RADIUS

Feature history for RADIUS

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature name and description	Supported platform
Cisco IOS XE 17.18.1	RADIUS: RADIUS is a distributed client/server system that secures networks against unauthorized access by providing flexible administrative control over authentication, authorization processes, and offers detailed accounting information.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Understand RADIUS

RADIUS is a distributed client/server system that secures networks against unauthorized access by providing flexible administrative control over authentication, authorization processes, and offers detailed accounting information. RADIUS clients operate on Cisco devices and send authentication requests to a central RADIUS server, which holds all user authentication and network service access information.

Key Concepts of RADIUS:

- **Authentication**: Verifies the identity of a user or device attempting to connect to the network.

- **Authorization**: Determines what actions the authenticated user or device is allowed to perform.
- **Accounting**: Tracks the actions and usage of authenticated users for auditing or billing purposes.

RADIUS authentication

RADIUS authentication is a process that verifies identity using a sequence of predefined authentication methods. To configure AAA authentication, define a list of authentication methods and apply it to various ports. The method list defines the types and sequence of authentication to be performed and must be applied to a specific port before any methods are executed. The only exception is the default method list. The default method list is automatically applied to all ports except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. Designate one or more security protocols to be used for authentication, ensuring a backup system for authentication if the initial method fails. The software uses the first method listed to authenticate users. If this method fails to respond, the next method in the list is selected. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point, that is, if the security server or local username database denies user access, the authentication process stops, and no other methods are attempted.

RADIUS authorization

RADIUS authorization is a process where the RADIUS server provides information about what a user or device is allowed to do after being authenticated. It ensures that authenticated users or devices only gain access to resources and privileges they are authorized to use.

RADIUS authorization involves configuring a user's session based on profile information from either a local database or security server, limiting access to services.

RADIUS accounting

RADIUS accounting feature is used to track and record network usage by users who access a network through AAA services, and provides detailed tracking of user activity, network performance monitoring, and troubleshooting.

Enable AAA accounting to report user activity as accounting records to the RADIUS security server. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. You can then analyze the data for network management, client billing, or auditing.

RADIUS server host

A RADIUS server host refers to the physical or virtual server that runs the RADIUS protocol, which is used for centralized AAA for network access. A RADIUS server host acts as the central point where user credentials are validated against a database or directory.

Device-to-RADIUS-server communication involves several components:

- Hostname or IP address
- Authentication destination port
- Accounting destination port

- Key string
- Timeout period
- Retransmission value

Identify RADIUS security servers by hostname, IP address, hostname with specific UDP port numbers, or IP address with specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.

When two host entries are configured for the same service on the same RADIUS server, such as accounting, the second host entry acts as a fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the %RADIUS-4-RADIUS_DEAD message appears, and then the device tries the second host entry configured on the same device for accounting services. The RADIUS host entries are attempted in the sequence they are established.

A RADIUS server and the device use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, specify the host running the RADIUS server daemon and the shared secret text (key) string with the device.

The timeout, retransmission, and encryption key values can be configured globally for all RADIUS servers, on a per-server basis, or in some combination of global and per-server settings.

RADIUS server groups

A RADIUS server group is a logical grouping of multiple RADIUS servers used in networking to provide redundancy, load balancing, and flexibility in AAA processes.

When a network device needs to authenticate users or devices, it sends requests to the RADIUS server group instead of a single server. The group determines which server to use based on priority, load balancing, or failover policies.

Server groups can include multiple host entries for the same server if each entry has a unique identifier. This identifier combines the IP address and UDP port number. This allows different ports to be individually defined as RADIUS hosts that provide a specific AAA service. This unique identifier allows RADIUS requests to be sent to different UDP ports on the same IP address. If you configure two different host entries on the same RADIUS server for the same service, such as accounting, the second configured host entry acts as a failover backup to the first one. If the first host entry fails to provide accounting services, the Network Access Server attempts to use the second host entry on the same device for accounting services. RADIUS host entries are processed in their configuration order.

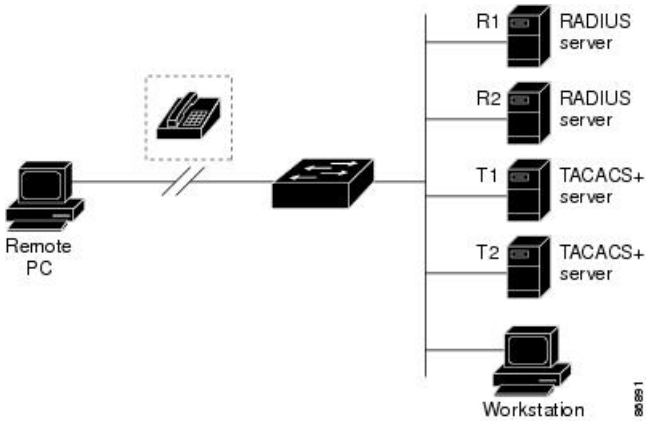
RADIUS usage

Use RADIUS in these network environments that require access security:

- In networks with multiple-vendor access servers, each supports RADIUS. For example, servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.
- Turnkey network security environments in which applications support the RADIUS protocol, such as in an access environment that uses a *smart card* access control system.

- Networks already using RADIUS. You can add a Cisco device containing a RADIUS client to the network. This might be the first step when you make a transition to a TACACS+ server. See the illustration: Transitioning from RADIUS to TACACS+ Services below.

Figure 1: Transitioning from RADIUS to TACACS+ Services



- Network in which the user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to the network through a protocol such as IEEE 802.1x.
- Networks that require resource accounting. You can use RADIUS accounting independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, showing the amount of resources (such as time, packets, bytes, and so forth) used during the session. An ISP might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

RADIUS operation

When a user attempts to log in and authenticate to a device that is access controlled by a RADIUS server, these events occur:

1. The user is prompted to enter a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The user receives one of the following responses from the RADIUS server:
   - ACCEPT: The user is authenticated.
   - REJECT: The user is either not authenticated and is prompted to re-enter the username and password, or access is denied.
   - CHALLENGE: A challenge requires additional data from the user.
   - CHALLENGE PASSWORD: A response requests the user to select a new password.

   The ACCEPT or REJECT response is bundled with additional data that is used for privileged EXEC or network authorization. The additional data included with the ACCEPT or REJECT packets includes these items:
   - Telnet, SSH, rlogin, or privileged EXEC services

- Connection parameters, including the host or client IP address, access list, and user timeouts

RADIUS default configuration

RADIUS and AAA are disabled by default. To prevent a lapse in security, you cannot configure RADIUS through a network management application. When enabled, RADIUS can authenticate users accessing the device through the CLI.

Vendor-specific RADIUS attributes

Vendor-specific RADIUS attributes (VSAs) are custom attributes that are defined within the RADIUS protocol to extend its functionality and provide features specific to their devices or services. These attributes fall outside the standard RADIUS attribute set defined by the Internet Engineering Task Force (IETF). VSAs allow vendors to enable additional capabilities, configure advanced features, and gather specific information relevant to their products.

Cisco implements RADIUS using the format recommended in attribute 26 specification. Cisco's vendor-ID is 9, and the supported option has vendor type 1, which is named *cisco-avpair*. The value is a string with this format:

```
protocol : attribute sep value *
```

Protocol is a value of the Cisco protocol attribute for a particular type of authorization. *Attribute* and *value* are an appropriate attributevalue (AV) pair defined in the Cisco TACACS+ specification, and *sep* is = for mandatory attributes and is * for optional attributes. The full set of features available for TACACS+ authorization can then be used for RADIUS.

For example, the following AV pair causes Cisco "multiple named IP address pools" feature to be activated during IP authorization (during PPP's Internet Protocol Control Protocol (IPCP) address assignment):

```
cisco-avpair= ”ip:addr-pool=first“
```

Inserting an "*" makes the AV pair "ip:addr-pool=first" optional. Any AV pair can be made optional.

```
cisco-avpair= ”ip:addr-pool*first“
```

The following example shows how to cause a user logging in from a network access server to have immediate access to EXEC commands:

```
cisco-avpair= ”shell:priv-lvl=15“
```

Other vendors have their own unique vendor-IDs, options, and associated VSAs. For more information about vendor-IDs and VSAs, see RFC 2138, "Remote Authentication Dial-In User Service (RADIUS)."

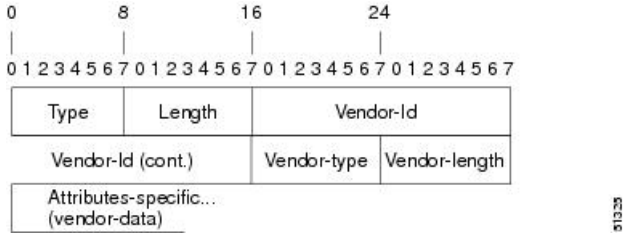
Attribute 26 contains the following three elements:

- Type
- Length
- String (also known as data)
    - Vendor-ID
    - Vendor-Type
    - Vendor-Length

- Vendor-Data

The figure below shows the packet format for a VSA encapsulated “behind” attribute 26.

Figure 2: VSA Encapsulated Behind Attribute 26



Note It is up to the vendor to specify the format of their VSA. The Attribute-Specific field (also known as Vendor-Data) is dependent on the vendor's definition of that attribute.

The table describes significant fields listed in the Vendor-Specific RADIUS IETF Attributes table, which contains supported vendor-specific RADIUS attributes (IETF attribute 26).

Table 1: Vendor-Specific Attributes Table Field Descriptions

Field	Description
Number	All attributes listed in the following table are extensions of IETF attribute 26.
Vendor-Specific Command Codes	A defined code used to identify a particular vendor. Code 9 defines Cisco VSAs, 311 defines Microsoft VSAs, and 529 defines Ascend VSAs.
Sub-Type Number	The attribute ID number. This number is much like the ID numbers of IETF attributes, except it is a “second layer” ID number encapsulated behind attribute 26.
Attribute	The ASCII string name of the attribute.
Description	Description of the attribute.

Table 2: Vendor-Specific RADIUS IETF Attributes

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
MS-CHAP Attributes				

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	311	1	MSCHAP-Response	It contains the response value provided by a PPP MS-CHAP user responding to the challenge. It is only used in Access-Request packets. This attribute is identical to the PPP CHAP Identifier. (RFC 2548)
26	311	11	MSCHAP-Challenge	Contains the challenge sent by a network access server to an MS-CHAP user. It can be used in both Access-Request and Access-Challenge packets. (RFC 2548)
VPDN Attributes				
26	9	1	l2tp-cm-local-window-size	This specifies the maximum receive window size for L2TP control messages, and this value is advertised to the peer during tunnel establishment.
26	9	1	l2tp-drop-out-of-order	Respects sequence numbers on data packets by dropping those that are received out of order. This does not ensure that sequence numbers will be sent on data packets, just how to handle them if they are received.
26	9	1	l2tp-hello-interval	Specifies the number of seconds for the hello keepalive interval. Hello packets are sent when no data has been sent on a tunnel for the number of seconds configured here.
26	9	1	l2tp-hidden-avp	When enabled, sensitive AVPs in L2TP control messages are scrambled or hidden.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	l2tp-nosession-timeout	Specifies the number of seconds that a tunnel will stay active with no sessions before timing out and shutting down.
26	9	1	tunnel-tos-reflect	Copies the IP ToS field from the IP header of each payload packet to the IP header of the tunnel packet for packets entering the tunnel at the LNS.
26	9	1	l2tp-tunnel-authen	If this attribute is set, it performs L2TP tunnel authentication.
26	9	1	l2tp-tunnel-password	This shared secret is used for L2TP tunnel authentication and AVP hiding.
26	9	1	l2tp-udp-checksum	This is an authorization attribute and defines whether L2TP should perform UDP checksums for data packets. Valid values are “yes” and “no.” The default is no.
Store and Forward Fax Attributes				
26	9	3	Fax-Account-Id-Origin	Indicates the account ID origin as defined by system administrator for the **mmoip aaa receive-id** or the **mmoip aaa send-id** commands.
26	9	4	Fax-Msg-Id=	Indicates a unique fax message identification number assigned by Store and Forward Fax.
26	9	5	Fax-Pages	Indicates the number of pages transmitted or received during this fax session. This page count includes cover pages.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	6	Fax-Coverpage-Flag	Indicates whether or not a cover page was generated by the off-ramp gateway for this fax session. True indicates that a cover page was generated; false means that a cover page was not generated.
26	9	7	Fax-Modem-Time	Indicates the amount of time in seconds the modem sent fax data (x) and the amount of time in seconds of the total fax session (y), which includes both fax-mail and PSTN time, in the form x/y. For example, 10/15 means that the transfer time took 10 seconds, and the total fax session took 15 seconds.
26	9	8	Fax-Connect-Speed	Indicates the modem speed at which this fax-mail was initially transmitted or received. Possible values are 1200, 4800, 9600, and 14400.
26	9	9	Fax-Recipient-Count	Indicates the number of recipients for this fax transmission. Until e-mail servers support Session mode, the number should be 1.
26	9	10	Fax-Process-Abort-Flag	True means the session was terminated; false means the session was successful, indicating the fax session's status.
26	9	11	Fax-Dsn-Address	Indicates the address to which DSNs will be sent.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	12	Fax-Dsn-Flag	Indicates whether or not DSN has been enabled. True indicates that DSN has been enabled; false means that DSN has not been enabled.
26	9	13	Fax-Mdn-Address	Indicates the address to which MDNs will be sent.
26	9	14	Fax-Mdn-Flag	Indicates whether message delivery notification (MDN) is enabled. True means MDN is enabled; false means MDN is not enabled.
26	9	15	Fax-Auth-Status	Indicates whether or not authentication for this fax session was successful. Possible values for this field are success, failed, bypassed, or unknown.
26	9	16	Email-Server-Address	Indicates the IP address of the e-mail server handling the on-ramp fax-mail message.
26	9	17	Email-Server-Ack-Flag	Indicates that the on-ramp gateway has received a positive acknowledgment from the e-mail server accepting the fax-mail message.
26	9	18	Gateway-Id	Indicates the name of the gateway that processed the fax session. The name appears in the following format: hostname.domain-name.
26	9	19	Call-Type	Describes the type of fax activity: fax receive or fax send.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	20	Port-Used	Indicates the slot/port number of the Cisco AS5300 used to either transmit or receive this fax-mail.
26	9	21	Abort-Cause	If the fax session terminates, indicates the system component that signaled the termination. Examples of system components that could trigger termination: FAP, TIFF, fax-mail client, fax-mail server, ESMTP client, ESMTP server.
H323 Attributes				
26	9	23	Remote-Gateway-ID (h323-remote-address)	Indicates the IP address of the remote gateway.
26	9	24	Connection-ID (h323-conf-id)	Identifies the conference ID.
26	9	25	Setup-Time (h323-setup-time)	Indicates the setup time for this connection in Coordinated Universal Time (UTC) formerly known as Greenwich Mean Time (GMT) or Zulu time.
26	9	26	Call-Origin (h323-call-origin)	Indicates the origin of the call relative to the gateway. Possible values are originating and terminating (answer).
26	9	27	Call-Type (h323-call-type)	Indicates call leg type. Possible values are **telephony** and **VoIP**.
26	9	28	Connect-Time (h323-connect-time)	Indicates the connection time for this call leg in UTC.
26	9	29	Disconnect-Time (h323-disconnect-time)	Indicates the time this call leg was disconnected in UTC.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	30	Disconnect-Cause (h323-disconnect-cause)	Specifies the reason a connection was taken offline per Q.931 specification.
26	9	31	Voice-Quality (h323-voice-quality)	Specifies the impairment factor (ICPIF) affecting voice quality for a call.
26	9	33	Gateway-ID (h323-gw-id)	Indicates the name of the underlying gateway.
Large Scale Dialout Attributes				
26	9	1	callback-dialstring	Defines a dialing string to be used for callback.
26	9	1	data-service	No description available.
26	9	1	dial-number	Defines the number to dial.
26	9	1	force-56	Determines whether the network access server uses only the 56 K portion of a channel, even when all 64 K appear to be available.
26	9	1	map-class	Allows the user profile to reference information configured in a map class of the same name on the network access server that dials out.
26	9	1	send-auth	Defines the protocol to use (PAP or CHAP) for username-password authentication following CLID authentication.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	send-name	PPP name authentication. To apply for PAP, do not configure the **ppp pap sent-name password** command on the interface. For PAP, "preauth:send-name" and "preauth:send-secret" will be used as the PAP username and PAP password for outbound authentication. For CHAP, "preauth:send-name" will be used not only for outbound authentication, but also for inbound authentication. For a CHAP inbound case, the NAS will use the name defined in "preauth:send-name" in the challenge packet to the caller box. **Note** The send-name attribute initially performed functions now executed by both the send-name and remote-name attributes. With the addition of the remote-name attribute, send-name is now restricted to its current operations.
26	9	1	send-secret	PPP password authentication. The vendor-specific attributes "preauth:send-name" and "preauth:send-secret" serve as both the PAP username and password during outbound authentication, while for CHAP outbound, they are applied in the response packet.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	remote-name	Provides the name of the remote host for use in large-scale dial-out. Dialer checks that the large-scale dial-out remote name matches the authenticated name, to protect against accidental user RADIUS misconfiguration. (For example, dialing a valid phone number but connecting to the wrong device.)
Miscellaneous Attributes				
26	9	2	Cisco-NAS-Port	Specifies additional vendor specific attribute (VSA) information for NAS-Port accounting. To specify additional NAS-Port information in the form an Attribute-Value Pair (AVPair) string, use the **radius-server vsa send** global configuration command. **Note** This VSA is typically used in Accounting, but may also be used in Authentication (Access-Request) packets.
26	9	1	min-links	Sets the minimum number of links for MLP.
26	9	1	proxyacl#<n>	Allows users to configure the downloadable user profiles (dynamic ACLs) by using the authentication proxy feature so that users can have the configured authorization to permit traffic going through the configured interfaces.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	spi	Carries the authentication information needed by the home agent to authenticate a mobile node during registration. The information is in the same syntax as the **ip mobile secure host <addr>** configuration command. Basically it contains the rest of the configuration command that follows that string, verbatim. It provides the Security Parameter Index (SPI), key, authentication algorithm, authentication mode, and replay protection timestamp range.

Vendor-proprietary RADIUS server communication

A vendor-proprietary RADIUS server communication is a method of exchanging unique proprietary information between a network device and a RADIUS server. Cisco IOS XE software supports a subset of vendor-proprietary RADIUS attributes.

Specify the host running the RADIUS server daemon and the secret text it shares with the device to configure RADIUS, whether vendor-proprietary or IETF draft-compliant. Use the **radius server** global configuration commands to specify the RADIUS host and secret text string.

DSCP marking for RADIUS packets

DSCP marking for RADIUS packets enables faster authentication and accounting of RADIUS packets. The six most significant bits of the DiffServ field are called the Differentiated Services Code Point (DSCP). Differentiated Services (DiffServ) is a model in which traffic is treated by intermediate systems with relative priorities based on the type of services (ToS) field.

You can configure DSCP marking on the RADIUS server, on the server group, and in global configuration mode. If you configure DSCP marking on the RADIUS server, it overrides settings on the server group and in global configuration mode.

- If there is no DSCP marking configuration on the RADIUS server, the DSCP marking values configured on the server group are applied to the RADIUS packets.
- If there is no DSCP marking configuration on the RADIUS server or the RADIUS server group, the DSCP marking values configured in global configuration mode are applied to the RADIUS packets.

DSCP marking for RADIUS packets is applicable to administrative access sessions such as SSH and Telnet. You can use the **aaa authentication** global configuration command to define RADIUS authentication for administrative sessions.

RADIUS Change of Authorization

The RADIUS Change of Authorization (CoA) provides a mechanism to change the attributes of an AAA session after it is authenticated. When a policy changes for a user or user group in AAA, administrators can send RADIUS CoA packets from the AAA server such as a Cisco Secure Access Control Server (ACS) to reinitialize authentication and apply the new policy. This section provides an overview of the RADIUS interface including available primitives and how they are used during a CoA.

- CoA requests
- CoA request response code
- CoA request commands
- Stacking guidelines for session termination

A standard RADIUS interface is typically used in a pulled model where the request originates from a network attached device and the response come from the queried servers. Cisco devices support RADIUS CoA extensions defined in RFC 5176, typically used in a pushed model and allow for the dynamic reconfiguring of sessions from external AAA or policy servers.

This feature is integrated with Cisco Secure Access Control Server (ACS) 5.1. The RADIUS interface is enabled by default on Cisco devices. However, some basic configuration are required attributes like security, password, and accounting,

Per-session CoA requests are supported for session identification, session termination, host reauthentication, port shutdown, and port bounce. This model comprises one request (CoA-Request) and two possible response codes:

- CoA acknowledgement (ACK) [CoA-ACK]
- CoA nonacknowledgement (NAK) [CoA-NAK]

The request is initiated from a CoA client (typically an AAA or policy server) and directed to the device that acts as a listener.

The table below shows the RADIUS CoA commands and vendor-specific attributes (VSAs) supported by Identity-Based Networking Services. All CoA commands must include the session identifier between the device and the CoA client.

Table 3: RADIUS CoA commands supported by Identity-Based Networking Services

CoA Command	Cisco VSA
Activate service	Cisco:Avpair="subscriber:command=activate-service" Cisco:Avpair="subscriber:service-name=<*service-name*>" Cisco:Avpair="subscriber:precedence=<*precedence-number*>" Cisco:Avpair="subscriber:activation-mode=replace-all"

CoA Command	Cisco VSA
Deactivate service	Cisco:Avpair="subscriber:command=deactivate-service" Cisco:Avpair="subscriber:service-name=<*service-name*>"
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
Session query	Cisco:Avpair="subscriber:command=session-query"
Session reauthenticate	Cisco:Avpair="subscriber:command=reauthenticate" Cisco:Avpair="subscriber:reauthenticate-type=last" or Cisco:Avpair="subscriber:reauthenticate-type=rerun"
Session terminate	This is a standard disconnect request and does not require a VSA.
Interface template	Cisco:AVpair="interface-template-name=<*interfacetemplate*>"

CoA requests

Change of Authorization (CoA) requests, as described in RFC 5176, are used in a push model to allow for session identification, host reauthentication, and session termination. The model is comprised of one request (CoA-Request) and two possible response codes:

- CoA acknowledgment (ACK) [CoA-ACK]
- CoA non-acknowledgment (NAK) [CoA-NAK]

The request is initiated from a CoA client (typically a RADIUS or policy server) and directed to the switch that acts as a listener.

Cisco devices support these per-session CoA requests:

- Session reauthentication
- Session termination
- Session termination with port shutdown
- Session termination with port bounce

RFC 5176 compliance

The Disconnect Request message, which is also referred to as Packet of Disconnect (POD), is supported by the switch for session termination.

This table shows the IETF attributes are supported for this feature.

Table 4: Supported IETF attributes

Attribute Number	Attribute Name
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

This table shows the possible values for the Error-Cause attribute.

Table 5: Error-cause values

Value	Explanation
201	Residual Session Context Removed
202	Invalid EAP Packet (Ignored)
401	Unsupported Attribute
402	Missing Attribute
403	NAS Identification Mismatch
404	Invalid Request
405	Unsupported Service
406	Unsupported Extension
407	Invalid Attribute Value
501	Administratively Prohibited
502	Request Not Routable (Proxy)
503	Session Context Not Found
504	Session Context Not Removable
505	Other Proxy Processing Error
506	Resources Unavailable
507	Request Initiated
508	Multiple Session Selection Unsupported

CoA request response code

The CoA Request response code conveys commands to the switch.

Session Identification

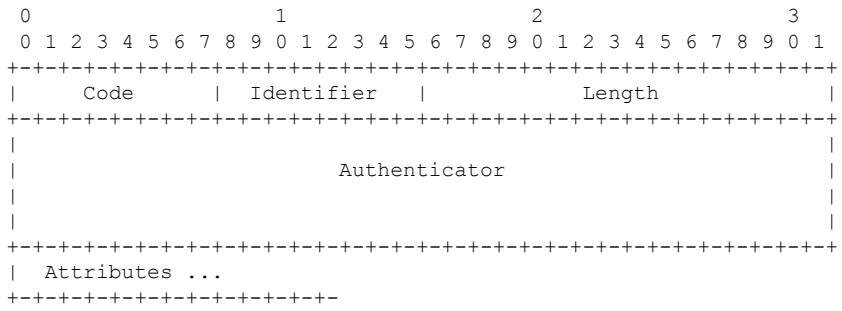
For disconnect and CoA requests targeted at a particular session, the switch locates the session based on one or more of the following attributes:

- Acct-Session-Id (IETF attribute #44)
- Audit-Session-Id (Cisco VSA)
- Calling-Station-Id (IETF attribute #31 which contains the host MAC address)
- IPv6 Attributes, which can be one of the following:
  - Framed-IPv6-Prefix (IETF attribute #97) and Framed-Interface-Id (IETF attribute #96), which together create a full IPv6 address per RFC 3162
  - Framed-IPv6-Address
- Plain IP Address (IETF attribute #8)

Unless all session identification attributes included in the CoA message match the session, the switch returns a Disconnect-NAK or CoA-NAK with the “Invalid Attribute Value” error-code attribute.

If more than one session identification attribute is included in the message, all the attributes must match the session or the switch returns a Disconnect- negative acknowledgment (NAK) or CoA-NAK with the error code “Invalid Attribute Value.”

The packet format for a CoA Request code as defined in RFC 5176 consists of the fields: Code, Identifier, Length, Authenticator, and Attributes in Type:Length:Value (TLV) format. The attributes field is used to carry Cisco vendor-specific attributes (VSAs).



For CoA requests targeted at a particular enforcement policy, the device returns a CoA-NAK with the error code “Invalid Attribute Value” if any of the above session identification attributes are not included in the message.

CoA ACK response code

If the authorization state is changed successfully, a positive acknowledgment (ACK) is sent. The attributes returned within CoA ACK will vary based on the CoA Request and are discussed in individual CoA commands.

CoA NAK response Code

A negative acknowledgment (NAK) indicates a failure to change the authorization state and can include attributes that indicate the reason for the failure. Use **show** commands to verify a successful CoA.

CoA request commands

All CoA commands must include the session identifier between the device and the CoA client.

Table 6: Supported CoA commands

Command	Cisco VSA
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	This is a standard disconnect request that does not require a VSA.
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"

Session reauthentication

The session reauthentication request is generally generated by the AAA server when a host with an unidentified identity or unknown posture connects to the network and is associated with a restricted-access authorization profile (such as a guest VLAN). A reauthentication request allows the host to be placed in the appropriate authorization group when its credentials are known.

To initiate session authentication, the AAA server sends a standard CoA-Request message which contains a Cisco VSA in this form: *Cisco:Avpair="subscriber:command=reauthenticate"* and one or more session identification attributes.

The current session state determines the switch response to the message. If the session is currently authenticated using IEEE 802.1x, the switch responds by sending an EAPoL (Extensible Authentication Protocol over LAN) request-ID message to the server.

If the session is currently authenticated by MAC authentication bypass (MAB), the switch sends an access-request to the server, passing the same identity attributes used for the initial successful authentication.

If the session authentication is in progress when the switch receives the command, the switch terminates the process, and restarts the authentication sequence, starting with the method configured to be attempted first.

If the session is not yet authorized, or is authorized via guest VLAN, or critical VLAN, or similar policies, the reauthentication message restarts the access control methods, beginning with the method configured to be attempted first. The current authorization of the session is maintained until the reauthentication leads to a different authorization result.

Session reauthentication in a switch stack

When a switch stack receives a session reauthentication message:

- It marks the need for re-authentication before returning an acknowledgment (ACK).
- It initiates reauthentication for the appropriate session.
- It removes the signal that triggered the reauthentication after the process is complete.

- If the active switch fails before authentication completes, the stack initiates reauthentication after the active switch changeover, removing the original command.
- If the active switch fails before sending an ACK, the subsequent active switch treats the re-transmitted command as a new command.

Session termination

Session termination involves three types of CoA requests that can trigger this process. A CoA Disconnect-Request terminates the session, without disabling the host port. This command causes re-initialization of the authenticator state machine for the specified host, but does not restrict that host access to the network.

To restrict access to the network for a host, use a CoA Request with the Cisco:Avpair="subscriber:command=disable-host-port" VSA. Use this command to immediately block network access for a host that is causing problems. When you want to restore network access on the port, re-enable it using a non-RADIUS mechanism.

To acquire a new IP address for a device without a supplicant, like a printer, terminate the session on the host port using port-bounce (disable and then re-enable the port), for instance, after a VLAN change.

CoA Disconnect-Request

This command is a standard Disconnect-Request. If you cannot locate the session, your device returns a Disconnect-NAK message with the “Session context not found” error-code attribute. If the session is located, the device terminates the session. The device returns a Disconnect-ACK after removing the session.

If the device fails over to a standby device before returning a Disconnect-ACK to the client, the new active device repeats the process when the client resends the request. If the session is not found after re-sending, a Disconnect-ACK is sent with the “Session Context Not Found” error-code attribute.

CoA Request: Disable Host Port

The RADIUS server CoA command shuts down the authentication port that hosts a session, thereby terminating it. Use this command when a host causes network issues and must be blocked immediately.

To restore network access on the port, reenable it using a non-RADIUS mechanism. The command is included in a CoA-Request message with the attribute Cisco:Avpair="subscriber:command=disable-host-port".

This session-oriented command requires specific attributes to identify the session. If the session cannot be located, the device returns a CoA-NAK message with the 'Session Context Not Found' error-code attribute. If the session is located, the device disables the hosting port and returns a CoA-ACK message.

If the device fails before returning a CoA-ACK to the client, the process is repeated on the new active device when the request is re-sent from the client. If the device fails after returning a CoA-ACK message to the client but before the operation has completed, the operation is restarted on the new active device.

Note If a Disconnect-Request fails after being resent, it could be due to a successful session termination before the change-over or due to issues like a link failure.

CoA Request: Bounce-Port

A RADIUS server can cause a link flap on an authentication port by sending a CoA bounce port. This action triggers DHCP renegotiation from one or more hosts connected to the port. This incident can occur when

there is a VLAN change and the endpoint is a device (such as a printer) that does not have a mechanism to detect a change on this authentication port. The CoA bounce port is carried in a standard CoA-Request message that contains the Cisco:Avpair="subscriber:command=bounce-host-port" VSA.

The command is session-oriented and must be accompanied by one or more session identification attributes. If the session cannot be located, the device returns a CoA-NAK message with the "Session Context Not Found" error-code attribute. If the session is located, the device disables the hosting port for 10 seconds, re-enables it (port-bounce), and returns a CoA-ACK.

If the device fails before returning a CoA-ACK to the client, the process is repeated on the new active device when the request is re-sent from the client. If the device fails after returning a CoA-ACK message to the client but before the operation has completed, the operation is re-started on the new active device.

Stacking guidelines for session termination

In a switch stack, special handling for CoA Disconnect-Request messages is not required.

Stacking guidelines for CoA-Request Bounce-Port

If the session is not found, you cannot execute the **bounce-port** command because it targets a session, not a port.

When the Auth Manager command handler on the active switch receives a valid **bounce-port** command, it checkpoints the following information before returning a CoA-ACK message:

- the need for a port-bounce
- the port-id (found in the local session context)

The switch performs a port-bounce by disabling the port for 10 seconds and then re-enabling it.

If the port-bounce is successful, the standby switch removes the signal that triggered the port-bounce.

If the active switch fails before the port-bounce completes, a port-bounce is initiated after active switch changeover based on the original command (which is subsequently removed).

If the active switch fails before sending a CoA-ACK message, the new active switch treats the re-sent command as a new command.

Stacking guidelines for CoA-Request Disable-Port

Because the **disable-port** command is targeted at a session, not a port, if the session is not found, the command cannot be executed.

When the Auth Manager command handler on the active switch receives a valid **disable-port** command, it verifies this information before returning a CoA-ACK message:

- the need for a port-disable
- the port-id (found in the local session context)

The switch attempts to disable the port.

If the port-disable operation is successful, the standby switch removes the signal that triggered the port-disable.

If the active switch fails before the port-disable operation completes, the port is disabled after active switch changeover based on the original command (which is subsequently removed).

If the active switch fails before sending a CoA-ACK message, the new active switch treats the re-sent command as a new command.

RadSec

RadSec is a secure extension of the traditional RADIUS protocol, designed to address the inherent security limitations of RADIUS by encrypting the communication between RADIUS clients and RADIUS servers. RadSec encrypts the RADIUS server data using a secure tunnel.

You can implement RadSec over TLS and DTLS in both client and device servers. While the client side controls RADIUS AAA, the device side controls CoA.

Configure the following parameters:

- Individual client: specific idle timeout, client trustpoint, and server trustpoint.
- Global CoA: specific TLS or DTLS listening port and the corresponding list of source interfaces.

Configure the **tls watchdoginterval** command to enable RadSec CoA request reception and response transmission over the same channel. Ensure that the TLS watchdog timer is set to a value less than the TLS idle timer, so the established tunnel remains active if RADIUS test authentication packets are detected before the idle timer expires. If the tunnel is torn down and **tls watchdoginterval** command is enabled, the tunnel gets re-established immediately. If **tls watchdoginterval** command is disabled, CoA requests on the same authentication channel are discarded.

Prerequisites for RADIUS

This section lists the prerequisites for controlling device access with RADIUS.

- RADIUS and Authentication, Authorization, and Accounting (AAA) must be enabled to use any of the configuration commands in this chapter.
- RADIUS is facilitated through AAA and can be enabled only through AAA commands.
- Use the **aaa new-model** global configuration command to enable AAA.
- Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication.
- Use **line** and **interface** commands to enable the defined method lists to be used.
- You should have access to and should configure a RADIUS server before configuring RADIUS features on your device.
- The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (Cisco Secure Access Control Server Version 3.0), Livingston, Merit, Microsoft, or another software provider. For more information, see the RADIUS server documentation.
- To use the Change-of-Authorization (CoA) interface, a session must already exist on the switch. CoA can be used to identify a session and enforce a disconnect request. The update affects only the specified session.
- Users must first successfully complete RADIUS authentication before proceeding to RADIUS authorization, if it is enabled.

- For RADIUS over IPv6 configurations, users must enable IPv6 unicast routing by enabling the **ipv6 unicast-routing** command.

Restrictions for RADIUS

General:

- To prevent a lapse in security, you cannot configure RADIUS through a network management application.
- 802.1x and MAC authentication bypass (MAB) authentication using RADIUS is not supported on Cisco C9610 Series Smart Switches.

RADIUS is not suitable in the following network security situations:

- Multiprotocol access environments. RADIUS does not support AppleTalk Remote Access (ARA), NetBIOS Frame Control Protocol (NBFCP), NetWare Asynchronous Services Interface (NASI), or X.25 PAD connections.
- Switch-to-switch or router-to-router situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one device to a non-Cisco device if the non-Cisco device requires authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

DSCP marking support for RADIUS packets:

- DSCP marking for authentication and accounting is not supported for private servers, fully qualified domain name (FQDN) servers and radsec servers.
- In the case of wired IEEE 802.1x authentication, when source port extension is not enabled, the default ports are in use. The DSCP marking is set to the default ports and all the requests will be marked with the same DSCP value.
- DSCP marking is not supported in the case of wireless IEEE 802.1x authentication, where the source port extension is enabled by default.

These restrictions apply to the RadSec feature:

- A RADIUS client uses an ephemeral port as the source port. Avoid using this port simultaneously for UDP, Datagram Transport Layer Security (DTLS), and Transport Layer Security (TLS).
- Use either TLS or DTLS for a server in an AAA group, although there are no configuration restrictions.
- RadSec is not supported on the DTLS port range from 1 to 1024.

Note DTLS ports must be configured to work with the RADIUS server.

- RadSec is not supported with high availability.
- RADIUS Change of Authorization (CoA) reception of requests and transmissions of responses over the authenticated channel are supported only with RadSec over TLS. It is not supported over DTLS or plain RADIUS.

- The **tls watchdoginterval** command is not applicable for Packet of Disconnect (PoD) use cases.
- FQDN configuration for CoA is not supported.

Configure RADIUS

At a minimum, you must identify the host or hosts that run the RADIUS server software and define the method lists for RADIUS authentication. You can optionally define method lists for RADIUS authorization and accounting, and other procedures available in this section.

Identify the RADIUS server host

To apply these settings globally to all RADIUS servers communicating with the device, use the three unique global configuration commands: **radius-server timeout**, **radius-server retransmit**, and **key** *string*.

You can configure the device to use AAA server groups to group existing server hosts for authentication.

You also need to configure some settings on the RADIUS server. The necessary settings include the IP address of the device and the key string shared by both the server and the device.

Use these steps to configure per-server RADIUS server communication.

Before you begin

If you configure both global and per-server functions (timeout, retransmission, and key commands) on the device, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server name* **Example:** `Device(config)# radius server rsim`	Specifies the name for the RADIUS server configuration for Protected Access Credential (PAC) provisioning, and enters RADIUS server configuration mode.
Step 4	**address** {**ipv4** | **ipv6**} *ip address* { **auth-port** *port number* | **acct-port** *port number*} **Example:**	(Optional) Specifies the RADIUS server parameters.

	Command or Action	Purpose
	`Device(config-radius-server)# address ipv4 10.2.2.12 auth-port 1612`	For **auth-port** *port-number*, specify the UDP destination port for authentication requests. The default is 1612. The range is 0–65536. For **acct-port** *port-number*, specify the UDP destination port for authentication requests. The default is 1613.
Step 5	**key** *string* **Example:** `Device(config-radius-server)# key rad123`	(Optional) For **key** *string*, specify the authentication and encryption key used between the device and the RADIUS daemon running on the RADIUS server. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Configure the key as the last item in the **radius server** command. Leading spaces are ignored, but spaces within and at the end of the key are utilized. Avoid using spaces in your key unless the quotation marks are part of the key.
Step 6	**retransmit** *value* **Example:** `Device(config-radius-server)# retransmit 10`	(Optional) Specifies how many times to resend a RADIUS request if the server responds slowly or not at all. The range is 1–100. This setting overrides the **radius-server retransmit** global configuration command setting.
Step 7	**timeout** *seconds* **Example:** `Device(config-radius-server)# timeout 60`	(Optional) Specifies the time interval that the device waits for the RADIUS server to reply before sending a request again. The range is 1–1000. This setting overrides the **radius-server timeout** global configuration command setting. **Note** We recommend that you configure timeout under the **radius-server timeout** command only and not under the **aaa group server radius** command.
Step 8	**end** **Example:** `Device(config-radius-server)# end`	Exits RADIUS server configuration mode and enters privileged EXEC mode.

Configure RADIUS authentication

Use the steps below to configure RADIUS login authentication:

Before you begin

Configure the **ip http authentication aaa** global configuration command to secure HTTP access with AAA methods. Configuring AAA authentication alone does not secure the device for HTTP access.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] **Example:** `Device(config)# aaa authentication login default local`	Creates a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports. • For *list-name*, specify a character string to name the list you are creating. • For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: • *enable*: Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the **enable** *password* global configuration command. • *group radius*: Use RADIUS authentication. Before you can use this authentication method, you must configure the RADIUS server.

	Command or Action	Purpose
		• *line*: Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the **password** *password* line configuration command. • *local*: Use the local username database for authentication. You must enter username information in the database. Use the **username** *name* **password** global configuration command. • *local-case*: Use a case-sensitive local username database for authentication. You must enter username information in the database by using the **username** *password* global configuration command. • *none*: Do not use any authentication for login.
Step 5	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*] **Example:** `Device(config)# line 1 4`	Enters line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 6	**login authentication** {**default** | *list-name*} **Example:** `Device(config-line)# login authentication default`	Applies the authentication list to a line or set of lines. • If you specify **default**, use the default list created with the **aaa authentication login** command. • For *list-name*, specify the list created with the **aaa authentication login** command.
Step 7	**end** **Example:** `Device(config-line)# end`	Exits line configuration mode and enters privileged EXEC mode.

Configure RADIUS authorization

Note Even if authorization is configured, it is bypassed for authenticated users who log in through the CLI.

Use the following steps to configure RADIUS authorization for user privileged access and network services:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa authorization network** *authorization-list* **radius** **Example:** `Device(config)# aaa authorization network list1 radius`	Configures the device for user RADIUS authorization for all network-related service requests.
Step 4	**aaa authorization exec** *authorization-list* **radius** **Example:** `Device(config)# aaa authorization exec list1 radius`	Configures the device for user RADIUS authorization if the user has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

What to do next

Use the **aaa authorization** global configuration command with the **radius** keyword to restrict network access to privileged EXEC mode.

The **aaa authorization exec radius local** command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.

Configure RADIUS accounting

Use these steps to start RADIUS accounting:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa accounting network** *accounting-list***start-stop radius** **Example:** `Device(config)# aaa accounting network start-stop radius`	Enables RADIUS accounting for all network-related service requests.
Step 4	**aaa accounting exec** *accounting-list***start-stop radius** **Example:** `Device(config)# aaa accounting exec acc-list start-stop radius`	Enables RADIUS accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Define RADIUS server groups

Use the **server** group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional **auth-port** and **acct-port** keywords.

Follow these steps to define AAA server groups:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**radius server** *name* **Example:** `Device(config)# radius server ISE`	Specifies the name of the RADIUS server configuration for Protected Access Credential (PAC) provisioning and enters RADIUS server configuration mode. The device also supports RADIUS for IPv6.
Step 4	**address** {**ipv4** | **ipv6**} {*ip-address* | *hostname*} **auth-port** *port-number* **acct-port** *port-number* **Example:** `Device(config-radius-server)# address ipv4 10.1.1.1 auth-port 1612 acct-port 1613`	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.
Step 5	**key** *string* **Example:** `Device(config-radius-server)# key cisco123`	Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server.
Step 6	**exit** **Example:** `Device(config-radius-server)# exit`	Exits RADIUS server configuration mode and enters global configuration mode.
Step 7	**aaa group server radius** *group_name* **Example:** `Device(config)# aaa group server radius abc`	Defines the RADIUS server group configuration and enters RADIUS server group configuration mode.
Step 8	**server name** *server* **Example:** `Device(config-sg-radius)# server name ISE`	Associates the RADIUS server to the server group.
Step 9	**end** **Example:** `Device(config-sg-radius)# end`	Exits RADIUS server group configuration mode and returns to privileged EXEC mode.

Configure RADIUS source-interface under a RADIUS server-group

Configure the RADIUS source-interface under a RADIUS server group using one of these methods:

- Configure a RADIUS source-interface under the RADIUS server-group using the **ip radius source-interface** *interface-name* command.
- Configure a VRF using the **vrf** *vrf-name* command under the RADIUS server-group, and then associate the configured VRF globally to a source-interface using the **ip radius source interface** *interface-name* **vrf** *vrf-name* command.

The source-interface configured under the server group takes priority over both methods.

Use these steps to configure RADIUS source-interface under a RADIUS server-group.

Before you begin

Configure a VRF routing table and associate it with an interface.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	{ **ip** | **ipv6** }**radius source-interface** *interface-number* **vrf** *vrf-name* **Example:** `Device(config)# ip radius source-interface GigabitEthernet1/0/23 vrf vrf17`	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, and enables the specification on a per-VRF basis. • *interface-name*: Specifies the name of the interface that RADIUS uses for all of its outgoing packets. • **vrf** *vrf-name*: Specifies the per-VRF configuration.
Step 4	**aaa group server radius** *group_name* **Example:** `Device(config-sg-radius)# aa group server radius rad-grp`	Groups different RADIUS server hosts into distinct lists and distinct methods and enters server-group configuration mode.
Step 5	**ip vrf forwarding** *vrf-name* **Example:** `Device(config-sg-radius)# ip vrf forwarding vrf17`	(Optional) Configures a VRF for the interface.
Step 6	{ **ip** | **ipv6** } **radius source-interface** *interface-number* **Example:** `Device(config-sg-radius)# ip radius source-interface loopback0`	(Optional) Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets from the RADIUS group server. *interface-name*: Specifies the name of the interface that RADIUS uses for all of its outgoing packets.

	Command or Action	Purpose
Step 7	**end** **Example:** `Device(config-sg-radius)# end`	Returns to privileged EXEC mode.

Configure settings for all RADIUS servers

Start in privileged EXEC mode and follow these steps to configure settings for all RADIUS servers:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server name* **Example:** `Device(config)# radius server rsim`	Specifies the name for the RADIUS server configuration for Protected Access Credential (PAC) provisioning, and enters RADIUS server configuration mode.
Step 4	**key** *string* **Example:** `Device(config-radius-server)# key your_server_key`	Specifies the shared secret text string used between the switch and all RADIUS servers. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, and spaces within and at the end of the key are considered. If spaces are used in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
Step 5	**retransmit** *retries* **Example:** `Device(config-radius-server)# retransmit 5`	Defines the retries for each RADIUS request until the server gives up. The default is 3; the range 1–1000.
Step 6	**timeout** *seconds* **Example:** `Device(config-radius-server)# timeout 3`	Specifies the number of seconds a switch waits for a reply to a RADIUS request before resending the request. The default is 5 seconds; the range is 1–1000.

	Command or Action	Purpose
Step 7	**end** **Example:** `Device(config-radius-server)# end`	Exits RADIUS server configuration mode and enters privileged EXEC mode.

Configure the device to use vendor-specific RADIUS attributes

Use these steps to configure vendor-specific RADIUS attributes:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius-server vsa send** [**accounting** | **authentication**] **Example:** `Device(config)# radius-server vsa send accounting`	Enables the device to recognize and use VSAs as defined by RADIUS IETF attribute 26. • (Optional) Use the **accounting** keyword to limit the set of recognized vendor-specific attributes to only accounting attributes. • (Optional) Use the **authentication** keyword to limit the set of recognized vendor-specific attributes to only authentication attributes. If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Configure the device for vendor-proprietary RADIUS server communication

Use these steps to configure vendor-proprietary RADIUS server communication:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server name* **Example:** `Device(config)# radius server rsim`	Specifies the name for the RADIUS server configuration for Protected Access Credential (PAC) provisioning, and enters RADIUS server configuration mode.
Step 4	**address** { **ipv4 | ipv6** } *ip address* **Example:** `Device(config-radius-server)# address ipv4 172.24.25.10`	(Optional) Specifies the IP address of the RADIUS server.
Step 5	**non-standard** **Example:** `Device(config-radius-server)# non-standard`	Identifies that the RADIUS server using a vendor-proprietary implementation of RADIUS.
Step 6	**key** *string* **Example:** `Device(config-radius-server)# key rad123`	Specifies the shared secret text string used between the device and the vendor-proprietary RADIUS server. The device and the RADIUS server use this text string to encrypt passwords and exchange responses.
Step 7	**end** **Example:** `Device(config-radius-server)# end`	Exits RADIUS server mode and enters privileged EXEC mode.

Configure DSCP marking on a RADIUS server

Use these steps to configure DSCP marking for authentication and accounting on a radius server:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server_name* **Example:** `Device(config)# radius server rsim`	Specifies the name for the RADIUS server configuration for Protected Access Credential (PAC) provisioning, and enters RADIUS server configuration mode.
Step 4	**address** { **ipv4** | **ipv6** } *ip address* [**auth-port** *auth_port_number* **acct-port** *acct_port_number*] **Example:** `Device(config-radius-server)# address ipv4 10.1.1.1 auth-port 1612 acct-port 1613`	(Optional) Specifies the IP address of the RADIUS server. • **auth-port** configures the port value for radius authentication server. The default value is 1812. • **acct-port** configures the port value for radius accounting server. The default value is 1813.
Step 5	**dscp** {**acct** *dscp_acct_value* | **auth** *dscp_auth_value*} **Example:** `Device(config-radius-server)# dscp auth 10 acct 20`	Configures DSCP marking for authentication and accounting on the radius server. • **acct** configures radius DSCP marking value for accounting. The valid range is from 1 to 63. The default value is 0. • **auth** configures radius DSCP marking value for authentication. The valid range is from 1 to 63. The default value is 0.
Step 6	**key** *string* **Example:** `Device(config-radius-server)# key rad123`	Specifies the shared secret text string used between the device and the vendor-proprietary RADIUS server. The device and the RADIUS server use this text string to encrypt passwords and exchange responses.
Step 7	**end** **Example:** `Device(config-radius-server)# end`	Exits RADIUS server mode and enters privileged EXEC mode.

Configure the source interface and DSCP marking on RADIUS server group

Use these steps to configure the source interface and DSCP marking for authentication and accounting on radius server groups:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa group server radius** *group_name* **Example:** `Device(config)# aaa group server radius abc`	Defines the RADIUS server group configuration and enters RADIUS server group configuration mode.
Step 4	**server name** *name* **Example:** `Device(config-sg-radius)# server name serv1`	Associates the RADIUS server to the server group.
Step 5	{**ip** | **ipv6**} **radius source-interface** *type number* **Example:** `Device(config-sg-radius)# ipv6 radius source-interface ethernet 0/0`	Specifies an interface to use for the source address in RADIUS server.
Step 6	**dscp** {**acct** *dscp_acct_value* | **auth** *dscp_auth_value*} **Example:** `Device(config-sg-radius)# dscp auth 10 acct 20`	Configures DSCP marking for authentication and accounting on the radius server group. • **acct** configures radius DSCP marking value for accounting. The valid range is from 1 to 63. The default value is 0. • **auth** configures radius DSCP marking value for authentication. The valid range is from 1 to 63. The default value is 0.
Step 7	**end** **Example:** `Device(config-radius-server)# end`	Exits RADIUS server mode and enters privileged EXEC mode.

Configure CoA on the device

Use these steps to configure CoA on a device. This procedure is required.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Configures the device as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server, and enters dynamic authorization local server configuration mode.
Step 5	**client** {*ip-address* | *name*} [**vrf** *vrfname*] [**server-key** *string*] **Example:** `Device(config-locsvr-da-radius)# client client1 vrf vrf1`	Specifies a RADIUS client from which a device will accept CoA and disconnect requests.
Step 6	**server-key** [**0** | **7**] *string* **Example:** `Device(config-locsvr-da-radius)# server-key your_server_key`	Configures the RADIUS key to be shared between a device and RADIUS clients.
Step 7	**port** *port-number* **Example:** `Device(config-locsvr-da-radius)# port 25`	Specifies the port on which a device listens for RADIUS requests from configured RADIUS clients.
Step 8	**auth-type** {**any** | **all** | **session-key**} **Example:** `Device(config-locsvr-da-radius)# auth-type any`	Specifies the type of authorization the device uses for RADIUS clients. The client must match all the configured attributes for authorization.
Step 9	**ignore server-key** **Example:** `Device(config-locsvr-da-radius)# ignore server-key`	(Optional) Configures the device to ignore the server-key.

	Command or Action	Purpose
Step 10	**exit** **Example:** `Device(config-locsvr-da-radius)# exit`	Exits dynamic authorization local server configuration mode and returns to global configuration mode.
Step 11	**authentication command bounce-port ignore** **Example:** `Device(config)# authentication command bounce-port ignore`	(Optional) Configures the device to ignore a CoA request to temporarily disable the port hosting a session. The purpose of temporarily disabling the port is to trigger a DHCP renegotiation from the host when a VLAN change occurs and there is no supplicant on the endpoint to detect the change.
Step 12	**authentication command disable-port ignore** **Example:** `Device(config)# authentication command disable-port ignore`	(Optional) Configures the device to ignore a nonstandard command requesting that the port hosting a session be administratively shut down. Shutting down the port results in termination of the session. Use standard CLI or SNMP commands to re-enable the port.
Step 13	**end** **Example:** `Device(config)# end`	Exits global configuration mode an returns to privileged EXEC mode.

Configure RadSec over TLS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *radius-server-name* **Example:** `Device(config)# radius server R1`	Specifies the name for the RADIUS server configuration for Protected Access Credential (PAC) provisioning, and enters RADIUS server configuration mode.
Step 4	**tls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [[**ip** | **ipv6**] {**radius**	Configures the TLS parameters. You can configure the following parameters:

	Command or Action	Purpose

	source-interface *interface-name* |**vrf forwarding** *forwarding-table-name*}] [**match-server-identity** {**email-address** *email-address* | **hostname** *host-name* | **ip-address** *ip-address*}] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name* | **server** *trustpoint name*}] [**watchdoginterval** *interval*]
	Example:
	`Device(config-radius-server)# tls connectiontimeout 10`
	`Device(config-radius-server)# tls idletimeout 75`
	`Device(config-radius-server)# tls retries 15`
	`Device(config-radius-server)# tls ip radius source-interface GigabitEthernet 1/0/1`
	`Device(config-radius-server)# tls ipv6 vrf forwarding table-1`
	`Device(config-radius-server)# tls match-server-identity ip-address 10.1.1.10`
	`Device(config-radius-server)# tls port 10`
	`Device(config-radius-server)# tls trustpoint client TP-self-signed-721943660`
	`Device(config-radius-server)# tls trustpoint server isetp`
	`Device(config-radius-server)# tls watchdoginterval 10`
		• **connectiontimeout**: Configures TLS connection timeout value. The default is 5 seconds.
		• **idletimeout**: Configures the TLS idle timeout value. The default is 60 seconds.
		• **ip**: Configures IP source parameters.
		• **ipv6**: Configures IPv6 source parameters.
		• **match-server-identity**: Configures RadSec certification validation parameters.
		Note This is a mandatory configuration.
		• **port**: Configures the TLS port number. The default is 2083.
		• **retries**: Configures the number of TLS connection retries. The default is 5.
		• **trustpoint**: Configures the TLS trustpoint for a client and a server. If the TLS trustpoint for the client and server are the same, the trustpoint name should also be the same for both.
		• **watchdoginterval**: Configures the watchdog interval. This configuration enables receiving CoA requests on the authentication channel. It also serves as a keepalive to keep the TLS tunnel up, and re-establishes the tunnel if it is torn down.
		Note **watchdoginterval** value must be lesser than **idletimeout**, for the established tunnel to remain up.

Step 5	**end** **Example:** `Device(config-radius-server)# end`	Exits RADIUS server configuration mode and returns to privileged EXEC mode.

Configure Dynamic Authorization for TLS CoA

Note When the **tls watchdoginterval** command is enabled, the client IP configuration under **aaa server radius dynamic-author** command is not used. Instead, the key configured under **radius server** command is used for CoA transactions.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Enters dynamic authorization local server configuration mode and specifies the RADIUS client from which a device accepts CoA and disconnect requests. Configures the device as an AAA server to facilitate interaction with an external policy server.

Step 4	**client {ip-addr | hostname}** [**tls** [**client-tp** *client-tp-name*] [**idletimeout** *idletimeout-interval*] [**server-key** *server-key*] [**server-tp** *server-tp-name*]]
	Example:
	`Device(config-locsvr-da-radius)# client 10.104.49.14 tls idletimeout 100 client-tp tls_ise server-tp tls_client server-key key1`
		Configures the IP address or hostname of the AAA server client. You can configure the following optional parameters:
		• **tls**: Enables TLS for the client.
		  • **client-tp**: Configures the client trustpoint.
		  • **idletimeout**: Configures the TLS idle timeout value.
		  • **server-key**: Configures a RADIUS client server key.
		  • **server-tp**: Configures the server trustpoint.

Step 5	**end** **Example:** `Device(config-locsvr-da-radius)# end`	Exits dynamic authorization local server configuration mode and returns to privileged EXEC mode.

Configure RadSec over DTLS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *radius-server-name* **Example:** `Device(config)# radius server R1`	Specifies the name for the RADIUS server configuration for Protected Access Credential (PAC) provisioning, and enters RADIUS server configuration mode.

Step 4	**dtls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [[**ip** | **ipv6**] {**radius source-interface** *interface-name* |**vrf forwarding** *forwarding-table-name*}] [**match-server-identity** {**email-address** *email-address* | **hostname** *host-name* | **ip-address** *ip-address*}] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name* | **server** *trustpoint name*}]
	Example:
	`Device(config-radius-server)# dtls connectiontimeout 10`
	`Device(config-radius-server)# dtls idletimeout 75`
	`Device(config-radius-server)# dtls retries 15`
	`Device(config-radius-server)# dtls ip radius source-interface GigabitEthernet 1/0/1`
	`Device(config-radius-server)# dtls ipv6 vrf forwarding table-1`
	`Device(config-radius-server)# tls match-server-identity ip-address 10.1.1.10`
	`Device(config-radius-server)# dtls port 10`
	`Device(config-radius-server)# dtls trustpoint client TP-self-signed-721943660`
	`Device(config-radius-server)# dtls trustpoint server isetp`
		Configures DTLS parameters. You can configure the following parameters:
		• **connectiontimeout**: Configures the DTLS connection timeout value. The default is 5 seconds.
		• **idletimeout**: Configures the DTLS idle timeout value. The default is 60 seconds.
		Note When the idle timeout expires, and there are no transactions after the last idle timeout, the DTLS session is closed. When you re-establish the session, restart the idle timer for it to work.
		If the configured idle timeout is 30 seconds, when the timeout expires, the number of RADIUS DTLS transactions are checked. If the RADIUS DTLS packets are more than 0, the transaction counter is reset and the timer is started again.
		• **ip**: Configures IP source parameters.
		• **ipv6**: Configures IPv6 source parameters.
		• **match-server-identity**: Configures RadSec certification validation parameters.
		Note This is a mandatory configuration.

	Command or Action	Purpose
		• **port**: Configures the DTLS port number. The default is 2083. • **retries**: Configures the number of DTLS connection retries. The default is 5. • **trustpoint**: Configures the DTLS trustpoint for the client and the server. If the DTLS trustpoint for the client and server are the same, the trustpoint name should also be the same for both.
Step 5	**end** **Example:** `Device(config-radius-server)# end`	Exits RADIUS server configuration mode and returns to privileged EXEC mode.

Configure Dynamic Authorization for DTLS CoA

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Enters dynamic authorization local server configuration mode and specifies a RADIUS client from which the device accepts CoA and disconnect requests. Configures the device as an AAA server to facilitate interaction with an external policy server.
Step 4	**client {ip-addr | hostname}** [**dtls** [**client-tp** *client-tp-name*] [**idletimeout** *idletimeout-interval*] [**server-key** *server-key*] [**server-tp** *server-tp-name*]] **Example:** `Device(config-locsvr-da-radius)# client 10.104.49.14 dtls idletimeout 100 client-tp tls_ise server-tp tls_client server-key key1`	Configures the IP address or hostname of the AAA server client. You can configure the following optional parameters: • **tls**: Enables TLS for the client. • **client-tp**: Configures the client trustpoint. • **idletimeout**: Configures the TLS idle timeout value.

	Command or Action	Purpose
		• **server-key**: Configures a RADIUS client server key. • **server-tp**: Configures the server trustpoint.

Step 5	**dtls** {{**ip** | **ipv6**} **radius source-interface** *interface-name* | **port** *radius-dtls-server-port-number*}
	Example:
	`Device(config-locsvr-da-radius)# dtls ip radius source-interface GigabitEthernet 1/0/24`
	`Device(config-locsvr-da-radius)# dtls port 100`
		Configures the RADIUS CoA server. You can configure the following parameters:
		• {**ip** | **ipv6**} **radius source-interface** *interface-name*: Specifies the interface for the source address in the RADIUS CoA server.
		• **port** *radius-dtls-server-port-number*: Specifies the port on which the local DTLS RADIUS server listens.

Step 6	**end** **Example:** `Device(config-locsvr-da-radius)# end`	Exits dynamic authorization local server configuration mode and returns to privileged EXEC mode.

Monitor RADIUS

Use the following commands to monitor RADIUS configuration.

Command	Purpose
show aaa servers	Displays information related to AAA RADIUS servers.
show aaa attributes protocol radius	Displays AAA attributes of RADIUS commands.
clear aaa counters servers radius {*server id* | **all**}	Clears the RADIUS TLS-specific or DTLS-specific statistics.
debug radius	Displays information for troubleshooting RADIUS.
debug aaa coa	Displays information for troubleshooting CoA processing.
debug aaa pod	Displays information for troubleshooting POD packets.
debug aaa subsys	Displays information for troubleshooting POD packets.
debug cmdhd [**detail** | **error** | **events**]	Displays information for troubleshooting command headers.

Command	Purpose
debug radius radsec	Enables RADIUS RadSec debugs.