Request to
192.168.202.169:2196 id 1646/32, len 179
*Jul  7 03:39:49.279: RADIUS:  authenticator 0A 85 2F F0 65 6F 25 E1 - 97 54
CC BF EA F7 62 89
*Jul  7 03:39:49.279: RADIUS:  Acct-Session-Id     [44]  10  "00000037"
*Jul  7 03:39:49.279: RADIUS:  Framed-Protocol     [7]   6
PPP                       [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Medium-Type  [65]  6
00:IPv4                   [1]
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Client-Endpoi[66]  10  "192.168.202.169"
*Jul  7 03:39:49.279: RADIUS:  Tunnel-Server-Endpoi[67]  10  "192.168.202.169"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Type         [64]  6
00:L2TP                   [3]
*Jul  7 03:39:49.283: RADIUS:  Acct-Tunnel-Connecti[68]  3   "0"
*Jul  7 03:39:49.283: RADIUS:  Tunnel-Client-Auth-I[90]  5   "lac"
*Jul  7 03:39:49.283: RADIUS:  User-Name           [1]   16  "user@domain.com"
*Jul  7 03:39:49.283: RADIUS:  Acct-Authentic      [45]  6
RADIUS                    [1]
*Jul  7 03:39:49.283: RADIUS:  Acct-Session-Time   [46]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Octets   [42]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Octets  [43]  6
```

```
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Input-Packets  [47]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Output-Packets [48]  6
0
*Jul  7 03:39:49.283: RADIUS:  Acct-Terminate-Cause[49]  6   nas-
error                 [9]
*Jul  7 03:39:49.283: RADIUS:  Acct-Status-Type    [40]  6
Stop                      [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Type       [61]  6
Virtual                   [5]
*Jul  7 03:39:49.283: RADIUS:  NAS-Port            [5]   6
0
*Jul  7 03:39:49.283: RADIUS:  NAS-Port-Id         [87]  9   "0/0/0/0"
*Jul  7 03:39:49.283: RADIUS:  Service-Type        [6]   6
Framed                    [2]
*Jul  7 03:39:49.283: RADIUS:  NAS-IP-Address      [4]   6
192.168.202.169
*Jul  7 03:39:49.283: RADIUS:  Acct-Delay-Time     [41]  6
0
*Jul  7 03:39:49.335: RADIUS: Received from id 1646/32 192.168.202.169:2196,
Accounting-response, len 20
*Jul  7 03:39:49.335: RADIUS:  authenticator C8 C4 61 AF 4D 9F 78 07 - 94 2B
44 44 17 56 EC 03
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.

aaa accounting session-duration ntp-adjusted

To calculate RADIUS attribute 46, Acct-Sess-Time, on the basis of the Network Time Protocol (NTP) clock time, use the **aaa accounting session-duration ntp-adjusted** command in global configuration mode. To disable the calculation that was configured on the basis of the NTP clock time, use the **no** form of this command.

aaa accounting session-duration ntp-adjusted

no aaa accounting session-duration ntp-adjusted

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not configured, RADIUS attribute 46 is calculated on the basis of the 64-bit monotonically increasing counter, which is not NTP adjusted.

Command Modes

Global configuration

Command History

Release	Modification
12.2(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

If this command is not configured, RADIUS attribute 46 can skew the session time by as much as 5 to 7 seconds for calls that have a duration of more than 24 hours. However, you may not want to configure the command for short-lived calls or if your device is up for only a short time because of the convergence time required if the session time is configured on the basis of the NTP clock time.

For RADIUS attribute 46 to reflect the NTP-adjusted time, you must configure the **ntp server** command as well as the **aaa accounting session-duration ntp-adjusted** command.

Examples

The following example shows that the attribute 46 session time is to be calculated on the basis of the NTP clock time:

```
aaa new-model
aaa authentication ppp default group radius
aaa accounting session-time ntp-adjusted
aaa accounting network default start-stop group radius
```

Related Commands

Command	Description
ntp server	Allows the software clock to be synchronized by a NTP time server.

aaa accounting suppress null-username

To prevent the Cisco IOS software from sending accounting records for users whose username string is NULL, use the **aaa accounting suppress null-username**command in global configuration mode. To allow sending records for users with a NULL username, use the **no** form of this command.

aaa accounting suppress null-username

no aaa accounting suppress null-username

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	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

When **aaa accounting** is activated, the Cisco IOS software issues accounting records for all users on the system, including users whose username string, because of protocol translation, is NULL. This command prevents accounting records from being generated for those users who do not have usernames associated with them.

Examples

The following example suppresses accounting records for users who do not have usernames associated with them:

```
aaa accounting suppress null-username
```

Related Commands

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

aaa accounting update

To enable periodic interim accounting records to be sent to the accounting server, use the **aaa accounting update**command in global configuration mode. To disable interim accounting updates, use the **no** form of this command.

aaa accounting update [newinfo] [**periodic** *number* [**jitter maximum max-value**]]

no aaa accounting update

Syntax Description

newinfo	(Optional) An interim accounting record is sent to the accounting server whenever there is new accounting information to report relating to the user in question.
periodic	(Optional) An interim accounting record is sent to the accounting server periodically, as defined by the *number*.
number	(Optional) Integer specifying number of minutes.
jitter	(Optional) Allows you to set the maximum jitter value in periodic accounting.
maximum max-value	The number of seconds to set for maximum jitter in periodic accounting. The value 0 turns off jitter. Jitter is set to 300 seconds (5 minutes) by default.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(13)T	Introduced support for generation of an additional updated interim accounting record that contains all available attributes when a call leg is connected.
12.2(15)T11	The jitter keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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

Usage Guidelines

- When the **aaa accounting update**commandis activated, the Cisco IOS software issues interim accounting records for all users on the system. If the **newinfo** keyword is used, interim accounting records will be sent to the accounting server every time there is new accounting information to report. An example would be when IP Control Protocol (IPCP) completes IP address negotiation with the remote peer. The interim accounting record will include the negotiated IP address used by the remote peer.
- When the **gw-accounting aaa** command and the **aaa accounting update newinfo** command and keyword are activated, Cisco IOS software generates and sends an additional updated interim accounting record to the accounting server when a call leg is connected. All attributes (for example, h323-connect-time and backward-call-indicators (BCI)) available at the time of call connection are sent through this interim updated accounting record.
- When used with the **periodic**keyword, interim accounting records are sent periodically as defined by the number. The interim accounting record contains all of the accounting information recorded for that user up to the time the accounting record is sent.
- When using both the **newinfo** and **periodic** keywords, interim accounting records are sent to the accounting server every time there is new accounting information to report, and accounting records are sent to the accounting server periodically as defined by the number. For example, if you configure the **aaa accounting update newinfo periodic** *number*command, all users currently logged in will continue to generate periodic interim accounting records while new users will generate accounting records based on the **newinfo** algorithm.
- Vendor-specific attributes (VSAs) such as h323-connect-time and backward-call-indicator (BCI) are transmitted in the interim update RADIUS message when the **aaa accounting update newinfo** command and keyword are enabled.
- Jitter is used to provide an interval of time between records so that the AAA server does not get overwhelmed by a constant stream of records. If certain applications require that periodic records be sent a exact intervals, you should disable jitter by setting it to 0.

Caution Using the **aaa accounting update periodic** command and keyword can cause heavy congestion when many users are logged into the network.

Examples

The following example sends PPP accounting records to a remote RADIUS server. When IPCP completes negotiation, this command sends an interim accounting record to the RADIUS server that includes the negotiated IP address for this user; it also sends periodic interim accounting records to the RADIUS server at 30-minute intervals.

```
aaa accounting network default start-stop group radius
aaa accounting update newinfo periodic 30
```

The following example sends periodic interim accounting records to the RADIUS server at 30-minute intervals and disables jitter:

```
aaa accounting update newinfo periodic 30 jitter maximum 0
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
gw-accounting aaa	Enables VoIP gateway accounting through the AAA system.

aaa attribute

To add calling line identification (CLID) and dialed number identification service (DNIS) attribute values to a user profile, use the **aaa attribute**command in AAA-user configuration mode. To remove this command from your configuration, use the **no** form of this command.

aaa attribute {**clid**| **dnis**} *attribute-value*

no aaa attribute {**clid**| **dnis**} *attribute-value*

Syntax Description

clid	Adds CLID attribute values to the user profile.
dnis	Adds DNIS attribute values to the user profile.
attribute-value	Specifies a name for CLID or DNIS attribute values.

Command Default

If this command is not enabled, you will have an empty user profile.

Command Modes

AAA-user configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
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

Use the **aaa attribute**command to add CLID or DNIS attribute values to a named user profile, which is created by using the **aaa user profile** command. The CLID or DNIS attribute values can be associated with the record that is going out with the user profile (via the **test aaa group**command), thereby providing the RADIUS server with access to CLID or DNIS information when the server receives a RADIUS record.

Examples

The following example shows how to add CLID and DNIS attribute values to the user profile “cat”:

```
aaa user profile cat
 aaa attribute clid clidval
 aaa attribute dnis dnisval
```

Related Commands

Command	Description
aaa user profile	Creates a AAA user profile.
test aaa group	Associates a DNIS or CLID user profile with the record that is sent to the RADIUS server.

aaa attribute list

To define an authentication, authorization, and accounting (AAA) attribute list locally on a router, use the **aaa attribute list** command in global configuration mode or IKEv2 authorization policy configuration mode. To remove the AAA attribute list, use the **no** form of this command.

aaa attribute list *list-name*

no aaa attribute list *list-name*

Syntax Description

list-name	Name of the aaa attribute list.

Command Default

A local attribute list is not defined.

Command Modes

Global configuration (config)

IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
12.3(7)XI1	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
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

There is no limit to the number of lists that can be defined (except for NVRAM storage limits).

Use this command to refer to a AAA attribute list. This list must be defined in global configuration mode. Among the AAA attributes, the list can have 'interface-config attribute that is used to apply interface configuration mode commands on the virtual access interface associated with the session.

Examples

The following example shows that the attribute list named “TEST” is to be added to the subscriber profile “cisco.com”:

```
aaa authentication ppp template1 local
```

```
aaa authorization network template1 local
!
aaa attribute list TEST
   attribute type interface-config "ip unnumbered FastEthernet0" service ppp protocol lcp
   attribute type interface-config "ip vrf forwarding blue" service ppp protocol lcp
!
ip vrf blue
 description vrf blue template1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
subscriber authorization enable
!
subscriber profile cisco.com
 service local
 aaa attribute list TEST
!
bba-group pppoe grp1
 virtual-template 1
 service profile cisco.com
!
interface Virtual-Template1
 no ip address
 no snmp trap link-status
 no peer default ip address
 no keepalive
 ppp authentication pap template1
 ppp authorization template1
!
```

The following examples shows how to configure an AAA attribute list 'attr-list1' which is referred from IKEv2 authorization policy. The AAA attribute list has 'interface-config' attributes.

```
!
aaa attribute list attr-list1
attribute type interface-config "ip mtu 1100"
attribute type interface-config "tunnel key 10"
!
!
crypto ikev2 authorization policy pol1
 aaa attribute list attr-list1
!
```

Related Commands

Command	Description
attribute type	Defines an attribute type that is to be added to an attribute list locally on a router.
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.

aaa authentication (IKEv2 profile)

To specify the AAA authentication list for Extensible Authentication Protocol (EAP) authentication, use the **aaa authentication**command in IKEv2 profile configuration mode. To remove the AAA authentication for EAP, use the **no** form of this command.

aaa authentication eap *list-name*

no aaa authentication eap

Syntax Description

eap	Specifies the external EAP server for the authentication list.
list-name	Name of the AAA authentication list.

Command Default

AAA authentication for EAP is not specified.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify the AAA authentication list for EAP authentication. The **crypto ikev2 profile** command must be enabled before this command is executed.

Examples

The following example shows how to configure the remote access server using the remote EAP authentication method with an external EAP server:

```
Router(config)# aaa new-model
Router(config)# aaa authentication login aaa-eap-list default group radius
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# authentication remote eap
Router(config-ikev2-profile)# aaa authentication eap aaa-eap-list
```

The following example shows how to configure the remote access server using the remote EAP authentication method with a local and external EAP server:

```
Router(config)# aaa new-model
Router(config)# aaa authentication login aaa-eap-list default group radius
Router(config)# aaa authentication login aaa-eap-local-list default group tacacs
Router(config)# crypto ikev2 profile profile2
```

```
Router(config-ikev2-profile)# authentication remote eap
Router(config-ikev2-profile)# authentication remote eap-local
Router(config-ikev2-profile)# aaa authentication eap aaa-eap-list
Router(config-ikev2-profile)# aaa authentication eap-local aaa-eap-local-list
```

Related Commands

Command	Description
crypt ikev2 profile	Defines an IKEv2 profile.

aaa authentication (WebVPN)

To configure authentication, authorization, and accounting (AAA) authentication for SSL VPN sessions, use the **aaa authentication** command in webvpn context configuration mode. To remove the AAA configuration from the SSL VPN context configuration, use the **no** form of this command.

aaa authentication {**domain** *name*| **list** *name*}

no aaa authentication {**domain**| **list**}

Syntax Description

domain *name*	Configures authentication using the specified domain name.
list *name*	Configures authentication using the specified list name.

Command Default

If this command is not configured or if the **no** form of this command is entered, the SSL VPN gateway will use global AAA parameters (if configured).

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **aaa authentication**command is entered to specify an authentication list or server group under a SSL VPN context configuration. If this command is not configured and AAA is configured globally on the router, global authentication will be applied to the context configuration.

The database that is configured for remote-user authentication on the SSL VPN gateway can be a local database, or the database can be accessed through any RADIUS or TACACS+ AAA server.

We recommend that you use a separate AAA server, such as a Cisco Access Control Server (ACS). A separate AAA server provides a more robust security solution. It allows you to configure unique passwords for each remote user and accounting and logging for remote-user sessions.

Examples

Examples

The following example configures local AAA for remote-user connections. Notice that the **aaa authentication** command is not configured in a context configuration.

```
Router (config)# aaa new-model
```

```
Router (config)# username USER1 secret 0 PsW2143
Router (config)# aaa authentication login default local
```

Examples

The following example configures a RADIUS server group and associates the AAA configuration under the SSL VPN context configuration.

```
Router (config)# aaa new-model
Router (config)# aaa group server radius myServer
Router (config-sg-radius)# server 10.1.1.20 auth-port 1645 acct-port 1646
Router (config-sg-radius)# exit
Router (config)# aaa authentication login default local group myServer
Router (config)# radius-server host 10.1.1.0 auth-port 1645 acct-port 1646
Router (config)# webvpn context context1
Router (config-webvpn-context)# aaa authentication list myServer
Router (config-webvpn-context)# exit
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

aaa authentication arap

To enable an authentication, authorization, and accounting (AAA) authentication method for AppleTalk Remote Access (ARA), use the **aaa authentication arap** command in global configuration mode. To disable this authentication, use the **no** form of this command.

aaa authentication arap {**default**| *list-name*} *method1* [*method2 ...*]

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

Syntax Description

default	Uses the listed methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string used to name the following list of authentication methods tried when a user logs in.
method1 [*method2...*]	At least one of the keywords described in the table below.

Command Default

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

```
aaa authentication arap default local
```

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server and local-case support were added as method keywords for this command.
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 list names and default that you set with the **aaa authentication arap**command are used with the **arap authentication** command. Note that ARAP guest logins are disabled by default when you enable AAA. To

allow guest logins, you must use either the **guest** or **auth-guest** method listed in the table below. You can only use one of these methods; they are mutually exclusive.

Create a list by entering the **aaa authentication arap** *list-name method*command, where *list-name* is any character string used to name this list (such as *MIS-access*). The *method*argument identifies the list of methods the authentication algorithm tries in the given sequence. See the table below for descriptions of method keywords.

To create a default list that is used if no list is specified in the **arap authentication** command, use the **default** keyword followed by the methods you want to be used in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails.

Use the **more system:running-config**command to view currently configured lists of authentication methods.

Note In the table below, the **group radius**, **group tacacs +**, 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** and **aaa group server tacacs+** commands to create a named group of servers.

Table 1: aaa authentication arap Methods

Keyword	Description
guest	Allows guest logins. This method must be the first method listed, but it can be followed by other methods if it does not succeed.
auth-guest	Allows guest logins only if the user has already logged in to EXEC. This method must be the first method listed, but can be followed by other methods if it does not succeed.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
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.

Examples

The following example creates a list called *MIS-access*, which first tries TACACS+ authentication and then none:

```
aaa authentication arap MIS-access group tacacs+ none
```

The following example creates the same list, but sets it as the default list that is used for all ARA protocol authentications if no other list is specified:

```
aaa authentication arap default group tacacs+ none
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

aaa authentication attempts login

To set the maximum number of login attempts that will be permitted before a session is dropped, use the **aaa authentication attempts login**command in global configuration mode. To reset the number of attempts to the default, use the **no** form of this command.

aaa authentication attempts login *number-of-attempts*

no aaa authentication attempts login

Syntax Description

number-of-attempts	Number of login attempts. Range is from 1 to 25. Default is 3.

Command Default

3 attempts

Command Modes

Global configuration

Command History

Release	Modification
12.2 T	This command was introduced.

Usage Guidelines

The **aaa authentication attempts login** command configures the number of times a router will prompt for username and password before a session is dropped.

The **aaa authentication attempts login** command can be used only if the **aaa new-model** command is configured.

Examples

The following example configures a maximum of 5 attempts at authentication for login:

```
aaa authentication attempts login 5
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

aaa authentication auto (WebVPN)

To allow automatic authentication for Secure Socket Layer virtual private network (SSL VPN) users, use the **aaa authentication auto** command in webvpn context configuration mode. To disable automatic authentication, use the **no** form of this command.

aaa authentication auto

no aaa authentication auto

Syntax Description

This command has no arguments or keywords.

Command Default

Automatic authentication is not allowed.

Command Modes

Webvpn context (config-webvpn-context)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Configuring this command allows users to provide their usernames and passwords via the gateway page URL. They do not have to enter the usernames and passwords again from the login page.

A user can embed his or her username and password in the URL using the following format:

```
http://<gateway-address>/<vw_context>/webvpnauth?username:password
```

Examples

The following example shows that automatic authentication has been configured for users:

```
Router (config)# webvpn context
Router (config-webvpn-context)# aaa authentication auto
```

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.

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. With CSCum15057, the AAA authentication banner message is always printed if the user logs into the system using the Secure Shell (SSH) server.

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 enable default

To enable authentication, authorization, and accounting (AAA) authentication to determine whether a user can access the privileged command level, use the **aaa authentication enable default** command in global configuration mode. To disable this authorization method, use the **no** form of this command.

aaa authentication enable default *method1* [*method2* ...]

no aaa authentication enable default *method1* [*method2* ...]

Syntax Description

method1 [*method2*...]	At least one of the keywords described in the table below.

Command Default

If the **default**list is not set, only the enable password is checked. This has the same effect as the following command:

```
aaa authentication enable default enable
```

On the console, the enable password is used if it exists. If no password is set, the process will succeed anyway.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server support was added as various method keywords for this command.
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 enable default** command to create a series of authentication methods that are used to determine whether a user can access the privileged command level. Method keywords are described in the table below. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.

All **aaa authentication enable default** requests sent by the router to a RADIUS server include the username "$enab15$."

Note An enable authentication request for $enab{x}$ is sent only for RADIUS servers.

If a default authentication routine is not set for a function, the default is **none** and no authentication is performed. Use the **more system:running-config** command to view currently configured lists of authentication methods.

Note In the table below, the **group radius**, **group tacacs +**, 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** and **aaa group server tacacs+** commands to create a named group of servers.

Table 2: aaa authentication enable default Methods

Keyword	Description
enable	Uses the enable password for authentication. **Note** An authentication request fails over to the next authentication method only if no enable password is configured on the router.
line	Uses the line password for authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication. **Note** The RADIUS method does not work on a per-username basis.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
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.

Examples

The following example shows how to create an authentication list that first tries to contact a TACACS+ server. If no server can be found, 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 enable default group tacacs+ enable none
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict network access to a user.

Command	Description
aaa new-model	Enables the AAA access control model.
enable password	Sets a local password to control access to various privilege levels.

aaa authentication eou default enable group radius

To set authentication lists for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), use the **aaa authentication eou default enable group radius**command in global configuration mode. To remove the authentication lists, use the **no** form of this command.

aaa authentication eou default enable group radius

no aaa authentication eou default enable group radius

Syntax Description

This command has no arguments or keywords.

Command Default

Authentication lists for EAPoUDP are not set.

Command Modes

Global 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.

Examples

The following example shows that authentication lists have been set for EAPoUDP:

```
Router (config)# aaa new-model
Router (config)# aaa authentication eou default enable group radius
```

Related Commands

Command	Description
eou	Provides information about EAPoUDP.
ip admission	Creates a Layer 3 network admission control rule to be applied to the 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*} *method1* [*method2* ...]

no aaa authentication login {**default** | *list-name*} *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.
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.
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.

Release	Modification
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 “Authentication Methods That Cannot be used for the list-name Argument” 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 password is prompted only once to authenticate the user credentials and in case of errors due to connectivity issues, multiple retries are possible through the additional methods of authentication. However, the switchover to the next authentication method happens 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 3: 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	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.

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 authentication nasi

To specify authentication, authorization, and accounting (AAA) authentication for Netware Asynchronous Services Interface (NASI) clients connecting through the access server, use the **aaa authentication nasi** command in global configuration mode. To disable authentication for NASI clients, use the **no** form of this command.

aaa authentication nasi {**default**| *list-name*} *method1* [*method2* ...]

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

Syntax Description

default	Makes the listed authentication methods that follow this argument the default list of methods used when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in.
method1 [*method2*...]	At least one of the methods described in the table below.

Command Default

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

```
aaa authentication nasi default local
```

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0(5)T	Group server support and local-case were added as method keywords for this command.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline releases or in Technology-based (T-train) releases. It might continue to appear in 12.2S-family releases.
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 default and optional list names that you create with the **aaa authentication nasi** command are used with the **nasi authentication** command.

Create a list by entering the **aaa authentication nasi** command, where *list-name* is any character string that names the list (such as *MIS-access*). The *method* argument identifies the list of methods the authentication algorithm tries in the given sequence. Method keywords are described in the table below.

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

The remaining 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.

Note In the table below, the **group radius**, **group tacacs +**, 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** and **aaa group server tacacs+** commands to create a named group of servers.

Table 4: aaa authentication nasi Methods

Keyword	Description
enable	Uses the enable password for authentication.
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.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
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.

Examples

The following example creates an AAA authentication list called *list1* . 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 nasi list1 group tacacs+ enable none
```

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

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

Related Commands

Command	Description
ip trigger-authentication (global)	Enables the automated part of double authentication at a device.
ipx nasi-server enable	Enables NASI clients to connect to asynchronous devices attached to a router.
nasi authentication	Enables AAA authentication for NASI clients connecting to a router.
show ipx nasi connections	Displays the status of NASI connections.
show ipx spx-protocol	Displays the status of the SPX protocol stack and related counters.

aaa authentication password-prompt

To change the text displayed when users are prompted for a password, use the **aaa authentication password-prompt** command in global configuration mode. To return to the default password prompt text, use the **no** form of this command.

aaa authentication password-prompt *text-string*

no aaa authentication password-prompt *text-string*

Syntax Description

text-string	String of text that will be displayed when the user is prompted to enter a password. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, “Enter your password:”).

Command Default

There is no user-defined *text-string*, and the password prompt appears as “Password.”

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **aaa authentication password-prompt** command to change the default text that the Cisco IOS software displays when prompting a user to enter a password. This command changes the password prompt for the enable password as well as for login passwords that are not supplied by remote security servers. The **no** form of this command returns the password prompt to the default value:

```
Password:
```

The **aaa authentication password-prompt** command does not change any dialog that is supplied by a remote TACACS+ server.

The aaa authentication password-prompt command works when RADIUS is used as the login method. The password prompt that is defined in the command will be shown even when the RADIUS server is unreachable. The aaa authentication password-prompt command does not work with TACACS+. TACACS+ supplies the

network access server (NAS) with the password prompt to display to the users. If the TACACS+ server is reachable, the NAS gets the password prompt from the server and uses that prompt instead of the one defined in the aaa authentication password-prompt command. If the TACACS+ server is not reachable, the password prompt that is defined in the aaa authentication password-prompt command may be used.

Examples

The following example changes the text for the password prompt:

```
aaa authentication password-prompt “Enter your password now:”
```

Related Commands

Command	Description
aaa authentication username-prompt	Changes the text displayed when users are prompted to enter a username.
aaa new-model	Enables the AAA access control model.
enable password	Sets a local password to control access to various privilege levels.

aaa authentication ppp

To specify one or more authentication, authorization, and accounting (AAA) methods for use on serial interfaces that are running PPP, use the **aaa authentication ppp** command in global configuration mode. To disable authentication, use the **no** form of this command.

aaa authentication ppp {**default**| *list-name*} *method1* [*method2* ...]

no aaa authentication ppp {**default**| *list-name*} *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 tried when a user logs in.
method1 method2...	Identifies 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 methods on serial interfaces running PPP are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server support and **local-case** were added as method keywords.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

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

aaa authentication ppp default local

The lists that you create with the **aaa authentication ppp**command are used with the **ppp authentication** command. These lists contain up to four authentication methods that are used when a user tries to log in to the serial interface.

Create a list by entering the **aaa authentication ppp** *list-name method*command, where *list-name* is any character string used to name this list MIS-access. The *method*argument identifies the list of methods that the authentication algorithm tries in the given sequence. You can enter up to four methods. Method keywords are described in the table below.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to have authentication succeed even if all methods return an error.

If authentication is not specifically set for a function, the default is **none** and no authentication is performed. Use the **more system:running-config** command to display currently configured lists of authentication methods.

Note In the table below, the **group radius**, **group tacacs +**, 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** and **aaa group server tacacs+** commands to create a named group of servers.

Table 5: aaa authentication ppp Methods

Keyword	Description
cache *group-name*	Uses a cache server group for authentication.
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 radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
if-needed	Does not authenticate if the user has already been authenticated on a tty line.
krb5	Uses Kerberos 5 for authentication (can be used only for Password Authentication Protocol [PAP] authentication).
local	Uses the local username database for authentication.

Keyword	Description
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.

Cisco 10000 Series Router

The Cisco 10000 series router supports a maximum of 2,000 AAA method lists. If you configure more than 2,000 AAA method lists, traceback messages appear on the console.

Examples

The following example shows how to create a AAA authentication list calledMIS-access for serial lines that use PPP. This authentication first tries to contact a TACACS+ server. If this action returns an error, the user is allowed access with no authentication.

```
aaa authentication ppp MIS-access group tacacs+ none
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs+	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
more system:running-config	Displays the contents of the currently running configuration file, the configuration for a specific interface, or map class information.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server host	Specifies a RADIUS server host.
tacacs+-server host	Specifies a TACACS host.

aaa authentication sgbp

To specify one or more authentication, authorization, and accounting (AAA) authentication methods for Stack Group Bidding Protocol (SGBP), use the **aaa authentication sgbp** command in global configuration mode. To disable SGBP authentication and return to the default, use the **no** form of this command.

aaa authentication sgbp {**default**| *list-name*} *method1* [*method2 ...*]

no aaa authentication sgbp {**default**| *list-name*} *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 tried when a user logs in.
method1 [*method2...*]	Identifies 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

Command Default

The **aaa authentication ppp default**command. If the **aaa authentication ppp default**command is not enabled, local authentication will be the default functionality.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command introduced.

Usage Guidelines

The lists that you create with the **aaa authentication sgbp** command are used with the **sgbp aaa authentication** command.

Create a list by entering the **aaa authentication sgbp**p *list-name method* command, where the *list-name* argument is any character string used to name this list. The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence. You can enter up to four methods. Method keywords are described in the table below.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to have authentication succeed even if all methods return an error.

Use the **more system:running-config** command to display currently configured lists of authentication methods.

Table 6: aaa authentication sgbp Methods

Keyword	Description
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
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.

Examples

The following example shows how to create a AAA authentication list called SGBP. The user first tries to contact a RADIUS server for authentication. If this action returns an error, the user will try to access the local database.

```
Router(config)# aaa authentication sgbp SGBP group radius local
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
sgbp aaa authentication	Enables a SGBP authentication list.

aaa authentication suppress null-username

To configure Cisco IOS software to prevent an Access Request with a blank username from being sent to the RADIUS server, use the **aaa authentication suppress null-username**command in global configuration mode.

To configure Cisco IOS software to allow an Access Request with a blank username to be sent to the RADIUS server, use the no form of this command:

aaa authentication suppress null-username

no aaa authentication suppress null-username

Syntax Description

Enables the prevention of an Access Request with a blank username from being sent to the RADIUS server.

Command Default

The *command-level defaul* t is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS Release 12.2(33)SRD	This command was introduced.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4

Usage Guidelines

This command ensures that unnecessary RADIUS server interaction is avoided, and RADIUS logs are kept short.

Examples

The following example shows how the **aaa authentication suppress null-username** is configured:

```
enable
configure terminal
aaa new-model
aaa authentication suppress null-username
```

Related Commands

Command	Description
aaa new-model	Enables AAA globally.

aaa authentication username-prompt

To change the text displayed when users are prompted to enter a username, use the **aaa authentication username-prompt** command in global configuration mode. To return to the default username prompt text, use the **no** form of this command.

aaa authentication username-prompt *text-string*

no aaa authentication username-prompt *text-string*

Syntax Description

text-string	String of text that will be displayed when the user is prompted to enter a username. If this text-string contains spaces or unusual characters, it must be enclosed in double-quotes (for example, “Enter your name:”).

Command Default

There is no user-defined *text-string*, and the username prompt appears as “Username.”

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **aaa authentication username-prompt** command to change the default text that the Cisco IOS software displays when prompting a user to enter a username. The **no** form of this command returns the username prompt to the default value:

```
Username:
```

Some protocols (for example, TACACS+) have the ability to override the use of local username prompt information. Using the **aaa authentication username-prompt** command will not change the username prompt text in these instances.

Note The **aaa authentication username-prompt** command does not change any dialog that is supplied by a remote TACACS+ server.

Examples

The following example changes the text for the username prompt:

```
aaa authentication username-prompt “Enter your name here:”
```

Related Commands

Command	Description
aaa authentication password-prompt	Changes the text that is displayed when users are prompted for a password.
aaa new-model	Enables the AAA access control model.
enable password	Sets a local password to control access to various privilege levels.

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 7: 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 authorization (IKEv2 profile)

To specify the authentication, authorization, and accounting (AAA) authorization for a local or external group policy, use the **aaa authorization** command in IKEv2 profile configuration mode. To remove the AAA authorization, use the **no** form of this command.

aaa authorization {**group** [**override**] {**cert**| **eap**| **psk**}| **user** {**cert list**| **eap**{**cached**| **list**}| **psk**{**cached**| **list**}} {*aaa-listname*| [*aaa-username*| [**local**]| **name-mangler** *mangler-name*]| [**password** *password*]}}

no aaa authorization {**group** [**override**] {**cert**| **eap**| **psk**}| **user** {**cert list**| **eap**{**cached**| **list**}| **psk**{**cached**| **list**}} {*aaa-listname*| [*aaa-username*| [**local**]| **name-mangler** *mangler-name*]| [**password** *password*]}}

Syntax Description

group	Specifies the AAA authorization for local or external group policy.
override	(Optional) Overrides user authorization with group authorization. By default, group authorization is overridden with user authorization.
user	Specifies the AAA authorization for each user policy.
cert	Specifies the AAA method list that is used when the remote authentication method is certificate based.
eap	Specifies the AAA method list that is used when the remote authentication method is Extensible Authentication Protocol (EAP).
psk	Specifies the AAA method list that is used when the remote authentication method is preshared key.
list	Specifies the AAA method list for the remote authentication method.
cached	Uses cached attributes from the EAP authentication or AAA preshared key.
aaa-listname	The AAA list name.
aaa-username	The AAA username.
name-mangler *mangler-name*	Derives the name mangler from the **crypto ikev2 name-mangler** command.

password *password*	Specifies the AAA password. This *password* argument defines the following values: • **0**—Specifies that the password is unencrypted. • **6**—Specifies that the password is encrypted. • *password*—Specifies an unencrypted user password.

Command Default

AAA authorization is not specified.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.3(3)M	This command was modified. The **list** keyword and the **password** *password* keyword-argument pair was added

Usage Guidelines

Use this command to specify the AAA authorization for local or external group policy. The **crypto ikev2 profile** command must be enabled before this command is executed.

If no AAA method list is specified, the list is common for all authentication methods. Local AAA is not supported for user authorization.

AAA user policies take precedence over AAA group policies.

The **user** keyword is not required and not recommended when RADIUS is the external AAA server as RADIUS combines authentication and authorization and returns authorization data with successful authentication. The **user** keyword can be used with AAA servers such as TACACS+ where authentication and authorization are decoupled.

If the **cached** keyword is specified, the **name-mangler** *mangler-name* keyword-argument pair cannot be specified.

Use the following variations of the **aaa authorization** command to configure the Internet Key Exchange version 2 (IKEv2) profile for the FlexVPN server:

- To specify the AAA method list and username for user authorization, enter both or one of the following commands:
  - **aaa authorization user** {**eap** | **psk**} {**cached** | **list** *aaa-listname* [*aaa-username* | **name-mangler** *mangler-name*]}
  - **aaa authorization user cert list** *aaa-listname* {*aaa-username* | **name-mangler** *mangler-name*}

- To specify the AAA method list and username for group authorization, enter both or one of the following commands:
  - **aaa authorization group** [**override**] {**eap** | **psk**} **list** *aaa-listname* [*aaa-username* | **name-mangler** *mangler-name*]
  - **aaa authorization group** [**override**] **cert list** *aaa-listname* {*aaa-username* | **name-mangler** *mangler-name*}

You can simultaneously configure all combinations of user and group authorizations for EAP, preshared key, and certificate-based authentication methods. For EAP and preshared key authentication methods, you can simultaneously configure two variants for user authorization with the **cached** and **list** keywords respectively.

Examples

The following example shows how to configure the AAA authorization for a local group policy. The **aaa-group-list** keyword specifies that group authorization is local and the AAA username is abc. The authorization list name corresponds to the group policy defined in the **crypto ikev2 client configuration group** command.

```
Router(config)# aaa new-model
Router(config)# aaa authorization network aaa-group-list default local
Router(config)# crypto ikev2 client configuration group 123
Router(config-ikev2-client-config-group)# pool addr-pool1
Router(config-ikev2-client-config-group)# dns 198.51.100.1 198.51.100.100
Router(config-ikev2-client-config-group)# wins 203.0.113.1 203.0.113.115
Router(config-ikev2-client-config-group)# exit
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# wins 203.0.113.1 203.0.113.115 authentication remote eap
Router(config-ikev2-profile)# aaa authorization group aaa-group-list abc
```

The following example shows how to configure an external AAA-based group policy. The **aaa-group-list** keyword specifies that the group authorization is RADIUS based. The name mangler derives the group name from the domain part of ID-FQDN, which is abc.

```
Router(config)# aaa new-model
Router(config)# aaa authorization network aaa-group-list default group radius
Router(config)# crypto ikev2 name-mangler mangler1
Router(config-ikev2-name-mangler)# fqdn domain
Router(config-ikev2-name-mangler)# exit
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# identity remote fqdn host1.abc
Router(config-ikev2-profile)# authentication remote eap
Router(config-ikev2-profile)# aaa authorization group aaa-group-list name-mangler mangler1
```

The following example shows how to configure an external AAA-based group policy. The **aaa-user-list** specifies that user authorization is RADIUS based. The name mangler derives the username from the hostname part of ID-FQDN, which is host1.

```
Router(config)# aaa new-model
Router(config)# aaa authorization network aaa-user-list default group radius
Router(config)# crypto ikev2 name-mangler mangler2
Router(config-ikev2-name-mangler)# fqdn hostname
Router(config-ikev2-name-mangler)# exit
Router(config-ikev2-profile)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# match identity remote fqdn host1.abc
Router(config-ikev2-profile)# authentication remote eap
Router(config-ikev2-profile)# aaa authorization user aaa-user-list name-mangler mangler2
```

Related Commands

Command	Description
crypto ikev2 name-mangler	Defines a name mangler.
crypto ikev2 profile	Defines an IKEv2 profile.

aaa authorization cache filterserver

To enable authentication, authorization, and accounting (AAA) authorization caches and the downloading of access control list (ACL) configurations from a RADIUS filter server, use the **aaa authorization cache filterserver** command in global configuration mode. To disable AAA authorization caches, use the **no** form of this command.

aaa authorization cache filterserver default *methodlist* [*methodlist2 ...*]

no aaa authorization cache filterserver default

Syntax Description

default	Default authorization list.
methodlist [*methodlist2...*]	One of the keywords listed in the table below.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
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

Use the **aaa authorization cache filterserver** command to enable the RADIUS ACL filter server.

Method keywords are described in the table below.

Table 8: aaa authorization cache filterserver Methods

Keyword	Description
group *group-name*	Uses a subset of RADIUS servers for authentication as defined by the **aaa group server radius** command.
local	Uses the local database for authorization caches and ACL configuration downloading.
none	No authorization is performed.

This command functions similarly to the **aaa authorization**command with the following exceptions:

- Named method-lists cannot be configured.
- Only one instance of this command can be configured.
- TACACS+ groups cannot be configured.

Examples

The following example shows how to configure the default RADIUS server group as the desired filter. If the request is rejected or a reply is not returned, local configuration will be consulted. If the local filter does not respond, the call will be accepted but filtering will not occur.

```
aaa authorization cache filterserver group radius local none
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.

aaa authorization config-commands

To reestablish the default created when the **aaa authorization commands** command was issued, use the aaa authorization config-commands command in global configuration mode. To disable authentication, authorization, and accounting (AAA) configuration command authorization, use the **no** form of this command.

aaa authorization config-commands

no aaa authorization config-commands

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(6.02)T	This command was changed from being enabled by default to being disabled by default.
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

If the **aaa authorization commands** *level method*commandis enabled, all commands, including configuration commands, are authorized by authentication, authorization, and accounting (AAA) using the method specified. Because there are configuration commands that are identical to some EXEC-level commands, there can be some confusion in the authorization process. Using the **no aaa authorization config-commands** command stops the network access server from attempting configuration command authorization.

After the **no** form of this command has been entered, AAA authorization of configuration commands is completely disabled. Care should be taken before entering the **no** form of this command because it potentially reduces the amount of administrative control on configuration commands.

Use the **aaa authorization config-commands**command if, after using the **no** form of this command, you need to reestablish the default set by the **aaa authorization commands** *level method* command.

Note You will get the same result if you (1) do not configure this command, or (2) configure **no aaa authorization config-commands**.

Examples

The following example specifies that TACACS+ authorization is run for level 15 commands and that AAA authorization of configuration commands is disabled:

```
aaa new-model
aaa authorization command 15 group tacacs+ none
no aaa authorization config-commands
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

aaa authorization console

To apply authorization to a console, use the **aaa authorization console** command in global configuration mode. To disable the authorization, use the **no** form of this command.

aaa authorization console

no aaa authorization console

Syntax Description

This command has no arguments or keywords.

Command Default

Authentication, authorization, and accounting (AAA) authorization is disabled on the console.

Command Modes

Global configuration

Command History

Release	Modification
12.0(6)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

If the **aaa new-model** command has been configured to enable the AAA access control model, the **no aaa authorization console**command is the default, and the authorization that is configured on the console line will always succeed. If you do not want the default, you need to configure the **aaa authorization console** command.

Note This command by itself does not turn on authorization of the console line. It needs to be used in conjunction with the **authorization** command under console line configurations.

If you are trying to enable authorization and the **no aaa authorization console** command is configured by default, you will see the following message:

```
%Authorization without the global command aaa authorization console
 is useless.
```

Examples

The following example shows that the default authorization that is configured on the console line is being disabled:

```
Router (config)# aaa authorization console
```

Related Commands

Command	Description
authorization	Enables AAA authorization for a specific line or group of lines.

aaa authorization list

To allow user attributes to get "pushed" during authentication, use the **aaa authorization list** command in webvpn context configuration mode. To disable the pushing of attributes, use the **no** form of this command.

aaa authorization list

no aaa authorization list

Syntax Description

name	Name of the list to be automatically authorized.

Command Default

User attributes are not pushed during authentication.

Command Modes

Webvpn context (config-webvpn-context)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

If this command is configured, a separate authorization step is no longer needed after authentication.

Examples

The following example shows that authorization is to be pushed during authentication for List 11:

```
Router (config)# webvpn context
Router (config-webvpn-context)# aaa authorization list 11
```

Related Commands

Command	Description
aaa authentication auto (WebVPN)	Allows automatic authentication for SSL VPN users.

aaa authorization reverse-access

To configure a network access server to request authorization information from a security server before allowing a user to establish a reverse Telnet session, use the **aaa authorization reverse-access**command in global configuration mode. To restore the default value for this command, use the **no** form of this command.

aaa authorization reverse-access {**group radius**| **group tacacs**+}

no aaa authorization reverse-access {**group radius**| **group tacacs**+}

Syntax Description

group radius	Specifies that the network access server will request authorization from a RADIUS security server before allowing a user to establish a reverse Telnet session.
group tacacs+	Specifies that the network access server will request authorization from a TACACS+ security server before allowing a user to establish a reverse Telnet session.

Command Default

This command is disabled by default, meaning that authorization for reverse Telnet is not requested.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(5)T	Group server support was added as various method keywords for this command.
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

Telnet is a standard terminal emulation protocol used for remote terminal connection. Normally, you log in to a network access server (typically through a dialup connection) and then use Telnet to access other network devices from that network access server. There are times, however, when it is necessary to establish a reverse Telnet session. In reverse Telnet sessions, the Telnet connection is established in the opposite direction--from inside a network to a network access server on the network periphery to gain access to modems or other devices connected to that network access server. Reverse Telnet is used to provide users with dialout capability by allowing them to open Telnet sessions to modem ports attached to a network access server.

It is important to control access to ports accessible through reverse Telnet. Failure to do so could, for example, allow unauthorized users free access to modems where they can trap and divert incoming calls or make outgoing calls to unauthorized destinations.

Authentication during reverse Telnet is performed through the standard AAA login procedure for Telnet. Typically the user has to provide a username and password to establish either a Telnet or reverse Telnet session. This command provides an additional (optional) level of security by requiring authorization in addition to authentication. When this command is enabled, reverse Telnet authorization can use RADIUS or TACACS+ to authorize whether or not this user is allowed reverse Telnet access to specific asynchronous ports, after the user successfully authenticates through the standard Telnet login procedure.

Examples

The following example causes the network access server to request authorization information from a TACACS+ security server before allowing a user to establish a reverse Telnet session:

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization reverse-access default group tacacs+
!
tacacs-server host 172.31.255.0
tacacs-server timeout 90
tacacs-server key goaway
```

The lines in this sample TACACS+ reverse Telnet authorization configuration are defined as follows:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default group tacacs+** command specifies TACACS+ as the default method for user authentication during login.
- The **aaa authorization reverse-access default group tacacs +** command specifies TACACS+ as the method for user authorization when trying to establish a reverse Telnet session.
- The **tacacs-server host**command identifies the TACACS+ server.
- The **tacacs-server timeout** command sets the interval of time that the network access server waits for the TACACS+ server to reply.
- The **tacacs-server key** command defines the encryption key used for all TACACS+ communications between the network access server and the TACACS+ daemon.

The following example configures a generic TACACS+ server to grant a user, “jim,” reverse Telnet access to port tty2 on the network access server named “site1” and to port tty5 on the network access server named site2:

```
user = jim
  login = cleartext lab
  service = raccess {
    port#1 = site1/tty2
    port#2 = site2/tty5
}
```

Note In this example, “site1” and “site2” are the configured host names of network access servers, not DNS names or alias.

The following example configures the TACACS+ server (CiscoSecure) to authorize a user named Jim for reverse Telnet:

```
user = jim
 profile_id = 90
 profile_cycle = 1
 member = Tacacs_Users
 service=shell {
 default cmd=permit
 }
 service=raccess {
 allow “c2511e0” “tty1” “.*”
 refuse “.*” “.*” “.*”
 password = clear “goaway”
```

Note CiscoSecure only supports reverse Telnet using the command line interface in versions 2.1(*x*) through version 2.2(1).

An empty “service=raccess {}” clause permits a user to have unconditional access to network access server ports for reverse Telnet. If no “service=raccess” clause exists, the user is denied access to any port for reverse Telnet.

For more information about configuring TACACS+, refer to the chapter “Configuring TACACS+” in the *CiscoIOS Security Configuration Guide* . For more information about configuring CiscoSecure, refer to the *CiscoSecure Access Control Server User Guide* , version 2.1(2) or later.

The following example causes the network access server to request authorization from a RADIUS security server before allowing a user to establish a reverse Telnet session:

```
aaa new-model
aaa authentication login default group radius
aaa authorization reverse-access default group radius
!
radius-server host 172.31.255.0
radius-server key goaway
```

The lines in this sample RADIUS reverse Telnet authorization configuration are defined as follows:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default group radius** command specifies RADIUS as the default method for user authentication during login.
- The **aaa authorization reverse-access default group radius** command specifies RADIUS as the method for user authorization when trying to establish a reverse Telnet session.
- The **radius-server host** command identifies the RADIUS server.
- The **radius-server key**command defines the encryption key used for all RADIUS communications between the network access server and the RADIUS daemon.

The following example configures the RADIUS server to grant a user named “jim” reverse Telnet access at port tty2 on network access server site1:

```
Password = “goaway”
User-Service-Type = Shell-User
cisco-avpair = “raccess:port#1=site1/tty2”
```

The syntax "raccess:port=any/any" permits a user to have unconditional access to network access server ports for reverse Telnet. If no "raccess:port={*nasname* }/{*tty number* }" clause exists in the user profile, the user is denied access to reverse Telnet on all ports.

For more information about configuring RADIUS, refer to the chapter "Configuring RADIUS" in the *CiscoIOS Security Configuration Guide* .

aaa authorization template

To enable usage of a local or remote customer template on the basis of Virtual Private Network (VPN) routing and forwarding (VRF), use the **aaa authorization template** command in global configuration mode. To disable the new authorization, use the **no** form of this command.

aaa authorization template

no aaa authorization template

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Examples

The following example enables usage of a remote customer template:

```
aaa authorization template
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.

Command	Description
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
tacacs-server host	Specifies a TACACS+ server host.
template	Accesses the template configuration mode for configuring a particular customer profile template.

aaa cache filter

To enable filter cache configuration, use the **aaa cache filter**command in global configuration mode. To disable this functionality, use the **no** form of this command.

aaa cache filter

no aaa cache filter

Syntax Description

This command has no arguments or keywords.

Command Default

Filter cache configuration is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
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

Use the **aaa cache filter**command to begin filter cache configuration and enter AAA filter configuration mode (config-aaa-filter).

After enabling this command, you can specify filter cache parameters with the following commands:

- **cache clear age** -- Specifies, in minutes, when cache entries expire and the cache is cleared.
- **cache disable** --Disables the cache.
- **cache max** --Refreshes a cache entry when a new sessions begins.
- **cache refresh** --Limits the absolute number of entries the cache can maintain for a particular server.
- **password** --Specifies the optional password that is to be used for filter server authentication requests.

Note Each of these commands is optional; thus, the default value will be enabled for any command that is not specified.

Examples

The following example shows how to enable filter cache configuration and specify cache parameters.

```
aaa cache filter
 password mycisco
 no cache refresh
 cache max 100
```

Related Commands

Command	Description
aaa authorization cache filterserver	Enables AAA authorization caches and the downloading of ACL configurations from a RADIUS filter server.
cache clear age	Specifies when, in minutes, cache entries expire and the cache is cleared.
cache disable	Disables the cache.
cache max	Refreshes a cache entry when a new sessions begins.
cache refresh	Limits the absolute number of entries the cache can maintain for a particular server.
password	Specifies the optional password that is to be used for filter server authentication requests.

aaa cache filterserver

To enable Authentication, Authorization, and Accounting (AAA) filter server definitions, use the **aaa cache filterserver** command in global configuration mode. To disable AAA filter server definitions, use the **no** form of this command.

aaa cache filterserver

no aaa cache filterserver

Syntax Description

This command has no arguments or keywords.

Command Default

This command is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

The **aaa cache filterserver** command is mainly used to define AAA cache filter server requirements for downloading access control lists (ACLs) commands but is also used for cache configurations, domain names, and passwords. To use this command, enable the **aaa authorization cache filterserver** command first.

Examples

The following example enables the **aaa cache filterserver** command:

```
Router> enable
Router# configure terminal
Router(config)# aaa new-model
Router (config)# aaa authorization cache filterserver default group radius
Router(config)# aaa cache filterserver
Router(config-filter)# cache max 100
Router(config-filter)# no cache refresh
```

Related Commands

Command	Description
show aaa cache filterserver	Displays the aaa cache filterserver status.

aaa cache profile

To create a named authentication and authorization cache profile group and enter profile map configuration mode, use the **aaa cache profile** command in global configuration mode. To disable a cache profile group, use the **no** form of this command.

aaa cache profile *group-name*

no aaa cache profile *group-name*

Syntax Description

group-name	Text string that specifies an authentication and authorization group. Group names cannot be duplicated.

Command Default

No cache profile groups are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use this command to define or modify an authentication or authorization cache group and to specify cache profile parameters using the following commands:

- **all** --Specifies that all authentication and authorization requests are cached. Using the **all** command makes sense for certain service authorization requests, but it should be avoided when dealing with authentication requests.
- **profile** --Specifies an exact profile match to cache. The profile name must be an exact match to the username being queried by the service authentication or authorization request. This is the recommended format to enter profiles that users want to cache.
- **regexp** --Allows entries to match based on regular expressions. Matching on regular expressions is not recommended for most situations.

The **any** keyword, which is available under the **regexp** submenu, allows any unique instance of a AAA server response that matches the regular expression to be saved in the cache. The **only** keyword allows for only one instance of a AAA server response that matches the regular expression to be saved in the cache.

Entering the **no** form of this command deletes the profile definition and all of its command definitions.

Examples

The following example creates the AAA cache profile group localusers:

```
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa cache profile localusers
```

Related Commands

Command	Description
all	Specifies that all authentication and authorization requests be cached.
profile	Defines or modifies an individual authentication and authorization cache profile.
regexp	Creates an entry in a cache profile group that allows authentication and authorization matches based on a regular expression.

aaa common-criteria policy

To configure authentication, authorization, and accounting (AAA) common criteria security policies, use the **aaa common-criteria policy** command in global configuration mode. To disable AAA common criteria policies, use the **no** form of this command.

aaa common-criteria policy *policy-name*

no aaa common-criteria policy *policy-name*

Syntax Description

policy-name	Name of the AAA common criteria security policy.

Command Default

The common criteria security policy is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(2)SE	This command was introduced.

Usage Guidelines

Use the **aaa common-criteria policy** command to enter the common criteria configuration policy mode. To check the available options in this mode, type **?** after entering into common criteria configuration policy mode (config-cc-policy).

The following options are available:

- **char-change—**Number of changed characters between old and new passwords. The range is from 1 to 64.
- **copy—**Copy the common criteria policy parameters from an existing policy.
- **exit—**Exit from common criteria configuration mode.
- **lifetime—**Configure the maximum lifetime of a password by providing the configurable value in years, months, days, hours, minutes, and seconds. If the lifetime parameter is not configured, the password will never expire.
- **lower-case—**Number of lowercase characters. The range is from 0 to 64.
- **upper-case—**Number of uppercase characters. The range is from 0 to 64.
- **min-length—**Minimum length of the password. The range is from 1 to 64.
- **max-length—**Maximum length of the password. The range is from 1 to 64.
- **numeric-count—**Number of numeric characters. The range is from 0 to 64.

- **special-case—**Number of special characters. The range is from 0 to 64.

Examples

The following example shows how to create a common criteria security policy:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa common-criteria policy policy1
Device(config-cc-policy)# end
```

Related Commands

Command	Description
aaa new-model	Enables AAA access control model.
debug aaa common-criteria	Enables debugging for AAA common criteria password security policies.
show aaa common-criteria policy	Displays common criteria security policy details.

aaa configuration

To configure the username and password that are to be used when downloading configuration requests, an IP pool, or static routes through RADIUS, use the **aaa configuration** command in global configuration mode. To disable this configuration, use the **no** form of this command.

aaa configuration {**config-username username** *username* [**password** [**0** | **7**] *password*] | {**pool** | **route**} **username** *username* [**password** [**0** | **6** | **7**] *password*]}

no aaa configuration {**config-username username** *username* [**password** [**0** | **7**] *password*] | {**pool** | **route**} **username** *username* [**password** [**0** | **6** | **7**] *password*]}

Syntax Description

config-username	Configures the username and password used in configuration requests that can be downloaded.
username *username*	Defines a username to be used instead of the device's hostname.
password	Specifies the RADIUS server password.
0	(Optional) Specifies the unencrypted (cleartext) shared password. **Note** Type 0 passwords are automatically converted to type 7 passwords by enabling the **service password-encryption** command.
6	(Optional) Specifies a password encrypted with a reversible, symmetric, advanced encryption scheme (AES) encryption algorithm. **Note** Type 6 AES encrypted passwords are configured using the **password encryption aes** command.
7	(Optional) Specifies a password encrypted using a Cisco-defined encryption algorithm.
password	The alphanumeric password to be used instead of the default "cisco."
pool	Configures the username and password used for downloading an IP pool. IP pools are used to define the range of IP addresses that are used for Dynamic Host Configuration Protocol (DHCP) servers and point-to-point servers.
route	Configures the username and password used when downloading static routes through RADIUS.

Command Default The hostname of the router and the password “cisco” are used during the static route configuration download.

Command Modes Global configuration (config)

Command History

Release	Modification
12.2(11)T	This command was introduced.
15.4(1)T	This command was modified. The **6** keyword was added.

Usage Guidelines The **aaa configuration** command allows you to specify a username other than the router’s hostname and a stronger password than the default “cisco.”

You can use the **service password-encryption** command to automatically convert type 0 passwords to type 7 passwords.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

Examples The following example shows how to specify the username “MyUsername” and the password “MyPass” when downloading a static route configuration:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius rad1
Device(config-sg-radius)# server 10.1.1.1
Device(config-sg-radius)# exit
Device(config)# aaa authorization configuration default group radius
Device(config)# aaa authorization configuration foo group rad1
Device(config)# aaa route download 1 authorization foo
Device(config)# aaa configuration route username MyUsername password 0 MyPass
Device(config)# radius-server host 10.2.2.2
Device(config)# radius-server key 0 RadKey
```

Related Commands

Command	Description
aaa route download	Enables the static route download feature and sets the amount of time between downloads.
password encryption aes	Enables a type 6 encrypted preshared key.
service password-encryption	Automatically converts unencrypted passwords to encrypted passwords.

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 9: 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 dnis map authorization network group

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

aaa dnis map *dnis-number* **authorization network group** *server-group-name*

no aaa dnis map *dnis-number* **authorization network group** *server-group-name*

Syntax Description

dnis-number	Number of the DNIS.
server-group-name	Character string used to name a group of security servers functioning within a server group.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)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

This command lets you assign a DNIS number to a particular AAA server group so that the server group can process authorization requests for users dialing in to the network using that particular DNIS number. To use this 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 will use RADIUS server 172.30.0.0 for authorization requests for users dialing in with DNIS 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 authorization network group group1
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
aaa dnis map accounting network group	Maps a DNIS number to a AAA server group used for accounting services.
aaa dnis map authentication ppp group	Maps a DNIS number to a AAA server used for authentication services.
aaa dnis map enable	Enables AAA server selection based on DNIS number.
aaa group server	Groups different server hosts into distinct lists and methods.
radius-server host	Specifies and defines the IP address of the RADIUS server host.

aaa group server diameter

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

aaa group server diameter *group-name*

no aaa group server diameter *group-name*

Syntax Description

group-name	Character string used to name the group of servers.

Command Default

None

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **aaa group server**diameter command introduces a way to group existing server hosts. This command 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 Diameter server hosts, 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.

Examples

The following example shows the configuration of a Diameter server group named dia_group_1 that comprises two member servers configured as Diameter peers:

```
aaa group server diameter dia_group_1
 server dia_peer_1
 server dia_peer_2
```

Note If a peer port is not specified, the default value for the peer port is 3868.

Related Commands

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

aaa group server ldap

To group different Lightweight Directory Access Protocol (LDAP) servers into distinct lists and distinct methods, use the **aaa group server ldap**command in global configuration mode. To remove a group server from the configuration list, enter the **no** form of this command.

aaa group server ldap *group-name*

no aaa group server ldap *group-name*

Syntax Description

group-name	Name of the server groups.

Command Default

No LDAP servers are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

The **aaa group server ldap** command enables you to group existing servers. This command allows you to select a subset of the configured server and use them for a particular service.

A group server is a list of servers of a particular type. 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.

Note LDAP authentication is not supported for interactive (terminal) sessions.

Examples

The following example shows how to configure an LDAP server group named ldp_group_1:

```
Router> enable
Router(config)# aaa group server ldp_group_1
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.
aaa authorization	Sets parameters that restrict user access to a network.

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

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 10: 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 11: 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 intercept

To enable lawful intercept on a router, use the **aaa intercept**command in global configuration mode. To disable lawful intercept, use the **no** form of this command.

aaa intercept

no aaa intercept

Syntax Description

This command has no arguments or keywords.

Command Default

Lawful intercept is not enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **aaa intercept** command to enable a RADIUS-Based Lawful Intercept solution on your router. Intercept requests are sent (via Access-Accept packets or CoA-Request packets) to the network access server (NAS) or the Layer 2 Tunnel Protocol (L2TP) access concentrator (LAC) from the RADIUS server. All data traffic going to or from a PPP or L2TP session is passed to a mediation device.

Configure this command with high administrative security so that unauthoried people cannot remove the command.

Examples

The following example shows the configuration of a RADIUS-Based Lawful Intercept solution on a router acting as NAS device employing a PPP over Ethernet (PPPoEo) link:

```
aaa new-model
!
aaa intercept
!
aaa group server radius SG
server 10.0.56.17 auth-port 1645 acct-port 1646
!
aaa authentication login LOGIN group SG
aaa authentication ppp default group SG
aaa authorization network default group SG
aaa accounting send stop-record authentication failure
aaa accounting network default start-stop group SG
!
aaa server radius dynamic-author
client 10.0.56.17 server-key cisco
!
```

```
vpdn enable
!
bba-group pppoe PPPoE-TERMINATE
virtual-template 1
!
interface Loopback0
ip address 10.1.1.2 255.255.255.0
!
interface FastEthernet4/1/0
description To RADIUS server
ip address 10.0.56.20 255.255.255.0
duplex auto
!
interface FastEthernet4/1/2
description To network
ip address 10.1.1.1 255.255.255.0
duplex auto
!
interface FastEthernet5/0/0
description To subscriber
no ip address
!
interface FastEthernet5/0/0.1 point-to-point
pvc 10/808
protocol pppoe group PPPoE-TERMINATE
!
interface Virtual-Template1
ip unnumbered Loopback0
ppp authentication chap
!
radius-server attribute 44 include-in-access-req
radius-server attribute nas-port format d
radius-server host 10.0.56.17 auth-port 1645 acct-port 1646
radius-server key cisco
```

aaa local authentication attempts max-fail

To specify the maximum number of unsuccessful authentication attempts before a user is locked out, use the **aaa local authentication attempts max-fail**command in global configuration mode. To remove the setting for the number of unsuccessful attempts, use the **no** form of this command.

aaa local authentication attempts max-fail *number-of-unsuccessful-attempts*

no aaa local authentication attempts max-fail *number-of-unsuccessful-attempts*

Syntax Description

number-of-unsuccessful-attempts	Number of unsuccessful authentication attempts.

Command Default

The Login Password Retry Lockout feature is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

A system message is generated when a user is either locked by the system or unlocked by the system administrator:

```
%AAA-5-USER_LOCKED: User user1 locked out on authentication failure.
```

An administrator cannot be locked out.

Note No messages are displayed to users after authentication failures that are due to the locked status (that is, there is no distinction between a normal authentication failure and an authentication failure due to the locked status of the user).

Note Unconfiguring this command will maintain the status of the user with respect to locked-out or number-of-failed attempts. To clear the existing locked-out or number-of-failed attempts, the system administrator has to explicitly clear the status of the user using **clear** commands.

Examples

The following **example** illustrates that the maximum number of unsuccessful authentication attempts before a user is locked out has been set for 2:

```
username sysadmin
username sysad privilege 15 password 0 cisco
username user1 password 0 cisco
aaa new-model
aaa local authentication attempts max-fail 2
!
!
aaa authentication login default local
aaa dnis map enable
aaa session-id common
ip subnet-zero
```

Related Commands

Command	Description
clear aaa local user fail-attempts	Clears the unsuccessful login attempts of the user.
clear aaa local user lockout	Unlocks the locked-out user.
show aaa local user locked	Displays a list of all locked-out users.