ISG RADIUS Interface

First Published: December 5, 2006

This chapter provides an overview of the Intelligent Services Gateway (ISG) RADIUS interface including available primitives and how they are used.

Overview

ISG offers a standard RADIUS interface that is typically used in a pulled model where the request originates from ISG and the response comes from the queried servers. ISG also supports the RADIUS Change of Authorization (CoA) extensions defined in RFC 5176 that are typically used in a pushed model and allow for the dynamic reconfiguring of services from external authentication, authorization, and accounting (AAA) or policy servers.

A set of well-defined primitives are used by ISG to communicate with external servers. Primitives are abstract representations of interactions across the service access points (SAPs), which indicates the type of information passed between the service gateway and service provider (SP) back-end systems. For examples of order of interaction between the various SAPs, refer to Use Case Scenarios.

The RADIUS interface is by default enabled on ISG. However, some basic configuration is required for the following attributes:

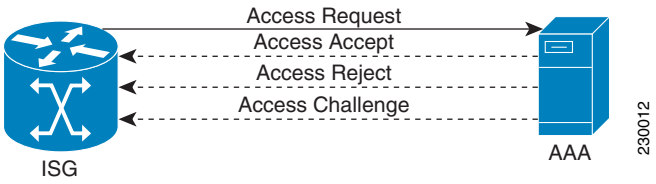
- Security and Password—refer to the “Enabling ISG to Interact with External Policy Servers” chapter in the *Intelligent Services Gateway Configuration Guide*, Cisco IOS Release 15.1S.
- Accounting—refer to the “Configuring ISG Accounting” chapter in the *Intelligent Services Gateway Configuration Guide*, Cisco IOS Release 15.1S.
- Pre-paid—refer to the “Configuring ISG Support for Prepaid Billing” chapter in the *Intelligent Services Gateway Configuration Guide*, Cisco IOS Release 15.1S.

Session Authentication or Authorization

Session authentication requests are generated for user authentication or authorization, typically to a service provider's AAA server. The requests contain session or user credentials such as username and password and the response contain authorization data that includes a user profile listing features and services that are applied to the session.

Figure 1 illustrates a session authentication or authorization request (Access-Request) from an ISG device and the three possible responses that are expected back. Only one of the possible responses is sent back.

Figure 1 Session Authentication Primitives



This section describes the available setup primitives and has the following topics:

Session Authentication or Authorization

A RADIUS Access-Request message is used for session authentication or authorization and implies credentials for verification are carried in the message. This request is automatically sent when a new PPP session is created and where authentication is required. For IP sessions, this request is sent after the session is created and when there is an “authenticate” action command configured on ISG within the session policy. In both cases, the username and password are supplied by the end-user. Refer to Use Case 1 for an example of session authentication.

For IP sessions, Transparent Auto Logon (TAL) can be used for session authorization. An access request is generated when a session identity needs to be verified based on some known identifiers, such as IP-Address or MAC-Address, but an explicit authentication is not required. This request is triggered when there is an “authorize” action command configured on ISG within the session policy. In this case, the username attribute is used to carry a network identifier (MAC, IP Line ID, and such) and the password is ISG supplied within the policy. This eliminates the need for the subscriber to manually enter the username and password. Refer to Use Case 2 for an example of session authorization.

For EAP type authentication, an access request may originate from a downstream device such as an AP or wireless controller and may be proxied by the ISG.

Table 1 lists the standard RADIUS attributes that are commonly associated with a session Access-Request attributes. Cisco uses two types of vendor-specific attributes (VSA); some are defined as Attribute-Value Pair (AVPair) and others that are not AVPair. The table also includes some Cisco vendor-specific AVPair attributes defined in Appendix A.

Table 1 Access-Request Attributes

Attribute/VSA		Type	Value
UserName		1	*<username>* or *<TAL Identifier>*
Password	or	2	*<user password>* or *<Password configured in TAL policy>*
CHAP-Password		3	*<chap challenge/response>*
NAS-IP-Address	or	4	*<ip-address>*
NAS-Identifier		32	*<identifier>* For example, Host Name
NAS-Port		5	*<port>*
Service-Type		6	*<type>* Outbound when common password is used. Framed when user password is used.
Framed-Protocol		7	*<protocol>*
Framed-IP-Address		8	*<ip-address>*
Framed-IP-Netmask		9	*<netmask>*
Calling-Station-ID		31	*<Ethernet Address>*
Acct-Session-ID		44	*<unique ID>*
Event-Timestamp		55	*<time>*
CHAP-Challenge		60	*<challenge>*
NAS-Port-Type		61	*<Ethernet>*
NAS-Port-ID		87	*<value>*

Table 2 lists additional attributes that are included for authentication when Extensible Authentication Protocol (EAP) is employed.

Table 2 Access-Request Attributes (Additional for EAP Deployment)

Attribute/VSA	Type	Value
EAP-Message	79	*<message>*
Message-Authenticator	80	*<signature>*

Session Authentication or Authorization Success

If the credential verification is successful, an Access-Accept response is used to provide the result, which returns the authorization information that is to be applied to the session. This response includes the user profile that contains the applicable service identifiers, service activations, features, and attributes. For an example of Access-Accept for session authentication, refer to Use Case 1, for session authorization, refer to Use Case 2.

Access-Accept

Table 3 shows some of the standard RADIUS attributes commonly associated with a Session Authentication Access-Accept. Additionally, the response will include some Cisco vendor-specific attributes defined in Appendix A.

Table 3 Session Authentication Access-Accept Attributes

Attribute/VSA	Type	Value
Service Type	6	*<service type>*
Reply-Message	18	*<Message>*
Class	25	*<Class>*
Session Timeout	27	*<Absolute Timeout>*
Idle Timeout	28	*<Idle Timeout>*

Session Authentication or Authorization Failure

If the session's credentials cannot be verified, the Access-Reject response indicates failure and might provide the reason for the failure.

Access-Reject

Table 4 lists the Session Authentication Access-Reject attributes.

Table 4 Access-Accept Attributes

Attribute/VSA	Type	Value
Reply-Message	18	*<message>*

Session Authentication Challenge

When EAP authentication is in effect, a back-end server can respond with a challenge. The challenge response is used for multistage EAP protocols, where, after an initial cryptographic exchange similar to EAP-Transport Layer Security (TLS), the simple tunneled EAP protocol is run to completion.

Access-Challenge

Table 5 lists the Session Access-Challenge attributes.

Table 5 Access-Challenge Attributes

Attribute/VSA	Type	Value
Reply-Message	18	*<challenge prompt>*
EAP-Message	79	*<message>*
Message-Authenticator	80	*<signature>*

Service Authentication and Service Profile Download

Service Profile Download is used by ISG to retrieve service definitions from an external server. This process occurs when a new service is activated and that service is not already cached on ISG. Refer to Use Case 1 for an example.

There are two types of scenarios for service authentication. Service authentication can happen after the service profile has been downloaded and identified (within the service profile) that additional authentication is required at a specified server. For auto-logon services, the username and password would be supplied within the user profile and would be used for logging onto the service. Refer to Use Case 3 for an example on how and when this scenario happens.

The second type of service authentication can happen when a user selects a new service at a portal and is required to enter a username and password to access that service. In this case, the username and password will be conveyed within a "CoA Request:Service Activate" described later in this document.

Figure 2 illustrates a service authentication or service profile download (Access Request) from an ISG device, and the two possible responses that are expected back. Only one of the possible responses is sent back.

Figure 2 Service Authentication or Service Profile Download

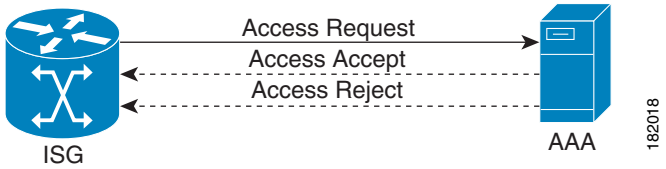


Table 6 lists the Service Authentication and Service Profile Download Access-Request attributes and contains some Cisco vendor-specific AVPair attributes as defined in Appendix A.

Table 6 Service Authentication or Service Profile Download Access-Request Attributes

Attribute/VSA	Type	Value
UserName	1	<*service name*> for Service Profile Download or <*username*> for Service Authentication
Password	2	<*ISG configured*> for Service Profile Download or <*user password*> for Service Authentication
NAS-IP-Address	4	<*ip-address*>
NAS-Port	5	<*value*>
Service-Type	6	<*Outbound*> for Service Profile Download <*Framed*> for Service Authentication
Calling-Station-ID	31	<*MAC address* or other >
NAS-Identifier	32	<*identifier*>
Acct-Session-ID	44	<*session-ID*>
Event-Timestamp	55	<*value*>
NAS-Port-Type	61	<*Ethernet* or *ATM*>
NAS-Port-ID	87	<*value*>

Service Profile Download Success

If the service profile can be retrieved, the server responds with Access Accept. The service profile contains service attributes such as traffic class, policing rate, and accounting information which can be any of the Cisco vendor-specific AVPair attributes and any of the Cisco vendor-specific non-AVPair attributes of type service-information. Refer to Appendix A.

Service Authentication Success

If the user service credentials are verified, the system prompt indicates success and may contain additional applicable attributes.

Service Authentication or Service Profile Download Failure

If the configuration authentication request cannot be verified, the system responds with an Authentication Failure message. The reason of the failure can be encoded using attribute 18.

Change-of-Authorization Requests

Change of Authorization (CoA) requests, as described in RFC 5176, are used in a push model to allow for dynamic activation and de-activation of service, session query, feature push, account logon, and session termination. The model is comprised of one request and two possible response codes:

- Change-of-Authorization Requests [CoA-Request]
- CoA ACK [CoA-ACK]
- CoA NAK [CoA-NAK]

The request is initiated from a CoA client (typically a RADIUS or policy server) and directed to the ISG that acts as a listener. This section includes the following topics:

- CoA Request Response Code
- CoA ACK Response Code
- CoA NAK Response Code

RFC 5176 Compliance

RFC 5176 describes two methods of authorization, including a standard set of messages where the requests are directly responded to by using the packet codes for ACK and NAK, which is the supported interface in Cisco IOS software.

- For Diameter compatibility, RFC 5176 suggests the use of a Pull mechanism for CoA via the Authorize-Only service-type attribute value; however, this mechanism is unsupported by Cisco IOS software.
- For security, RFC 5176 mentions the use of IPSec, which is supported in Cisco IOS software. The prevention of replays without IPSec, via the Event-Timestamp attribute, is not supported.

- The Disconnect Request message as specified in RFC 5176, which is also referred to as Packet of Disconnect (POD), is supported by ISG for the termination of PPP sessions only. Use the CoA Request: Account Logoff primitive described later in this section to terminate ISG sessions from a remote terminal.
- RFC 5176 describes the use of a State Attribute. This attributed is not supported.
- RFC 5176 describes the use of a Proxy-State Attribute. This attributed is not supported.

Note Sending an encrypted User Password attribute within a CoA message requires special considerations. See the "Account Logon" section on page 1-11 for more information.

Preconditions

When using the CoA interface, you must assume that a session or service target already exists on the device. CoA can be used to modify features (traffic policies) on a session or to apply new features on a session. The update only affects only the subject's parent session, not the active services. For example, you cannot change active services or on-box service definitions, however, you can deactivate an existing service or activate a new one.

CoA Request Response Code

This section describes primitives and attributes used for the CoA Request feature. The CoA Request response code is used as a "Feature Push" to add or modify feature to a parent session. The CoA Request response code can also be used to convey a command to ISG. The supported commands are listed in Table 7.

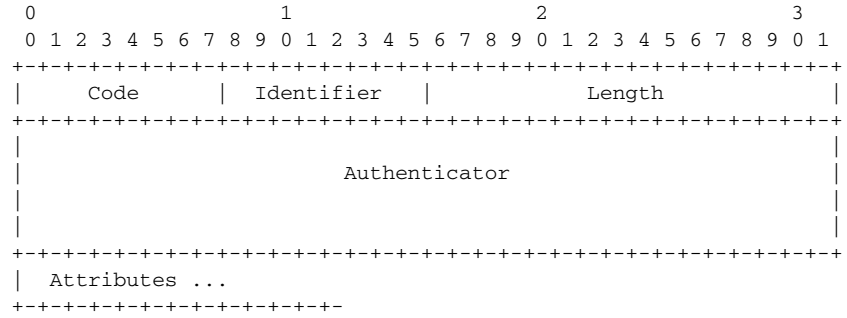
To target a session, either one of the following session identifier can be used:

- Client's IP address (encoded as non-AVPair Account-Info attribute "S")
- Session's PBHK Identifier (encoded as non-AVPair Account-Info attribute "S")
- Session Account-Session-Id using RADIUS attribute 44 (requires CSCek31466).

To target a service, the following service identifier must be used:

- Service Name (encoded as non-AVPair Service-Info attribute "N")

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 VSAs. For "Feature Push", no CoA command code is used, hence only the VSAs are included in the CoA Request.

For CoA command, sub-attribute 252 is used to carry the Command code. The command codes can be encoded in binary or in ASCII.

Table 7 lists the CoA commands that are supported on ISG:

Table 7 CoA Commands Supported on ISG

Command[1]	Code	Value	Binary Command Code examples	ASCII Command Code Examples
Account Logon[2]	1	<*username*>	vsa cisco 252 command-code = 01	vsa cisco generic 1 string "subscriber:command=account-logon"
Account Logoff	2	<*username*>	vsa cisco 252 command-code = 02	vsa cisco generic 1 string "subscriber:command=account-logoff" [3]
Session Query	4			[3]
(for service info)		' ' (*space*)	vsa cisco 252 command-code = 04 20	vsa cisco generic 1 string "subscriber:command=account-status-query"
(for Complete ID)		'&' (*ampersand*)	vsa cisco 252 command-code = 04 26	vsa cisco generic 1 string "subscriber:command=profile-status-query"
(for both)		' &' (*space-ampersand*)	vsa cisco 252 command-code = 04 20 26	vsa cisco generic 1 string "subscriber:command=account-profile-status-query"
Session Query for Service Status	4	<*service name*>[4]	vsa cisco 252 command-code = 04 <service name>	vsa cisco generic 1 string "subscriber:command=service-status-query"
Service Activate	11	<*service name*>[4]	vsa cisco 252 command-code = 0B <service name>	vsa cisco generic 1 string "subscriber:command=activate-service"
Service Deactivate	12	<*service name*>[4]	vsa cisco 252 command-code = 0C <service name>	vsa cisco generic 1 string "subscriber:command=deactivate-service"

1. All CoA commands must include the session identifier between ISG and the CoA client. This is usually the client's IP address, or when PBHK is used, the ISG IP address followed by a port number. The session identifier is sent as a separate VSA, for example: vsa cisco 250 account-info = S10.10.10.11:85
2. See the "Account Logon" section on page 1-11 for information about the required format of the user-password.
3. For Account-logoff and Session Query sent in ASCII format, the username attribute must be included even if attribute value is blank.
4. When a hexadecimal command code format is used, the service name is appended immediately after the command code but when an ASCII command code format is used, the service name is sent as a separate attribute:

. vsa cisco generic 1 string "subscriber:service-name=service_name"

CoA ACK Response Code

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

CoA NAK Response Code

A negative acknowledgement (NAK) indicates a failure to change the authorization state and can include attributes that indicate the reason for the failure. If you push multiple traffic policies, the NAK cannot specify which CoA has failed. Currently, the only way you can verify a successful CoA is by using show commands. Table 8 shows CoA NAK attributes.

Table 8 CoA-NAK Attributes

Attribute/VSA	Type	Value
UserName	1	*<username>*
ErrorCause <error cause>		*<error cause>*
Reply-Message 18 <message>	18	*<message>*

Feature Push

A "Feature Push" is used to modify the parent session only and cannot be used to change features or traffic policies on a service.

The "Feature Push" allows overriding the feature instance and adding new features not already configured. However, you cannot remove a newly added traffic policy; therefore, one must use a service container to do that. Deactivating a service allows for the removal of a traffic policy. Incomplete policy definitions can result in a NAK message (an application can then decide to terminate a session).

A "Feature Push" has no command code. A "Feature Push" contains the session identifier and Cisco VSA related to features to be added or modified. Refer to Use Case 1 for an example on how a "Feature Push" is used.

ISG Commands that Use CoA Requests

The following sections describe the CoA Request commands that provide specific capabilities for using ISG sessions.

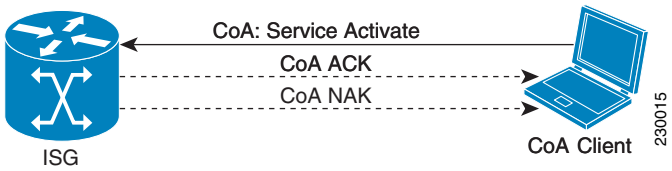
- Service Activate
- Service Deactivate
- Activating and Deactivating Multiple Services
- Account Logon
- Account Logoff
- Session Query
- Session Query for Service Status

Service Activate

You can use the Service Activate interface to activate a service for the identified session. The parameters include the session identification attributes and the name of the service you want to activate. For services that require authentication, these requests can also include a username and an authorization password for the service.

Figure 3 illustrates a service activation request from the CoA client and the two possible response from ISG (only one sent back).

Figure 3 CoA-Request; Service Activate



If the ISG receives a request to activate a service that is not already cached on the device, the ISG downloads the appropriate profile for the service (see Service Profile Download).

If the service requires further authentication, the ISG will attempt to authenticate the user to a specified RADIUS server (see Service Authentication).

The RADIUS server is specified in the service profile (referenced in a method-list attribute within the service profile: subscriber:policy-directive = authenticate aaa-method-list service-list) with the username and password from the CoA Request.

The service edge device provides a notification as to whether the service activation was successful or not successful. If the service activation is successful, and if the service required authentication, this response can also include any additional attributes that further describe the per subscriber behavior for that service.

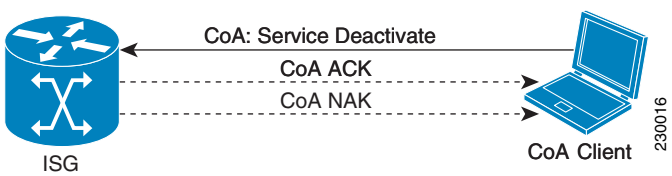
If the service activation is not successful, an error code (which identifies the failure mode) is also returned. (For RADIUS, this error code is sent as an Error Message Code VSA - Command-Code.) Refer to user case 2 for an example on how to use Service Activate.

Service Deactivate

You can use the Service Deactivate interface to deactivate a service on a session. The service edge device sends a reply to acknowledge receipt of this message and the result of the deactivation process.

Table 5 illustrates a service deactivation request from the CoA client and the two possible responses from ISG (only one sent back).

Figure 4 CoA-Request, Service Deactivate



Refer to Use Case 2 for an example on how to use the Service Deactivate message.

Activating and Deactivating Multiple Services

You can use the Service Activate and Deactivate interface to activate and deactivate multiple services in a single CoA-Request message. A CoA-Request message can have more than one service activation and deactivation request.

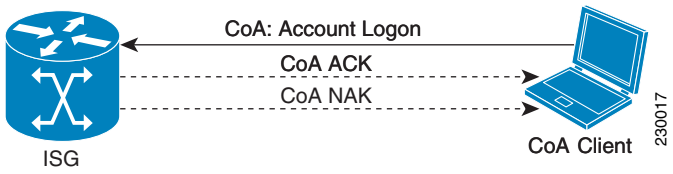
Note Text-based commands are not supported for multiple-service activation and deactivation in a single CoA message. Only binary commands are supported for multiple-service activation and deactivation in a single CoA message.

Account Logon

An Account Logon request is often sent from a portal to trigger an account-logon event on ISG. (The account-logon event is generally used by ISG as a signal to authenticate a new session.) The Account Logon request contains the user credentials that were collected at the portal. Refer to Use Case 1 for an example of how account logon is used.

Figure 5 illustrates an Account Logon request being sent from the CoA client and the two possible responses from ISG (only one of which is sent back).

Figure 5 CoA-Request: Account Logon

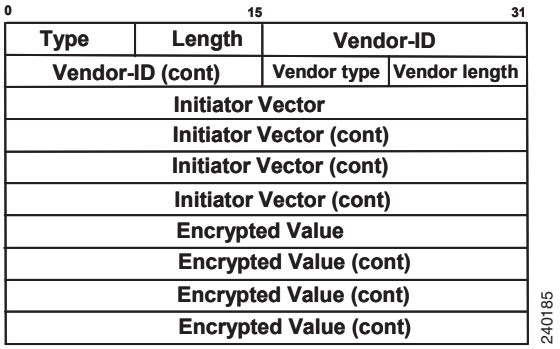


CoA messages (as specified by RFC 5176) use the message authenticator format of RADIUS Accounting messages; not the format of RADIUS Access messages. The CoA request authenticator is calculated as a hash of length and data inside the entire packet, which means it requires an encrypted password, whereas the User-Password attribute is calculated as a hash of plain text password, shared secret, and request authenticator, which means it requires a request authenticator. Carrying an encrypted password attribute in a CoA message using standard RADIUS attribute 2 will create a cyclic dependency and is therefore not possible.

The User-Password must use the format of Cisco VSA 249 as detailed in Figure 6. Cisco VSA 249 has an initiator vector and an encrypted password. The initiator vector is a 16-octet pseudo-random number uniquely generated for each attribute. The encrypted value field is 16 or more octets containing data that is length-prefixed and zero padded to an even multiple of 16 octets.

Note Do not use US-ASCII to encrypt the data length and the encoding from a string to bytes. You must use encoding that uses character set ISO8859-1.

Figure 6 Format of Cisco VSA 249



Password Example

The following example shows how to create a valid account logon.

Step 1 Construct a plain text version of the string field by concatenating the Data-Length and Password sub-fields:

- If necessary, pad the resulting string until its length (in octets) is an even multiple of 16. We recommend using zero octets (0x00) for padding to obfuscate the password length.
- Prefix the password with its length (raw, not ASCII) and pad to a multiple of 16 bytes; not to an even multiple of 16. In this example, the plain text string is P and the password is web:

  P = 0x03 + web (in hex bytes: 03 77 65 62 00 00 00 00 00 00 00 00 00 00 00 00)

Step 2 Break the clear text string P into chunks of up to 16-octets each, for example, p1, p2. The last chunk can contain fewer than 16 octets if no padding is used.

In this example, the shared secret is S, and the pseudo-random 128-bit initiator vector is I.

S = cisco

I = IIIIIIIIIIIIIIII (in hex bytes: 49 49 49 49 49 49 49 49 49 49 49 49 49 49 49 49)

The cipher text blocks are c(1), c(2), and so on. The intermediate values are b1, b2, and so on.

b1 = MD5 (cisco + IIIIIIIIIIIIIIII) = b4 04 ba b5 24 cb 6d f6 60 5e 21 ae e9 37 9d 26

b1 = MD5 (S + I) c(1) = p1 XOR b1

b2 = MD5 (S + c(1)) c(2) = p2 XOR b2

bi = MD5 (S + c(i-1)) c(i) = pi XOR bi

Step 3 The resulting encrypted value will contain c(1)+c(2)+...+c(i) where + denotes concatenation.

c(1) = p1 XOR b1

p1 03 77 65 62 00 00 00 00 00 00 00 00 00 00 00 00

XOR

b1 b4 04 ba b5 24 cb 6d f6 60 5e 21 ae e9 37 9d 26

---

c(1) = b7 73 df d7 24 cb 6d f6 60 5e 21 ae e9 37 9d 26

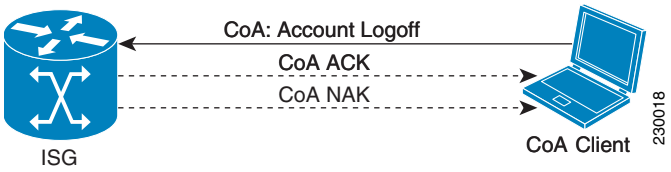
VSA 249 value = 49 49 49 49 49 49 49 49 49 49 49 49 49 49 49 49 b7 73 df d7 24 cb 6d f6 60 5e 21 ae e9 37 9d 26

Account Logoff

An account logoff is used to remove a session on the service gateway from a remote server. This can be done for administrative reasons, if the user disconnects from a portal or if for example, pre-paid is implemented outside of ISG. Refer to Use Case 1 for an example on how an account logoff is used.

Figure 7 illustrates an Account Logoff request from the CoA client and the two possible responses from ISG (only one sent back).

Figure 7 CoA-Request; Account Logoff



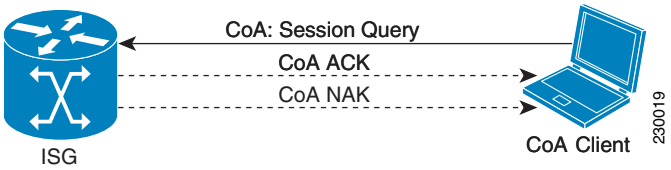
Session Query

Use the Session Query CoA command to request session information. There are three different ways to encode a Session Query:

- A ' ' (space) after the command code instructs ISG to return service information for a particular session.
- An '&' (ampersand) after the command code instructs ISG to return session information known as the session's “Complete ID”.
- A ' &' (space followed by ampersand) combines the two. ISG is instructed to return both the Complete ID and service information.

Figure 8 illustrates CoA-Request, Session Query from the CoA client.

Figure 8 CoA-Request, Session Query



When the Query VSA is encoded with a single space character, the system response to the session query returns full details about each active user service. The current returned parameters include the duration of an active service and the packet and byte counts for data moving to and from the service network. The VRF in use might be returned if the service is not tunnel-based. An absence of a VRF indicates that a tunnel-based service is in use when a primary service status is being returned.

The status of each active service is returned embedded within a Service Name VSA, which has the format indicated in Table 9.

Table 9 Service Name VSA Format

Attribute/VSA	Type	Value
Service Name VSA	9, 250 Account-Info	N;1;<*service name*>;<elapsed time (secs)>; <*username*>;<*downstream pkts*>; <*upstream pkts*>;<*downstream* i>; <*upstream bytes*>;<*VRF ID*>

When the Query VSA is encoded with an ampersand character, the session's profile and the information that relates to the session's complete ID is returned to the client. The complete ID fields are used to identify a session. The complete ID fields include valid fields (such as the IP address, MAC address, PBHK-id, VPI/VCI, circuit-id, remote-id, MSISDN or subinterface).

The RADIUS complete ID field uses the standard attributes (1 and 8) for username and IP address, respectively. The additional ID fields are sent as Account-Info VSA subattributes. These subattributes have the Complete ID value of "$" followed by other characters, which represent the ID type (for example, MA indicates MAC address, SI indicates subinterface, and VP indicates VPI/VCI) followed by the ID string. The RADIUS complete ID field attributes are listed in Table 10.

Table 10 RADIUS Complete ID Field Attributes

Attribute/VSA	Type	Value
Complete ID VSA (MAC)	9, 250 Account-Info	$MA<*MAC address*>
Complete ID VSA (sub interface)	9, 250 Account-Info	$SI<*sub interface*>
Complete ID VSA (VPI/VCI)	9, 250 Account-Info	$VP<*VPI/VCI*>

When the Query VSA is encoded with both a space and an ampersand character, all informative listed above is returned. Refer to Use Case 1 for an example on how a Query VSA is used.

A successful RADIUS response is sent as a CoA-ACK and returns the Query VSA attribute appended with a value of "1" if session is authenticated and a value of "0" for other sessions (for example a session not yet authenticated or for authorized sessions). Additional attributes normally found in user profile are appended.

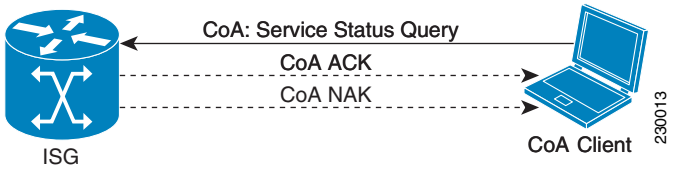
If the session identifier does not refer to a valid session, the ISG returns an error message. With RADIUS, this failure is returned in a CoA-NAK, and the returned Query VSA contains the appended value of "0".

Session Query for Service Status

You can use the Session Query for Service Status interface to determine the current state of a service on a given session. The returned information includes the active duration of the service.

Figure 9 illustrates a request for a service status from the CoA client.

Figure 9 CoA-Request; Service Status Query



CoA-Request; Service Status Query

The ISG device replies to the CoA-Request; Session Query for Service Status with either a CoA ACK or CoA NAK.

If the session and service are active, the ISG device returns the Query VSA with a value of "1" within the CoA-ACK message, and the service status is appended after the service name (within a Service Name VSA). A "1" indicates that the service is active and is followed by the amount of time the service has been up.

This attribute is formatted as shown in Table 11.

Table 11 CoA-Request, Service Status Query Format

Attribute/VSA	Type	Value
Query VSA	9, 250 Command-Code	4"1"
Subscriber IP VSA	9, 250 Account-Info	S<IP[:port]>
Service Name VSA	9, 250 Account-Info	N"1"<*servicename*>;<*elapsed time (secs)*>;username

Refer to Use Case 1 for an example on how a CoA Service Status Query is used.

If the session is active but not the service, ISG returns the Query VSA with a value of "1' within the CoA-ACK message and the service is appended after the service name (within a Service Name VSA). A "0" indicates that the service is inactive as shown in Table 12.

Table 12 ISG Aware/Session Service not Active

Attribute/VSA	Type	Value
Query VSA	9, 252 Command-Code	4"1"
Subscriber IP VSA	9, 250 Account-Info	S<IP[:port]>
Service Name VSA	9, 250 Account-Info	N"0"<*servicename*>

If the request is not successful and the ISG is not aware of the session, the ISG returns the Query VSA attribute with a value of "0" appended in a CoA-NAK message as shown in Table 13.

Table 13 CoA-Request, Service Status Query Unsuccessful

Attribute/VSA	Type	Value
Query VSA	9, 250 Command-Code	4"0"
Subscriber IP VSA	9, 250 Account-Info	S<IP[:port]>

Accounting

Session and service activation states are reported through Accounting Request attributes that are sent at the session start and the session stop and also through interim accounting. You can control the frequency of these requests using the standard **aaa accounting update** {*newinfo* | *periodic number*} command configuration, or by using the IETF standard attribute Acct-Interim-Interval, or the Cisco AVPair acct-interval.

Prerequisites

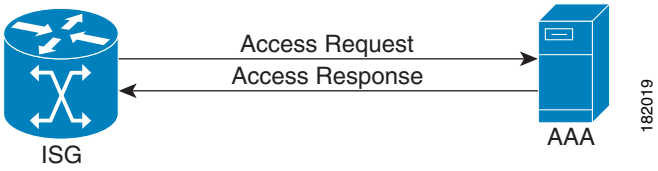
With these interfaces, the assumption is that a session or service is up, authentication has already taken place, and a policy governs the method-list to be used for accounting.

This section includes the following topics:

- Session Accounting
- Service Accounting

Figure 10 illustrates an accounting request to the AAA server.

Figure 10 Accounting Request/Response



Session Accounting

Session accounting is used to report information about a session's state.

Three different Acct-Status-Types are used to gather session information:

- Session Accounting-Start
- Session Accounting-Stop
- Session Accounting-Interim
- Session Accounting Response

If the accounting request is successful, the AAA server responds with a positive acknowledgement for the specified accounting request (refer to the “Session Accounting Response” section).

Session Accounting-Start

The start request indicates the session has begun and is ready for data traffic. Refer to Use Case 1 to see how a Session Accounting Start is used. Table 14 shows the Acct-Status-Start attributes.

Table 14 Acct-Status - Start Attribute

Attribute/VSA	Type	Value
UserName	1	*<username>*
NAS-IP-Address	4	*<nasip>*
NAS-Port	5	*<port>*
Service-Type	6	Framed
Framed-Protocol	7	PPP
Framed-IP-Address	8	*<ip-address>*
Cisco VSA for session-id	9,250	S*<IP_addr>*:*<portbundle>*
NAS-Identifier	32	*<value>*
Acct-Status-Type	40	Start
Acct-Delay-Time	41	*<value>*
Acct-Session-Id	44	*<session-Id>*
NAS-Port-Type	61	*<type>*
NAS-Port-ID	87	*<id>*

Session Accounting-Stop

The Stop request indicates that the session has terminated and additional data traffic is not allowed. Refer to Use Case 1 to see how an Accounting Stop is used.

Table 15 shows the Acct-Status-Stop attributes.

Table 15 Acct-Status - Stop Attributes

Attribute/VSA	Type	Value
UserName	1	*<username>*
NAS-IP-Address	4	*<nasip>*
NAS-Port	5	*<port>*
Service-Type	6	Framed
Framed-Protocol	7	PPP
Framed-IP-Address	8	*<ip-address>*
Cisco-AVPair	9, 1	disc-cause-ext=*<value>*
Cisco VSA for session-id	9,250	S*<IP_addr>*:*<portbundle>*
Control-Info	9, 253	I*<value>*
Control-Info	9, 253	O*<value>*
NAS-Identifier	32	*<value>*

Table 15 Acct-Status - Stop Attributes

Attribute/VSA	Type	Value
Acct-Status-Type	40	Stop
Acct-Delay-Time	41	<*value*>
Acct-Input-Octets	42	<*value*>
Acct-Output-Octets	43	<*value*>
Acct-Session-Id	44	<*session-Id*>
Acct-Session-time	46	<*value*> (secs)
Acct-Input-Packets	47	<*value*>
Acct-Output-Packets	48	<*value*>
Acct-Terminate-Cause	49	<*value*>
NAS-Port-Type	61	<*type*>
NAS-Port-ID	87	<*id*>

Session Accounting-Interim

The Interim requests are used to send cumulative counters since session start and new information, such as a change in an IP address.

Session Accounting Response

If the session accounting request is successful, the AAA server responds to the ISG device with a positive acknowledgment for the specified accounting request.

Service Accounting

Service accounting is used to report information about a service's state.

Three different Acct-Status-Types are used to gather service information:

- Service Accounting-Start
- Service Accounting-Stop
- Service Accounting-Interim
- Service Accounting Response
- Prepaid Accounting
- Prepaid Accounting Response
- Class-Based Accounting

If the accounting request is successful, the AAA server responds with a positive acknowledgement for the specified accounting request (refer to the “Service Accounting Response” section).

Service Accounting-Start

The start request indicates that the service is configured and is ready to pass data traffic. Refer to Use Case 1 for an example of how a Service Accounting Start is used.

Table 16 shows the Acct-Status-Start attributes.

Table 16 Acct-Status-Start Attributes

Attribute/VSA	Type	Value
username	1	<*username*>
NAS-IP-Address	4	<*nasip*>
NAS-Port	5	<*port*>
Service-Type	6	Framed
Framed-Protocol	7	PPP
Framed-IP-Address	8	<*ip-address*>
Cisco VSA for session-id	9,250	S<*IP_addr*>:<*portbundle*>
Service-Info	9, 251	N<*service-name*>
Parent-Session-ID	26, 9, 1	parent-session-id=<*id*>
Acct-Status-Type	40	Start
Acct-Delay-Time	41	<*value*>
Acct-Session-Id	44	<*session-Id*>
NAS-Port-Type	61	<*type*>
NAS-Port-ID	87	<*id*>

Service Accounting-Stop

The Stop request indicates that the service has terminated and additional data traffic is not allowed. Refer to Use Case 1 for an example of how a Service Accounting Start is used.

Table 17 shows the Acct-Status-Stop attributes.

Table 17 Acct-Status-Stop Attributes

Attribute/VSA	Type	Value
Username	1	<*username*>
NAS-IP-Address	4	<*nasip*>
NAS-Port	5	<*port*>
Service-Type	6	Framed
Framed-Protocol	7	PPP
Framed-IP-Address	8	<*ip-address*>
Service-Info	9, 251	N<*service-name*>
Cisco-AVPair	9, 1	disc-cause-ext=<*value*>
Cisco VSA for session-id	9,250	S<*IP_addr*>:<*portbundle*>

Table 17 Acct-Status-Stop Attributes

Attribute/VSA	Type	Value
Control-Info	9, 253	I<*value*>
Control-Info	9, 253	O<*value*>
Parent-Session-ID	26, 9, 1	parent-session-id=<*id*>
NAS-Identifier	32	<*value*>
Acct-Status-Type	40	Start
Acct-Delay-Time	41	<*value*>
Acct-Input-Octets	42	<*value*>
Acct-Output-Octets	43	<*value*>
Acct-Session-Id	44	<*session-Id*>
Acct-Session-time	46	<*value*> (secs)
Acct-Input-Packets	47	<*value*>
Acct-Output-Packets	48	<*value*>
Acct-Terminate-Cause	49	<*value*>
NAS-Port-Type	61	<*type*>
NAS-Port-ID	87	<*id*>

Service Accounting-Interim

The Interim requests are used to send cumulative counters since session start and new information that is related to the service.

Service Accounting Response

If the service accounting request is successful, the AAA server responds to the ISG device with a positive acknowledgement for the specified accounting request.

Prepaid Accounting

The prepaid accounting message indicates the quota usage. Table 18 shows the Prepaid Accounting-Request attribute.

Table 18 Prepaid Accounting-Request Attribute

Attribute/VSA	Type	Value
UserName	1	<*username*>

Prepaid Accounting Response

The prepaid accounting response is an acknowledgement from the AAA server, indicating receipt of the request. Table 19 shows the Prepaid Account-Response attribute.

Table 19 Prepaid Account-Response Attributes

Attribute/VSA	Type	Value
None		

Class-Based Accounting

Class-based accounting messages include information that pertains to traffic matching a modular QoS CLI (MQC) class-map.

Quota Reauthorizations

When services are paid for in advance, the Quota Reauthorizations feature is used to ensure that the delivered service is within the credit limits.

There are two types of quota reauthorizations:

- Basic Quota Reauthorizations-Includes information that accounts for the differing tariff rates across a tariff boundary. Tariff rates are set in accordance with the time of day.
- Quota with Tariff switching-No tariff boundary exists.

Service credit is allotted in fragments, or quotas, that can be allocated to the user.

There are two types of credit quotas:

- Time-based quota in seconds, as indicated in the SSG Control Info attribute (QT).
- Volume-based quota in bytes, as indicated in the SSG Control Info attribute (QV).

When a quota allotment expires, or when usage crosses the configured threshold, reauthorization events are generated.

Precondition

When you use this interface, you must assume that a session or service target already exists on the device. Reauthorization events can be controlled by means of the prepaid feature configuration. Also, an assumption is made that an initial authorization has been done to ensure that the prepaid feature is allowed for a particular service instance on a session.

Basic Quota Reauthorization

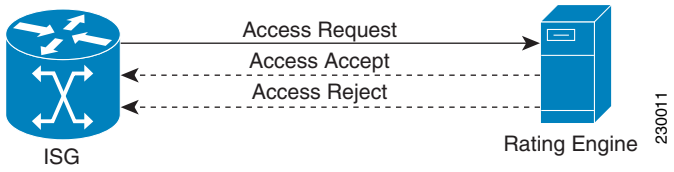
For basic prepaid services, three types of reauthorization requests are available:

- Quota Expiry
- Idle-Timer Expiry
- Time Quota Expires During Idle State

When the attributes Control-Info QT and Control-Info QV are included in the reauthorization request, the quota values include the cumulative total, from the beginning of the service.

In all cases, the reauthorization requests takes the form of an Access-Request followed by either an Access-Accept or Access-Reject as shown in Figure 11.

Figure 11 Quota Reauthorization Access-Request



Quota Expiry

If either of the quotas is depleted or is close to depletion, a reauthorization message is sent to the server (rating engine). Table 20 lists the Access-Request attributes for the Quota Expiry primitive.

Table 20 Access-Request Attributes for Quota Expiry

Attribute/VSA	Type	Value
VolumeQuota	9, 253 Control-Info	*QV<value>*
TimeQuota	9, 253 Control-Info	*QT<value>*

Idle-Timer Expiry

If the idle-timer expires, the system initiates a reauthorization message to allow the quota to be reclaimed for an idle service, which is then granted an active service. Table 21 lists the Access-Request attributes for the idle-timer expiry primitive.

Table 21 Access-Request Attributes for Idle-Timer Expiry

Attribute/VSA	Type	Value
VolumeQuota	9, 253 Control-Info	*QV<value>*
TimeQuota	9, 253 Control-Info	*QT<value>*
PrepaidReauthReason	9, 253 Control-Info	*QR1*

Time Quota Expires During Idle State

This section describes how the system responds if a time quota expires while the service is in an idle state. If a time quota expires while the service is in an idle state, the following attributes are used. Table 22 lists the Access-Request attributes for the time-quota-expiry primitive.

Table 22 Access-Request Attributes for Time-Quota-Expiry

Attribute/VSA	Type	Value
VolumeQuota	9, 253 Control-Info	*QV<value>*
TimeQuota	9, 253 Control-Info	*QT<value>*
PrepaidReauthReason	9, 253 Control-Info	*QR0*

Basic Quota Reauthorization Success

If the rating engine is able to allocate new quotas, an Access-Accept is returned from the server rating engine. Table 23 lists the Access-Accept attributes for the time-quota-expiry primitive.

Table 23 Access-Request Attributes for Time-Quota-Expiry

Attribute/VSA	Type	Value
VolumeQuota	9, 253 Control-Info	*QV<value>*
TimeQuota	9, 253 Control-Info	*QT<value>*
Idle-Timeout	28	*<idle-timeout>*

Basic Quota Reauthorization Failure

If the rating engine cannot allocate new quotas, an Access-Reject failure message is sent from the server rating engine.

Quota with Tariff Switching

This section describes Quota with Tariff Switching primitives, and includes the following topics:

- Overview
- PT Quota Expiration
- PT Idle-Timer Expiration
- Time Quota Expiration During Idle State
- Post Tariff Reauthorization Success
- Post Tariff Reauthorization Failure

Overview

The basic quota requests, along with tariff switch epochs, form a two-dimensional matrix of primitives that are based on either Pre-switch or Post-switch reauthorization requests.

There are six primitives:

- Pre-switch reauthorization requests
  - Quota expiry
  - Idle-timer expiry
  - Time quota expiry while the service is idle

  Pre-switch reauthorization primitives are functionally equivalent to the basic quota primitives and are not considered separate primitives.
- Post-switch reauthorization requests
  - Quota expiry
  - Idle-timer expiry
  - Time quota expiry while the service is idle

  Post-switch reauthorization primitives differ from the basic quota primitives because they might contain quota usage information received after the tariff epoch.

PT Quota Expiration

When a quota expires after the Tariff switch epoch, an Access-Request is sent for a pre-switch reauthorization request. Table 24 lists the Access-Request attributes for the PT Quota Expiry primitive.

Table 24 Access-Request Attributes for PT Quota Expiry

Attribute/VSA	Type	Value
VolumeQuota	9, 253 Control-Info	*QV<value>*
TimeQuota	9, 253 Control-Info	*QT<value>*
QuotaPostSwitch	9, 253 Control-Info	*QB<bytes used since switch>*

PT Idle-Timer Expiration

If the idle-timer expires for a post-tariff (PT) epoch, the system initiates a reauthorization message to allow the quota to be reclaimed for an idle service, which is then granted an active service. Table 25 lists the Access-Request attributes for the PT Idle-Timer Expiry primitive.

Table 25 Access-Request Attributes for PT Idle-Timer Expiry

Attribute/VSA	Type	Value
VolumeQuota	9, 253 Control-Info	*QV<value>*
TimeQuota	9, 253 Control-Info	*QT<value>*
QuotaPostSwitch	9, 253 Control-Info	*QB<bytes used since switch>*
PrepaidReauthReason	9, 253 Control-Info	*QR1*

Time Quota Expiration During Idle State

This section describes how the system responds if a PT time quota expires while the service is in an idle state.

Table 26 lists the Access-Request attributes for the PT Time-Quota-Expiry primitive.

Table 26 Access-Request Attributes for PT Time-Quota-Expiry

Attribute/VSA	Type	Value
VolumeQuota	9, 253 Control-Info	*QV<value>*
TimeQuota	9, 253 Control-Info	*QT<value>*
PrepaidReauthReason	9, 253 Control-Info	*QR0*

Post Tariff Reauthorization Success

If the rating engine can allocate new quotas, the rating engine responds with a PT Reauthorization Access-Accept message.

Table 27 lists the Access-Accept attributes for the PT Reauthorization Success message.

Table 27 Access-Accept Attributes for TPT Reauthorization Success

Attribute/VSA	Type	Value
VolumeQuota	9, 253 Control-Info	*QX<seconds>;<bytes>;<bytes>*
TimeQuota	9, 253 Control-Info	*QT<value>*
Idle-Timeout	28	*<idle-timeout>*

Post Tariff Reauthorization Failure

If the rating engine cannot allocate new quotas, the rating engine responds with a PT Reauthorization Failure, Access-Reject message.

Monitoring and Troubleshooting ISG CoA Functionality

The following Cisco IOS commands can be used to monitor and troubleshoot ISG CoA functionality on the router:

- **debug radius**
- **debug aaa coa**
- **debug aaa pod**
- **debug aaa subsys**
- **show aaa attributes protocol radius**