A through Z

aaa accounting identity

To enable accounting and to create an accounting method list for Session Aware Networking subscriber services, use the **aaa accounting identity** command in global configuration mode. To disable accounting for Session Aware Networking, use the **no** form of this command.

aaa accounting identity {*method-list-name*| **default**} **start-stop [broadcast] group** {*server-group-name*| **radius**| **tacacs+**} [**group**{*server-group-name*| **radius**| **tacacs+**}]

no aaa accounting identity {*method-list-name*| **default**}

Syntax Description

method-list-name	Name of the method list for which to create accounting services by specifying the accounting methods that follow this name.
default	Creates a default method list for accounting services using the accounting methods that follow this keyword.
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.
broadcast	(Optional) Sends accounting records to multiple authentication, authorization, and accounting (AAA) servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, the device uses the backup servers defined within that group.
group	Specifies one or more server groups to use for accounting services. Server groups are applied in the specified order.
server-group-name	Named subset of RADIUS or TACACS+ servers as defined by the **aaa group server radius** command or **aaa group server tacacs+** command.
radius	Uses the list of all RADIUS servers configured with the **radius-server host** command.
tacacs+	Uses the list of all TACACS+ servers configured with the **tacacs-server host** command.

Command Default Accounting is disabled.

Command Modes Global configuration (config)

Command History

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

Usage Guidelines The **aaa accounting identity** command enables accounting services and creates method lists that define specific accounting methods for Session Aware Networking subscriber services. A method list identifies the list of security servers to which the network access server sends accounting records.

Cisco IOS software supports the following two methods of accounting for Session Aware Networking:

- RADIUS—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- TACACS+—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

The default method list is automatically applied to all subscriber sessions except those that have a named method list explicitly defined. A named method list overrides the default method list.

When AAA accounting is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server.

You must enable AAA with the **aaa new-model** command before you can enter the **aaa accounting identity** command.

Examples The following example shows how to configure a default accounting method list where accounting services are provided by a TACACS+ server.

```
aaa new-model
aaa accounting identity default start-stop group tacacs+
```

The following example shows how to configure a named accounting method list, where accounting services are provided by a RADIUS server.

```
aaa new model
aaa accounting identity LIST_1 start-stop group radius
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists.
aaa group server tacacs+	Groups different TACACS+ server hosts into distinct lists.
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 local authentication

To specify the method lists to use for local authentication and authorization from a Lightweight Directory Access Protocol (LDAP) server, use the **aaa local authentication** command in global configuration mode. To return to the default value, use the **no** form of this command.

aaa local authentication {*method-list-name*| **default**} **authorization** {*method-list-name*| **default**}

no aaa local authentication {*method-list-name*| **default**} **authorization** {*method-list-name*| **default**}

Syntax Description

method-list-name	Name of the AAA method list.
default	Uses the default AAA method list.

Command Default

Local LDAP-based authentication is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(1)S	This command was introduced.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use the **aaa local authentication** command to retrieve Extensible Authentication Protocol (EAP) credentials from local or remote LDAP servers.

Examples

The following example shows how to configure local authentication to use the method list named EAP_LIST:

```
aaa new-model
aaa local authentication EAP_LIST authorization EAP_LIST
```

Related Commands

aaa new-model	Enables the AAA access control model.
ldap server	Defines an LDAP server.

access-session closed

To prevent preauthentication access on a port, use the **access-session closed** command in interface configuration mode. To return to the default value, use the **no** form of this command.

access-session closed

no access-session closed

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled (access is open on the port).

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The **access-session closed** command closes access to a port, preventing clients or devices from gaining network access before authentication is performed.

Examples

The following example shows how to set port 1/0/2 to closed access.

```
interface GigabitEthernet 1/0/2
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 access-session control-direction in
```

Related Commands

access-session control-direction	Sets the direction of authentication control on a port.
access-session host-mode	Allows hosts to gain access to a controlled port.
access-session port-control	Sets the authorization state of a port.

access-session control-direction

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

access-session control-direction {**both**| **in**}

no access-session control-direction

Syntax Description

both	Enables bidirectional control on the port. This is the default value.
in	Enables unidirectional control on the port.

Command Default

The port is set to bidirectional mode.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **access-session control-direction** command to set the port control to either unidirectional or bidirectional.

The **in** keyword configures a port as unidirectional, allowing a device on the network to "wake up" the client and force it to reauthenticate. The port can send packets to the host but cannot receive packets from the host.

The **both** keyword configures a port as bidirectional so that access to the port is controlled in both directions. The port cannot send or receive packets.

You can use the **show access-session interface** command to verify the port setting.

Examples

The following example shows how to enable unidirectional control on port 1/0/2:

```
interface GigabitEthernet 1/0/2
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 access-session control-direction in
```

Related Commands

access-session closed	Prevents preauthentication access on a port.
access-session host-mode	Allows hosts to gain access to a controlled port.

access-session port-control	Sets the authorization state of a port.
show access-session	Displays information about authentication sessions.

access-session host-mode

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

access-session host-mode {**multi-auth**| **multi-domain**| **multi-host**| **single-host**}

no access-session host-mode

Syntax Description

multi-auth	Specifies that multiple clients can be authenticated on the port at any given time. This is the default value.
multi-domain	Specifies that only one client per domain (DATA or VOICE) can be authenticated at a time.
multi-host	Specifies that after the first client is authenticated all subsequent clients are allowed access.
single-host	Specifies that only one client can be authenticated on a port at any given time. A security violation occurs if more than one client is detected.

Command Default

Access to a port is multi-auth.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Before you use this command, you must enable the **access-session port-control auto** command.

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

You can use the **show access-session interface** command to verify the port setting.

Examples

The following example shows how to authenticate a single client at a time on port 1/0/2:

```
interface GigabitEthernet 1/0/2
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 access-session control-direction in
```

Related Commands

access-session closed	Prevents preauthentication access on a port.
access-session control-direction	Sets the direction of authentication control on a port.
access-session port-control	Sets the authorization state of a port.
show access-session	Displays information about authentication sessions.

access-session port-control

To set the authorization state of a port, use the **access-session port-control** command in interface configuration mode. To return to the default value, use the **no** form of this command.

access-session port-control {**auto**| **force-authorized**| **force-unauthorized**}

no access-session port-control

Syntax Description

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

Command Default

The port is set to the force-authorized state.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

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

Examples

The following example shows how to set the authorization state on port 1/0/2 to automatic:

```
interface GigabitEthernet 1/0/2
 access-session host-mode single-host
 access-session closed
 access-session port-control auto
 access-session control-direction in
```

Related Commands

access-session closed	Prevents preauthentication access on a port.
access-session host-mode	Allows hosts to gain access to a controlled port.
access-session port-control	Sets the authorization state of a port.

access-session tunnel vlan

To configure an access session for a VLAN tunnel, use the **access-session tunnel vlan** command in global configuration mode. To remove the access session, use the **no** form of this command.

access-session tunnel vlan *vlan-id*

no access-session tunnel vlan [*vlan-id*]

Syntax Description

vlan-id	Specifies the tunnel VLAN ID. The range is from 1 to 4096.

Command Default

Access to VLAN tunnel is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.3SE	This command was introduced.

Usage Guidelines

Before you use this command, you must configure a VLAN using the **vlan** command.

You can use the **show access-session** command to verify access session settings.

Note If a wired guest access is not being configured, VLAN ID of 325 is used as default.

Examples

The following example shows how to configure access to tunnel a VLAN :

```
Device# configure terminal
Device(config)# vlan 1755
Device(config-vlan)# exit
Device(config)# access-session vlan 1755
```

Related Commands

show access-session	Displays information about access sessions.
vlan (service template)	Assigns a VLAN to subscriber sessions.

debug ip admission

To display web authentication debugging information, use the **debug ip admission** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

Cisco IOS XE Release 3SE and Later Releases

debug ip admission {**aaa**| **acl**| **all**| **dos**| **eapoudp**| **error**| **ha**| **httpd**| **idle**| **input-feature**| **io**| **page**| **qualify**| **session**| **sm**| **state**| **timer**}

no debug ip admission {**aaa**| **acl**| **all**| **dos**| **eapoudp**| **error**| **ha**| **httpd**| **idle**| **input-feature**| **io**| **page**| **qualify**| **session**| **sm**| **state**| **timer**}

All Other Releases

debug ip admission {**api**| **consent**| **detailed**| **dos**| **eapoudp**| **error**| **ezvpn**| **fallback**| **function-trace**| **httpd**| **object-creation**| **object-deletion**| **timers**}

no debug ip admission {**api**| **consent**| **detailed**| **dos**| **eapoudp**| **error**| **ezvpn**| **fallback**| **function-trace**| **httpd**| **object-creation**| **object-deletion**| **timers**}

Syntax Description

aaa	Displays IP admission authentication, authorization, and accounting (AAA) events.
acl	Displays IP admission access control list (ACL) events.
all	Displays all IP admission debugging information.
dos	Displays authentication proxy DOS prevention events.
eapoudp	Displays information about Extensible Authentication Protocol over User Datagram Protocol (UDP) (EAPoUDP) network admission control events.
error	Displays web authentication error messages.
ha	Displays high availability (HA) events.
httpd	Displays web authentication HTTP Daemon information.
idle	Displays Layer 3 (L3) idle timer events.
input-feature	Displays IP admission input-feature events.
io	Displays IP admission HTTP proxy daemon input/output events.
page	Displays IP admission HTTP page events.

qualify	Displays IP admission packet qualification.
session	Displays IP admission session events.
sm	Displays IP admission session manager events.
state	Displays IP admission state transitions.
timers	Displays authentication proxy timer-related events.
api	Displays IP Admission API events.
consent	Displays web authentication consent page information.
detailed	Displays details of the TCP events during an authentication proxy process. The details are generic to all FTP, HTTP, and Telnet protocols.
ezvpn	Displays authentication proxy Easy VPN (EzVPN)-related events
fallback	Displays IP admission fallback events.
function-trace	Displays the authentication proxy functions.
object-creation	Displays additional entries to the authentication proxy cache.
object-deletion	Displays deletion of cache entries for the authentication proxy.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC (#)

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.
Cisco IOS XE Release 3.2SE	This command was modified. The **aaa**, **acl**, **all**, **dos**, **ha**, **idle**, **input-feature**, **io**, **page**, **qualify**, **session**, **sm**, and **state** keywords were added.

Usage Guidelines

Use the **debug ip admission** command to troubleshoot web authentication.

Examples

The following is sample output from the **debug ip admission eapoudp** command:

```
Device# debug ip admission eapoudp

Posture validation session created for client mac= 0001.027c.f364 ip= 10.0.0.1
Total Posture sessions= 1 Total Posture Init sessions= 1
*Apr  9 19:39:45.684: %AP-6-POSTURE_START_VALIDATION: IP=10.0.0.1|
Interface=FastEthernet0/0.420
*Apr  9 19:40:42.292: %AP-6-POSTURE_STATE_CHANGE: IP=10.0.0.1| STATE=POSTURE ESTAB
*Apr  9 19:40:42.292: auth_proxy_posture_parse_aaa_attributes:
CiscoDefined-ACL name= #ACSACL#-IP-HealthyACL-40921e54
Apr  9 19:40:42.957: %AP-6-POSTURE_POLICY: Apply access control list
(xACSACLx-IP-HealthyACL-40921e54) policy for host (10.0.0.1)
```

Related Commands

debug access-session	Displays debugging information about Session Aware Networking sessions.
show ip admission	Displays the network admission control (NAC) cache entries or the NAC configuration.

guest-lan

To configure the wireless guest LAN, use the **guest-lan** command in global configuration mode. To remove the wireless guest LAN configuration, use the **no** form of this command.

guest-lan *profile-name* [*lan-id*]

no guest-lan *profile-name* [*lan-id*]

Syntax Description

profile-name	Specifies the wireless guest profile name.
lan-id	(Optional) Specifies the guest LAN identifier. The range is from 1 to 5.

Command Default

The wireless guest LAN is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.3SE	This command was introduced.

Usage Guidelines

Use the **guest-lan** command to specify a wireless guest profile. This wireless guest profile is used in the **tunnel type capwap** command to configure a a CAPWAP tunnel within a service template and configure wired guest access for guest users of an enterprise network.

Examples

The following example shows how to configure access to tunnel a VLAN :

```
Device# configure terminal
Device(config)# guest-lan guest-lan-name 1
```

Related Commands

tunnel type capwap	Configures a CAPWAP tunnel in a service template.

key-wrap enable

To enable Advanced Encryption Standard (AES) key wrap on a RADIUS server, use the **key-wrap enable** command in server group configuration mode. To disable key wrap, use the **no** form of this command.

key-wrap enable

no key-wrap enable

Syntax Description

This command has no arguments or keywords.

Command Default

The key wrap feature is disabled.

Command Modes

Server group configuration (config-sg-radius)

Command History

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

Usage Guidelines

Use the **key-wrap enable** command to enable AES key-wrap functionality. The AES key-wrap feature makes the shared secret between the controller and the RADIUS server more secure. AES key wrap is designed for Federal Information Processing Standards (FIPS) customers and requires a key-wrap compliant RADIUS authentication server.

Examples

The following example shows how to configure a RADIUS server group named LAB_RAD with key-wrap support enabled:

```
aaa group server radius LAB_RAD
 key-wrap enable
 subscriber mac-filtering security-mode mac
 mac-delimiter colon
```

Related Commands

Command	Description
mac-delimiter	Specifies the MAC delimiter for RADIUS compatibility mode.
radius-server host	Specifies a RADIUS server host.
subscriber mac-filtering security-mode	Specifies the RADIUS compatibility mode for MAC filtering.

linksec policy (service template)

To set a data link layer security policy, use the **linksec policy** command in service template configuration mode. To remove the link layer security policy, use the **no** form of this command.

linksec policy {**must-not-secure | must-secure | should-secure**}

no linksec policy

Syntax Description

must-not-secure	Specifies that the session must not be secured with Media Access Control Security (MACsec) standard.
must-secure	Specifies that the device port must be authorized only if a secure MACsec session is established.
should-secure	Specifies that the link security policy has optionally secured sessions. If an attempt to establish a MACsec session fails, an authorization failure message is not sent.

Command Default

A data link layer security policy is not configured.

Command Modes

Service template configuration (config-service-template)

Command History

Release	Modification
15.2(1)E	This command was introduced.

Usage Guidelines

Configure the link layer security policy within a service template and its associated policy action.

Examples

The following example shows how to configure the link security policy so that the device port is authorized only if a secure MACsec session is established:

```
Device(config)# service-template dot1x-macsec-policy
Device(config-service-template)# linksec policy must-secure
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.

Command	Description
policy-map type control subscriber	Defines a control policy for subscriber sessions.

mac-delimiter

To specify the MAC delimiter for RADIUS compatibility mode, use the **mac-delimiter** command in server group configuration mode. To return to the default value, use the **no** form of this command.

mac-delimiter {**colon**| **hyphen**| **none**| **single-hyphen**}

no mac-delimiter {**colon**| **hyphen**| **none**| **single-hyphen**}

Syntax Description

colon	Sets the delimiter to a colon, in the format xx:xx:xx:xx:xx:xx.
hyphen	Sets the delimiter to a hyphen (-), in the format xx-xx-xx-xx-xx-xx.
none	Sets the delimiter to none, in the format xxxxxxxxxxxx. This is the default value.
single-hyphen	Sets the delimiter to a single hyphen, in the format xxxxxx-xxxxxx.

Command Default

The MAC delimiter is set to none.

Command Modes

Server group configuration (config-sg-radius)

Command History

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

Usage Guidelines

Use the **mac-delimiter** command to set the delimiter that is used in MAC addresses that are sent to the RADIUS authentication server.

Examples

The following example shows how to configure a RADIUS server group with the MAC delimiter set to a colon:

```
aaa group server radius LAB_RAD
 key-wrap enable
 subscriber mac-filtering security-mode mac
 mac-delimiter colon
```

Related Commands

Command	Description
key-wrap enable	Enables AES key wrap.

Command	Description
subscriber mac-filtering security-mode	Specifies the RADIUS compatibility mode for MAC filtering.

match authorization-failure

To create a condition that returns true, based on the type of authorization failure of a session, use the **match authorization-failure** command in control class-map filter configuration mode. To remove the condition, use the **no** form of this command.

match authorization-failure {**domain-change-failed | linksec-failed | tunnel-return**}

no match authorization-failure {**domain-change-failed | linksec-failed | tunnel-return**}

Syntax Description

domain-change-failed	Specifies that the domain change has failed.
linksec-failed	Specifies that the data link security has failed.
tunnel-return	Specifies that the Converged Guest Access (CGA) tunnel authorization has failed.

Command Default

The control class does not contain a condition based on the type of authorization failure.

Command Modes

Control class-map filter configuration (config-filter-control-classmap)

Command History

Release	Modification
15.2(1)E	This command was introduced.
Cisco IOS XE Release 3.3SE	This command was integrated into Cisco IOS XE Release 3.3SE.

Usage Guidelines

The **match authorization-failed** command configures a match condition in a control class based on the type of authorization failure that is configured for a session. Authorization failure can be either a data link layer security failure or a domain change failure. A control class can contain multiple conditions, that are evaluated as either true or false. The control class defines whether all, any, or none of the conditions must evaluate true to execute the actions of the control policy.

The **class** command associates a control class with a control policy.

Examples

The following example shows how to configure a control class that evaluates true if a session failure is caused by the data link layer security failure:

```
Device(config)# class-map type control subscriber match-all CLASS-1
Device(config-filter-control-classmap)# match authorization-failure linksec-failed
```

Related Commands

Command	Description
class	Associates a control class with one or more actions in a control policy.
class-map type control subscriber	Creates a control class that defines the conditions that execute actions of a control policy.
policy-map type control subscriber	Defines a control policy for subscriber sessions.

radius-server host

To specify a RADIUS server host, use the **radius-server host** command in global configuration mode. To delete the specified RADIUS host, use the **no** form of this command.

Cisco IOS Release 12.4T and Later Releases

radius-server host {*hostname*| *ip-address*} [**alias**{*hostname*| *ip-address*}| [**acct-port** *port-number*] [**auth-port** *port-number*] **[non-standard]** [**timeout** *seconds*] [**retransmit** *retries*] [**backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *number-of-retransmits*]] [**key** *encryption-key*]]

no radius-server host {*hostname*| *ip-address*}

All Other Releases

radius-server host {*hostname*| *ip-address*} [**alias**{*hostname*| *ip-address*}| [**acct-port** *port-number*] [**auth-port** *port-number*] **[non-standard]** [**timeout** *seconds*] [**retransmit** *retries*] [**test username** *user-name* **[ignore-acct-port] [ignore-auth-port]** [**idle-time** *minutes*]] [**backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *number-of-retransmits*]] [**key-wrap encryption-key** *encryption-key* **message-auth-code-key** *encryption-key* [**format** {**ascii**| **hex**}]| **pac**] [**key** *encryption-key*]]

no radius-server host {*hostname*| *ip-address*}

Syntax Description

hostname	Domain Name System (DNS) name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.
alias	(Optional) Allows up to eight aliases per line for any given RADIUS server.
acct-port *port-number*	(Optional) UDP destination port for accounting requests. • The host is not used for authentication if the port number is set to zero. If the port number is not specified, the default port number assigned is 1646.
auth-port *port-number*	(Optional) UDP destination port for authentication requests. • The host is not used for authentication if the port number is set to zero. If the port number is not specified, the default port number assigned is 1645.
non-standard	Parses attributes that violate the RADIUS standard.

timeout *seconds*	(Optional) Time interval (in seconds) that the device waits for the RADIUS server to reply before retransmitting. • The timeout keyword overrides the global value of the **radius-server timeout** command. • If no timeout value is specified, a global value is used; the range is from 1 to 1000.
retransmit *retries*	(Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or there is a delay in responding. • The retransmit keyword overrides the global setting of the **radius-server retransmit** command. • If no retransmit value is specified, a global value is used; the range is from 1 to 100.
test username *user-name*	(Optional) Sets the test username for the automated testing feature for RADIUS server load balancing.
ignore-acct-port	(Optional) Disables the automated testing feature for RADIUS server load balancing on the accounting port.
ignore-auth-port	(Optional) Disables the automated testing feature for RADIUS server load balancing on the authentication port.
idle-time *minutes*	(Optional) Length of time (in minutes) the server remains idle before it is quarantined and test packets are sent out. The range is from 1 to 35791. The default is 60.
backoff exponential	(Optional) Sets the exponential retransmits backup mode.
max-delay *minutes*	(Optional) Sets the maximum delay (in minutes) between retransmits. • **max-delay** *minutes* *minutes*—The range is from 1 to 120. The default value is 3.
key-wrap encryption-key	(Optional) Specifies the key-wrap encryption key.

message-auth-code-key	Specifies the key-wrap message authentication code key.
format	(Optional) Specifies the format of the message authenticator code key. • Valid values are: ◦ **ascii—**Configures the key in ASCII format. ◦ **hex—**Configures the key in hexadecimal format.
backoff-retry *number-of-retransmits*	(Optional) Specifies the exponential backoff retry. • *number-of-retransmits***—**Number of backoff retries. The range is from 1 to 50. The default value is 8.
pac	(Optional) Generates the per-server Protected Access Credential (PAC) key.
key	(Optional) Encryption key used between the device and the RADIUS daemon running on this RADIUS server. • The **key** keyword overrides the global setting of the **radius-server key** command. If no key string is specified, a global value is used. **Note** The **key** keyword is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command syntax because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
encryption-key	Specifies the encryption key. • Valid values for *encryption-key* are: ◦ **0—**Specifies that an unencrypted key follows. ◦ **7—**Specifies that a hidden key follows. ◦ String specifying the unencrypted (clear-text) server key.

Command Default No RADIUS host is specified and RADIUS server load balancing automated testing is disabled by default.

Command Modes Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.0(5)T	This command was modified to add options for configuring timeout, retransmission, and key values per RADIUS server.
12.1(3)T	This command was modified. The **alias** keyword was added.
12.2(15)B	This command was integrated into Cisco IOS Release 12.2(15)B. The **backoff exponential**, **backoff-retry**, **key**, and **max-delay** keywords and *number-of-retransmits, encryption-key*, and *minutes* arguments were added.
12.2(28)SB	This command was integrated into Cisco release 12.2(28)SB. The **test username** *user-name*, **ignore-auth-port**, **ignore-acct-port**, and **idle-time** *seconds* keywords and arguments were added for configuring the RADIUS server load balancing automated testing functionality.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB apply to Cisco IOS Release 12.2(33)SRA and subsequent 12.2SR releases.
12.4(11)T	This command was modified. **Note** The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB do not apply to Cisco IOS Release 12.4(11)T or to subsequent 12.4T releases.
12.2 SX	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. **Note** The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB do not apply to Cisco IOS Release 12.2SX.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.3(1)S	This command was modified. The **key-wrap encryption-key**, **message-auth-code-key**, **format**, **ascii**, and **hex** keywords were added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

You can use multiple **radius-server host** commands to specify multiple hosts. The software searches for hosts in the order in which you specify them.

If no host-specific timeout, retransmit, or key values are specified, the global values apply to each host.

We recommend the use of a test user who is not defined on the RADIUS server for the automated testing of the RADIUS server. This is to protect against security issues that can arise if the test user is not configured correctly.

If you configure one RADIUS server with a nonstandard option and another RADIUS server without the nonstandard option, the RADIUS server host with the nonstandard option does not accept a predefined host. However, if you configure the same RADIUS server host IP address for different UDP destination ports, where one UDP destination port (for accounting requests) is configured using the **acct-port** keyword and another UDP destination port (for authentication requests) is configured using the **auth-port** keyword with and without the nonstandard option, the RADIUS server does not accept the nonstandard option. This results in resetting all the port numbers. You must specify a host and configure accounting and authentication ports on a single line.

To use separate servers for accounting and authentication, use the zero port value as appropriate.

RADIUS Server Automated Testing

When you use the **radius-server host** command to enable automated testing for RADIUS server load balancing:

- The authentication port is enabled by default. If the port number is not specified, the default port number (1645) is used. To disable the authentication port, specify the **ignore-auth-port** keyword.
- The accounting port is enabled by default. If the port number is not specified, the default port number (1645) is used. To disable the accounting port, specify the **ignore-acct-port** keyword.

Examples

The following example shows how to specify host1 as the RADIUS server and to use default ports for both accounting and authentication depending on the Cisco release that you are using:

```
radius-server host host1
```

The following example shows how to specify port 1612 as the destination port for authentication requests and port 1616 as the destination port for accounting requests on the RADIUS host named host1:

```
radius-server host host1 auth-port 1612 acct-port 1616
```

Because entering a line resets all the port numbers, you must specify a host and configure accounting and authentication ports on a single line.

The following example shows how to specify the host with IP address 192.0.2.46 as the RADIUS server, uses ports 1612 and 1616 as the authorization and accounting ports, sets the timeout value to six, sets the retransmit value to five, and sets “rad123” as the encryption key, thereby matching the key on the RADIUS server:

```
radius-server host 192.0.2.46 auth-port 1612 acct-port 1616 timeout 6 retransmit 5 key
rad123
```

To use separate servers for accounting and authentication, use the zero port value as appropriate.

The following example shows how to specify the RADIUS server host1 for accounting but not for authentication, and the RADIUS server host2 for authentication but not for accounting:

```
radius-server host host1.example.com auth-port 0
radius-server host host2.example.com acct-port 0
```

The following example shows how to specify four aliases on the RADIUS server with IP address 192.0.2.1:

```
radius-server host 192.0.2.1 auth-port 1646 acct-port 1645
radius-server host 192.0.2.1 alias 192.0.2.2 192.0.2.3 192.0.2.4
```

The following example shows how to enable exponential backoff retransmits on a per-server basis. In this example, assume that the retransmit is configured for three retries and the timeout is configured for five seconds; that is, the RADIUS request will be transmitted three times with a delay of five seconds. Thereafter, the device will continue to retransmit RADIUS requests with a delayed interval that doubles each time until 32 retries have been achieved. The device will stop doubling the retransmit intervals after the interval surpasses the configured 60 minutes; it will transmit every 60 minutes.

The **pac** keyword allows the PAC-Opaque, which is a variable length field, to be sent to the server during the Transport Layer Security (TLS) tunnel establishment phase. The PAC-Opaque can be interpreted only by the server to recover the required information for the server to validate the peer's identity and authentication. For example, the PAC-Opaque may include the PAC-Key and the PAC's peer identity. The PAC-Opaque format and contents are specific to the issuing PAC server.

The following example shows how to configure automatic PAC provisioning on a device. In seed devices, the PAC-Opaque has to be provisioned so that all RADIUS exchanges can use this PAC-Opaque to enable automatic PAC provisioning for the server being used. All nonseed devices obtain the PAC-Opaque during the authentication phase of a link initialization.

```
enable
configure terminal
radius-server host 10.0.0.1 auth-port 1812 acct-port 1813 pac
```

Examples

The following example shows how to enable RADIUS server automated testing for load balancing with the authorization and accounting ports specified depending on the Cisco release that you are using:

```
radius-server host 192.0.2.176 test username test1 auth-port 1645 acct-port 1646
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces that run PPP.
aaa authorization	Sets parameters that restrict network access to a user.
debug aaa test	Shows when the idle timer or dead timer has expired for RADIUS server load balancing.
load-balance	Enables RADIUS server load balancing for named RADIUS server groups.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are to be selected on the interface.

Command	Description
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon.
radius-server load-balance	Enables RADIUS server load balancing for the global RADIUS server group.
radius-server retransmit	Specifies the number of times Cisco software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval that a device waits for a server host to reply.
test aaa group	Tests the RADIUS load balancing server response manually.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

show ip admission

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

Cisco IOS XE Release 3SE and Later Releases

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

All Other Releases

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

Syntax Description

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

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

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Device# show ip admission cache

Authentication Proxy Cache
Total Sessions: 1 Init Sessions: 1
 Client MAC 5cf3.fc25.7e3d Client IP 1.150.128.2 IPv6 :: Port 0, State INIT, Method Webauth
```

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

```
Device# show ip admission statistics

Webauth input-feature statistics:
                                                        IPv4          IPv6
  Total packets received                                46            0
    Delivered to TCP                                    46            0
    Forwarded                                           0             0
    Dropped                                             0             0
    TCP new connection limit reached                    0             0

Webauth HTTPd statistics:

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

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

```
Device# show ip admission status

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

  Parameter Map: Global
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH
    Custom Pages
      Custom pages not configured
    Banner
      Type: text
        Banner                  " <H2>Login Page Banner</H2> "
        Html                    " <H2>Login Page Banner</H2> "
        Length                  48

  Parameter Map: PMAP_CONSENT
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBCONSENT
    Custom Pages
      Custom pages not configured
```

```
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH_CUSTOM_FLASH
    Custom Pages
      Type: "login"
        File                    flash:webauth_login.html
        File status             Ok - File cached
        File mod time           2012-07-20T02:29:36.000Z
        File needs re-cached    No
        Cache                   0x3AEE1E1C
        Cache len               246582
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "success"
        File                    flash:webauth_success.html
        File status             Ok - File cached
        File mod time           2012-02-21T06:57:28.000Z
        File needs re-cached    No
        Cache                   0x3A529B3C
        Cache len               70
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "failure"
        File                    flash:webauth_fail.html
        File status             Ok - File cached
        File mod time           2012-02-21T06:55:49.000Z
        File needs re-cached    No
        Cache                   0x3A5BEBC4
        Cache len               67
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "login expired"
        File                    flash:webauth_expire.html
        File status             Ok - File cached
        File mod time           2012-02-21T06:55:25.000Z
        File needs re-cached    No
        Cache                   0x3AA20090
        Cache len               69
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH_CUSTOM_EXTERNAL
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured
```

The following is sample output from the **show ip admission status banners** command for a banner configured with the **banner text** command:

```
Device# show ip admission status banners

IP admission status:
  Parameter Map: Global
    Banner not configured

  Parameter Map: PMAP_WEBAUTH
    Type: text
      Banner                    " <H2>Login Page Banner</H2> "
      Html                      " <H2>Login Page Banner</H2> "
      Length                    48
```

The following is sample output from the **show ip admission status banners** command for a banner configured with the **banner file** command:

```
Device# show ip admission status banners

IP admission status:
  Parameter Map: Global
    Banner not configured
```

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

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

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

```
Device# show ip admission status custom pages

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

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

Table 1: show ip admission Field Descriptions

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

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

```
Device# show ip admission configuration

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

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

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

```
Device# show ip admission cache eapoudp

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

The fields in the displays are self-explanatory.

Related Commands

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

subscriber aging

To enable an inactivity timer for subscriber sessions, use the **subscriber aging** command in interface configuration mode. To return to the default, use the **no** form of this command.

subscriber aging {**inactivity-timer** *seconds* **[probe]| probe**}

no subscriber aging

Syntax Description

inactivity-timer *seconds*	Maximum amount of time, in seconds, that a session can be inactive. Range: 1 to 65535. Default: 0, which sets the timer to disabled.
probe	Enables an address resolution protocol (ARP) probe.

Command Default

The inactivity timer is disabled.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use the **subscriber aging** command to set the maximum amount of time that a subscriber session can exist with no activity or data from the end client. If this timer expires before there is any activity or data, the session is cleared.

Examples

The following example shows how to set the inactivity timer to 60 seconds on Ten Gigabit Ethernet interface 1/0/2:

```
interface TenGigabitEthernet 1/0/2
 subscriber aging inactivity-timer 60 probe
 service-policy type control subscriber POLICY_1
```

Related Commands

inactivity-timer	Enables an inactivity timeout for subscriber sessions.
ip device tracking probe	Enables the tracking of device probes.
service-policy type control subscriber	Applies a control policy to an interface.

subscriber mac-filtering security-mode

To specify the RADIUS compatibility mode for MAC filtering, use the **subscriber mac-filtering security-mode** command in server group configuration mode. To return to the default value, use the **no** form of this command.

subscriber mac-filtering security-mode {**mac**| **none**| **shared-secret**}

no subscriber mac-filtering security-mode {**mac**| **none**| **shared-secret**}

Syntax Description

mac	Sends the MAC address as the password.
none	Does not send the password attribute. This is the default value.
shared-secret	Sends the shared-secret as the password.

Command Default

The security mode is set to none.

Command Modes

Server group configuration (config-sg-radius)

Command History

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

Usage Guidelines

Use the **subscriber mac-filtering security-mode** command to set the type of security used for MAC filtering in RADIUS compatibility mode.

Examples

The following example shows how to configure a server group with MAC filtering to send the MAC address as the password:

```
aaa group server radius LAB_RAD
 key-wrap enable
 subscriber mac-filtering security-mode mac
 mac-delimiter colon
```

Related Commands

Command	Description
key-wrap enable	Enables AES key wrap.
mac-delimiter	Specifies the MAC delimiter for RADIUS compatibility mode.

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

tunnel type capwap (service-template)

To configure a Control And Provisioning of Wireless Access Points protocol (CAPWAP) tunnel in a service template, use the **tunnel type capwap** command in service-template configuration mode. To disable the CAPWAP tunnel, use the **no** form of this command.

tunnel type capwap name *tunnel-name*

no tunnel type capwap name *tunnel-name*

Syntax Description

name *tunnel-name*	Specified the name of the CAPWAP tunnel.

Command Default

CAPWAP tunnel is not configured.

Command Modes

Service-template configuration (config-service-template)

Command History

Release	Modification
Cisco IOS XE Release 3.3SE	This command was introduced.

Usage Guidelines

Use this command to create a CAPWAP tunnel to enable wired guest access through a wireless port. For wireless access, guests are directed through a Control And Provisioning of Wireless Access Points (CAPWAP) tunnel to the wireless controller in the DMZ (demilitarized zone) and are provided open or web-authenticated access from the wireless controller.

Examples

The following example shows how to configure a CAPWAP tunnel:

```
Device(config)# service-template GUEST-TUNNEL
Device(config-service-template)# tunnel type capwap name tunnel1
```

Related Commands

Command	Description
service-template	Defines a template that contains a set of service policy attributes to apply to subscriber sessions.

voice vlan (service template)

To assign a voice VLAN to subscriber sessions, use the **voice vlan** command in service template configuration mode. To disable the voice VLAN, use the **no** form of this command.

voice vlan

no voice vlan

Syntax Description

This command has no keywords or arguments.

Command Default

The service template does not assign a voice VLAN.

Command Modes

Service template configuration (config-service-template)

Command History

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

Usage Guidelines

Use the **voice vlan** command to assign a voice VLAN to sessions on which the service template is activated.

Examples

The following example shows how to configure a service template that applies a VLAN:

```
Device(config)# service-template CRITICAL-VOICE
Device(config-service-template)# voice vlan
```

Related Commands

Command	Description
activate (policy-map action)	Activates a control policy or service template on a subscriber session.