RADIUS Attributes Configuration Guide, Cisco IOS Release 15M&T

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CONTENTS

CHAPTER 1

RADIUS Attributes Overview and RADIUS IETF Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are used to define specific authentication, authorization, and accounting (AAA) elements in a user profile, which are stored on the RADIUS program. This chapter lists the RADIUS attributes that are supported.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

RADIUS Attributes Overview

IETF Attributes Versus VSAs

RADIUS Internet Engineering Task Force (IETF) attributes are the original set of 255 standard attributes that are used to communicate AAA information between a client and a server. The IETF attributes are standard and the attribute data is predefined. All clients and servers that exchange AAA information using IETF attributes must agree on attribute data such as the exact meaning of the attributes and the general bounds of the values for each attribute.

RADIUS vendor-specific attributes (VSAs) are derived from a vendor-specific IETF attribute (attribute 26). Attribute 26 allows a vendor to create an additional 255 attributes; that is, a vendor can create an attribute that does not match the data of any IETF attribute and encapsulate it behind attribute 26. The newly created attribute is accepted if the user accepts attribute 26.

For more information on VSAs, refer to the chapter “RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values.”

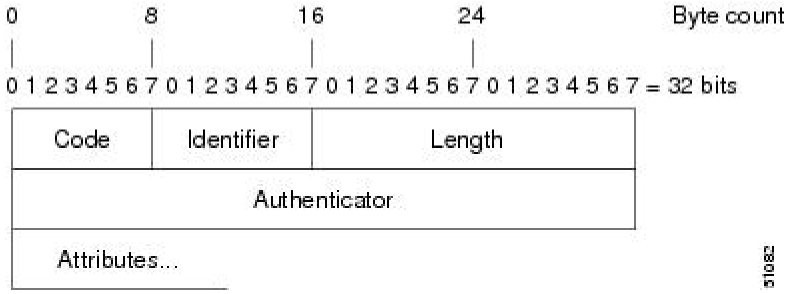
RADIUS Packet Format

The data between a RADIUS server and a RADIUS client is exchanged in RADIUS packets. The data fields are transmitted from left to right.

The figure below shows the fields within a RADIUS packet.

Note For a diagram of VSAs, refer to Figure 1 in the chapter “RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values.”

Figure 1: RADIUS Packet Diagram


0
8
16
24
Byte count
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 = 32 bits
Code
Identifier
Length
Authenticator
Attributes...
51082

Each RADIUS packet contains the following information:

- Code—The code field is one octet; it identifies one of the following types of RADIUS packets:
  - Access-Request (1)
  - Access-Accept (2)
  - Access-Reject (3)
  - Accounting-Request (4)
  - Accounting-Response (5)
- Identifier—The identifier field is one octet; it helps the RADIUS server match requests and responses and detect duplicate requests.
- Length—The length field is two octets; it specifies the length of the entire packet.

- Authenticator—The authenticator field is 16 octets. The most significant octet is transmitted first; it is used to authenticate the reply from the RADIUS server. The two types of authenticators are:
    - Request-Authentication: Available in Access-Request and Accounting-Request packets.
    - Response-Authenticator: Available in Access-Accept, Access-Reject, Access-Challenge, and Accounting-Response packets.

RADIUS Packet Types

The following list defines the various types of RADIUS packet types that contain attribute information:

Access-Request—Sent from a client to a RADIUS server. The packet contains information that allows the RADIUS server to determine whether to allow access to a specific network access server (NAS), which will allow access to the user. A user performing authentication must submit an Access-Request packet. After the Access-Request packet is received, the RADIUS server must forward a reply.

Access-Accept—After a RADIUS server receives an Access-Request packet, it must send an Access-Accept packet if all attribute values in the Access-Request packet are acceptable. Access-Accept packets provide the configuration information necessary for the client to provide service to the user.

Access-Reject—After a RADIUS server receives an Access-Request packet, it must send an Access-Reject packet if any of the attribute values are not acceptable.

Access-Challenge—After the RADIUS server receives an Access-Accept packet, it can send the client an Access-Challenge packet, which requires a response. If the client does not know how to respond or if the packets are invalid, the RADIUS server discards the packets. If the client responds to the packet, a new Access-Request packet must be sent with the original Access-Request packet.

Accounting-Request—Sent from a client to a RADIUS accounting server, which provides accounting information. If the RADIUS server successfully records the Accounting-Request packet, it must submit an Accounting Response packet.

Accounting-Response—Sent by the RADIUS accounting server to the client to acknowledge that the Accounting-Request has been received and recorded successfully.

RADIUS Files

Understanding the types of files used by RADIUS is important for communicating AAA information from a client to a server. Each file defines a level of authentication or authorization for the user. The dictionary file defines which attributes the user’s NAS can implement, the clients file defines which users are allowed to make requests to the RADIUS server, and the users file defines which user requests the RADIUS server will authenticate based on security and configuration data.

Dictionary File

A dictionary file provides a list of attributes that are dependent on which attributes your NAS supports. However, you can add your own set of attributes to your dictionary for custom solutions. It defines attribute values, so you can interpret attribute output such as parsing requests. A dictionary file contains the following information:

- Name—The ASCII string “name” of the attribute, such as User-Name.

- ID—The numerical “name” of the attribute; for example, User-Name attribute is attribute 1.
- Value type—Each attribute can be specified as one of the following five value types:
    - abinary—0 to 254 octets.
    - date—32-bit value in big-endian order. For example, seconds since 00:00:00 GMT, JAN. 1, 1970.
    - ipaddr—4 octets in network byte order.
    - integer—32-bit value in big-endian order (high byte first).
    - string—0 to 253 octets.

When the data type for a particular attribute is an integer, you can optionally expand the integer to equate to some string. The following sample dictionary includes an integer-based attribute and its corresponding values.

```
# dictionary sample of integer entry
#
ATTRIBUTE       Service-Type            6                     integer
VALUE           Service-Type            Login                    1
VALUE           Service-Type            Framed                   2
VALUE           Service-Type            Callback-Login           3
VALUE           Service-Type            Callback-Framed          4
VALUE           Service-Type            Outbound                 5
VALUE           Service-Type            Administrative           6
VALUE           Service-Type            NAS-Prompt               7
VALUE           Service-Type            Authenticate-Only        8
VALUE           Service-Type            Callback-NAS-Prompt      9
VALUE           Service-Type            Call-Check               10
VALUE           Service-Type            Callback-Administrative  11
```

Clients File

A clients file contains a list of RADIUS clients that are allowed to send authentication and accounting requests to the RADIUS server. To receive authentication, the name and authentication key that the client sends to the server must be an exact match with the data contained in the clients file.

The following is an example of a clients file. The key, as shown in this example, must be the same as the **radius-server key***SomeSecret* command.

```
#Client Name        Key
#----------------  ---------------
10.1.2.3:256        test
nas01               bananas
nas02               MoNkEys
nas07.foo.com       SomeSecret
```

Users File

A RADIUS users file contains an entry for each user that the RADIUS server will authenticate; each entry, which is also known as a user profile, establishes an attribute the user can access.

The first line in any user profile is always a “user access” line; that is, the server must check the attributes on the first line before it can grant access to the user. The first line contains the name of the user, which can be up to 252 characters, followed by authentication information such as the password of the user.

Additional lines, which are associated with the user access line, indicate the attribute reply that is sent to the requesting client or server. The attributes sent in the reply must be defined in the dictionary file. When looking at a user file, note that the data to the left of the equal (=) character is an attribute defined in the dictionary file, and the data to the right of the equal character is the configuration data.

Note A blank line cannot appear anywhere within a user profile.

The following is an example of a RADIUS user profile (Merit Daemon format). In this example, the user name is company.com, the password is user1, and the user can access five tunnel attributes.

```
# This user profile includes RADIUS tunneling attributes
company.com  Password="user1" Service-Type=Outbound
     Tunnel-Type = :1:L2TP
     Tunnel-Medium-Type = :1:IP
     Tunnel-Server-Endpoint = :1:10.0.0.1
     Tunnel-Password = :1:"welcome"
     Tunnel-Assignment-ID = :1:"nas"
```

RADIUS IETF Attributes

Note For RADIUS tunnel attributes, 32 tagged tunnel sets are supported for L2TP.

Supported RADIUS IETF Attributes

Table 1 lists Cisco-supported IETF RADIUS attributes and the Cisco IOS release in which they are implemented. In cases where the attribute has a security server-specific format, the format is specified.

Refer to Table 2 for a description of each listed attribute.

Note Attributes implemented in special (AA) or early development (T) releases are added to the next mainline image.

Table 1: Supported RADIUS IETF Attributes

Number	IETF Attribute	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
1	User-Name	yes	yes	yes	yes	yes	yes	yes	yes
2	User-Password	yes	yes	yes	yes	yes	yes	yes	yes
3	CHAP-Password	yes	yes	yes	yes	yes	yes	yes	yes
4	NAS-IP Address	yes	yes	yes	yes	yes	yes	yes	yes
5	NAS-Port	yes	yes	yes	yes	yes	yes	yes	yes

Number	IETF Attribute	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
6	Service-Type	yes	yes	yes	yes	yes	yes	yes	yes
7	Framed-Protocol	yes	yes	yes	yes	yes	yes	yes	yes
8	Framed-IP-Address	yes	yes	yes	yes	yes	yes	yes	yes
9	Framed-IP-Netmask	yes	yes	yes	yes	yes	yes	yes	yes
10	Framed-Routing	yes	yes	yes	yes	yes	yes	yes	yes
11	Filter-Id	yes	yes	yes	yes	yes	yes	yes	yes
12	Framed-MTU	yes	yes	yes	yes	yes	yes	yes	yes
13	Framed-Compression	yes	yes	yes	yes	yes	yes	yes	yes
14	Login-IP-Host	yes	yes	yes	yes	yes	yes	yes	yes
15	Login-Service	yes	yes	yes	yes	yes	yes	yes	yes
16	Login-TCP-Port	yes	yes	yes	yes	yes	yes	yes	yes
18	Reply-Message	yes	yes	yes	yes	yes	yes	yes	yes
19	Callback-Number	no	no	no	no	no	no	yes	yes
20	Callback-ID	no	no	no	no	no	no	no	no
22	Framed-Route	yes	yes	yes	yes	yes	yes	yes	yes
23	Framed-IPX-Network	no	no	no	no	no	no	no	no
24	State	yes	yes	yes	yes	yes	yes	yes	yes
25	Class	yes	yes	yes	yes	yes	yes	yes	yes
26	Vendor-Specific	yes	yes	yes	yes	yes	yes	yes	yes
27	Session-Timeout	yes	yes	yes	yes	yes	yes	yes	yes
28	Idle-Timeout	yes	yes	yes	yes	yes	yes	yes	yes
29	Termination-Action	no	no	no	no	no	no	no	no
30	Called-Station-Id	yes	yes	yes	yes	yes	yes	yes	yes
31	Calling-Station-Id	yes	yes	yes	yes	yes	yes	yes	yes

Number	IETF Attribute	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
32	NAS-Identifier	no	no	no	no	no	no	no	yes
33	Proxy-State	no	no	no	no	no	no	no	no
34	Login-LAT-Service	yes	yes	yes	yes	yes	yes	yes	yes
35	Login-LAT-Node	no	no	no	no	no	no	no	yes
36	Login-LAT-Group	no	no	no	no	no	no	no	no
37	Framed-AppleTalk-Link	no	no	no	no	no	no	no	no
38	Framed-AppleTalk-Network	no	no	no	no	no	no	no	no
39	Framed-AppleTalk-Zone	no	no	no	no	no	no	no	no
40	Acct-Status-Type	yes	yes	yes	yes	yes	yes	yes	yes
41	Acct-Delay-Time	yes	yes	yes	yes	yes	yes	yes	yes
42	Acct-Input-Octets	yes	yes	yes	yes	yes	yes	yes	yes
43	Acct-Output-Octets	yes	yes	yes	yes	yes	yes	yes	yes
44	Acct-Session-Id	yes	yes	yes	yes	yes	yes	yes	yes
45	Acct-Authentic	yes	yes	yes	yes	yes	yes	yes	yes
46	Acct-Session-Time	yes	yes	yes	yes	yes	yes	yes	yes
47	Acct-Input-Packets	yes	yes	yes	yes	yes	yes	yes	yes
48	Acct-Output-Packets	yes	yes	yes	yes	yes	yes	yes	yes
49	Acct-Terminate-Cause	no	no	no	yes	yes	yes	yes	yes
50	Acct-Multi-Session-Id	no	yes	yes	yes	yes	yes	yes	yes
51	Acct-Link-Count	no	yes	yes	yes	yes	yes	yes	yes
52	Acct-Input-Gigawords	no	no	no	no	no	no	no	no
53	Acct-Output-Gigawords	no	no	no	no	no	no	no	no
55	Event-Timestamp	no	no	no	no	no	no	no	yes
60	CHAP-Challenge	yes	yes	yes	yes	yes	yes	yes	yes

Number	IETF Attribute	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
61	NAS-Port-Type	yes	yes	yes	yes	yes	yes	yes	yes
62	Port-Limit	yes	yes	yes	yes	yes	yes	yes	yes
63	Login-LAT-Port	no	no	no	no	no	no	no	no
64	Tunnel-Type[1]	no	no	no	no	no	no	yes	yes
65	Tunnel-Medium-Type[1]	no	no	no	no	no	no	yes	yes
66	Tunnel-Client-Endpoint	no	no	no	no	no	no	yes	yes
67	Tunnel-Server-Endpoint[1]	no	no	no	no	no	no	yes	yes
68	Acct-Tunnel-Connection-ID	no	no	no	no	no	no	yes	yes
69	Tunnel-Password[1]	no	no	no	no	no	no	yes	yes
70	ARAP-Password	no	no	no	no	no	no	no	no
71	ARAP-Features	no	no	no	no	no	no	no	no
72	ARAP-Zone-Access	no	no	no	no	no	no	no	no
73	ARAP-Security	no	no	no	no	no	no	no	no
74	ARAP-Security-Data	no	no	no	no	no	no	no	no
75	Password-Retry	no	no	no	no	no	no	no	no
76	Prompt	no	no	no	no	no	no	yes	yes
77	Connect-Info	no	no	no	no	no	no	no	yes
78	Configuration-Token	no	no	no	no	no	no	no	no
79	EAP-Message	no	no	no	no	no	no	no	no
80	Message-Authenticator	no	no	no	no	no	no	no	no
81	Tunnel-Private-Group-ID	no	no	no	no	no	no	no	no
82	Tunnel-Assignment-ID[1]	no	no	no	no	no	no	yes	yes

Number	IETF Attribute	11.1	11.2	11.3	11.3 AA	11.3T	12.0	12.1	12.2
83	Tunnel-Preference	no	no	no	no	no	no	no	yes
84	ARAP-Challenge-Response	no	no	no	no	no	no	no	no
85	Acct-Interim-Interval	no	no	no	no	no	no	yes	yes
86	Acct-Tunnel-Packets-Lost	no	no	no	no	no	no	no	no
87	NAS-Port-ID	no	no	no	no	no	no	no	no
88	Framed-Pool	no	no	no	no	no	no	no	no
90	Tunnel-Client-Auth-ID [2]	no	no	no	no	no	no	no	yes
91	Tunnel-Server-Auth-ID	no	no	no	no	no	no	no	yes
200	IETF-Token-Immediate	no	no	no	no	no	no	no	no

[1] This RADIUS attribute complies with the following two draft IETF documents: RFC 2868 RADIUS Attributes for Tunnel Protocol Support and RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support.

[2] This RADIUS attribute complies with RFC 2865 and RFC 2868.

Comprehensive List of RADIUS Attribute Descriptions

The table below lists and describes IETF RADIUS attributes. In cases where the attribute has a security server-specific format, the format is specified.

Table 2: RADIUS IETF Attributes

Number	IETF Attribute	Description
1	User-Name	Indicates the name of the user being authenticated by the RADIUS server.
2	User-Password	Indicates the user’s password or the user’s input following an Access-Challenge. Passwords longer than 16 characters are encrypted using RFC 2865 specifications.
3	CHAP-Password	Indicates the response value provided by a PPP Challenge Handshake Authentication Protocol (CHAP) user in response to an Access-Challenge.

Number	IETF Attribute	Description
4	NAS-IP Address	Specifies the IP address of the network access server that is requesting authentication. The default value is 0.0.0.0/0.
5	NAS-Port	Indicates the physical port number of the network access server that is authenticating the user. The NAS-Port value (32 bits) consists of one or two 16-bit values (depending on the setting of the **radius-server extended-portnames** command). Each 16-bit number should be viewed as a 5-digit decimal integer for interpretation as follows: For asynchronous terminal lines, asynchronous network interfaces, and virtual asynchronous interfaces, the value is **00ttt**, where **ttt** is the line number or asynchronous interface unit number. • For ordinary synchronous network interface, the value is **10xxx**. • For channels on a primary rate ISDN interface, the value is **2ppcc** • For channels on a basic rate ISDN interface, the value is **3bb0c**. • For other types of interfaces, the value is **6nnss**.

Number	IETF Attribute	Description
6	Service-Type	Indicates the type of service requested or the type of service to be provided. • In a request: Framed for known PPP or Serial Line Internet Protocol (SLIP) connection. Administrative-user for **enable** command. • In response: Login—Make a connection. Framed--Start SLIP or PPP. Administrative User--Start an EXEC or **enable ok**. Exec User—Start an EXEC session. Service type is indicated by a particular numeric value as follows: • 1: Login • 2: Framed • 3: Callback-Login • 4: Callback-Framed • 5: Outbound • 6: Administrative • 7: NAS-Prompt • 8: Authenticate Only • 9: Callback-NAS-Prompt
7	Framed-Protocol	Indicates the framing to be used for framed access. No other framing is allowed. Framing is indicated by a numeric value as follows: • 1: PPP • 2: SLIP • 3: ARA • 4: Gandalf-proprietary single-link/multilink protocol • 5: Xylogics-proprietary IPX/SLIP

Number	IETF Attribute	Description
8	Framed-IP-Address	Indicates the IP address to be configured for the user, by sending the IP address of a user to the RADIUS server in the access-request. To enable this command, use the **radius-server attribute 8 include-in-access-req** command in global configuration mode.
9	Framed-IP-Netmask	Indicates the IP netmask to be configured for the user when the user is using a device on a network. This attribute value results in a static route being added for Framed-IP-Address with the mask specified.
10	Framed-Routing	Indicates the routing method for the user when the user is using a device on a network. Only “None” and “Send and Listen” values are supported for this attribute. Routing method is indicated by a numeric value as follows: • 0: None • 1: Send routing packets • 2: Listen for routing packets • 3: Send routing packets and listen for routing packets
11	Filter-Id	Indicates the name of the filter list for the user and is formatted as follows: %d, %d.in, or %d.out. This attribute is associated with the most recent service-type command. For login and EXEC, use %d or %d.out as the line access list value from 0 to 199. For Framed service, use %d or %d.out as interface output access list, and %d.in for input access list. The numbers are self-encoding to the protocol to which they refer.
12	Framed-MTU	Indicates the maximum transmission unit (MTU) that can be configured for the user when the MTU is not negotiated by PPP.

Number	IETF Attribute	Description
13	Framed-Compression	Indicates a compression protocol used for the link. This attribute results in a "/compress" being added to the PPP or SLIP autocommand generated during EXEC authorization. This is not implemented for non-EXEC authorization. Compression protocol is indicated by a numeric value as follows: • 0: None • 1: VJ-TCP/IP header compression • 2: IPX header compression
14	Login-IP-Host	Indicates the host to which the user will connect when the Login-Service attribute is included. This begins immediately after login.
15	Login-Service	Indicates the service that should be used to connect the user to the login host. Service is indicated by a numeric value as follows: • 0: Telnet • 1: Rlogin • 2: TCP-Clear • 3: PortMaster • 4: LAT
16	Login-TCP-Port	Defines the TCP port with which the user is to be connected when the Login-Service attribute is also present.
18	Reply-Message	Indicates text that might be displayed to the user using the RADIUS server. You can include this attribute in user files; however, you cannot exceed a maximum of 16 Reply-Message entries per profile.
19	Callback-Number	Defines a dialing string to be used for callback.

Number	IETF Attribute	Description
20	Callback-ID	Defines the name (consisting of one or more octets) of a place to be called, to be interpreted by the network access server.
22	Framed-Route	Provides routing information to be configured for the user on this network access server. The RADIUS RFC format (net/bits [router [metric]]) and the old style dotted mask (net mask [router [metric]]) are supported. If the device field is omitted or 0, the peer IP address is used. Metrics are currently ignored. This attribute is access-request packets.
23	Framed-IPX-Network	Defines the IPX network number configured for the user.
24	State	Allows state information to be maintained between the network access server and the RADIUS server. This attribute is applicable only to CHAP challenges.
25	Class	(Accounting) Arbitrary value that the network access server includes in all accounting packets for this user if supplied by the RADIUS server.

Number	IETF Attribute	Description

26	Vendor-Specific	Allows vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the 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 of the 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 AV pair defined in the Cisco TACACS+ specification, and “sep” is “=” for mandatory attributes and “*” for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS. For example:
		`cisco-avpair= ”ip:addr-pool=first“`
		`cisco-avpair= ”shell:priv-lvl=15“`
		The first example causes Cisco’s Multiple Named ip address Pools” feature to be activated during IP authorization (during PPP’s IPCP address assignment). The second example causes a user logging in from a network access server to have immediate access to EXEC commands.
		Table 1 lists supported vendor-specific RADIUS attributes (IETF attribute 26).

27	Session-Timeout	Sets the maximum number of seconds of service to be provided to the user before the session terminates. This attribute value becomes the per-user absolute timeout.
28	Idle-Timeout	Sets the maximum number of consecutive seconds of idle connection allowed to the user before the session terminates. This attribute value becomes the per-user session-timeout.
29	Termination-Action	Termination is indicated by a numeric value as follows: • 0: Default • 1: RADIUS request

Number	IETF Attribute	Description
30	Called-Station-Id	(Accounting) Allows the network access server to send the telephone number the user called as part of the Access-Request packet (using Dialed Number Identification Service [DNIS] or a similar technology). This attribute is only supported on ISDN and modem calls on the Cisco AS5200 if used with PRI.
31	Calling-Station-Id	(Accounting) Allows the network access server to send the telephone number the call came from as part of the Access-Request packet (using Automatic Number Identification or a similar technology). This attribute has the same value as “remote-addr” from TACACS+. This attribute is only supported on ISDN and modem calls on the Cisco AS5200 if used with PRI.
32	NAS-Identifier	String identifying the network access server originating the Access-Request. Use the **radius-server attribute 32 include-in-access-req** global configuration command to send RADIUS attribute 32 in an Access-Request or Accounting-Request. By default, the Fully Qualified Domain Name (FQDN) is sent in the attribute when the format is not specified.
33	Proxy-State	Attribute that can be sent by a proxy server to another server when forwarding Access-Requests; this must be returned unmodified in the Access-Accept, Access-Reject or Access-Challenge and removed by the proxy server before sending the response to the network access server.
34	Login-LAT-Service	Indicates the system with which the user is to be connected by local area transport (LAT). This attribute is only available in the EXEC mode.
35	Login-LAT-Node	Indicates the node with which the user is automatically connected by LAT.
36	Login-LAT-Group	Identifies the LAT group codes that the user is authorized to use.

Number	IETF Attribute	Description
37	Framed-AppleTalk-Link	Indicates the AppleTalk network number that should be used for serial links, which is another AppleTalk device.
38	Framed-AppleTalk- Network	Indicates the AppleTalk network number that the network access server uses to allocate an AppleTalk node for the user.
39	Framed-AppleTalk-Zone	Indicates the AppleTalk Default Zone to be used for the user.
40	Acct-Status-Type	(Accounting) Indicates whether this Accounting-Request marks the beginning of the user service (start) or the end (stop).
41	Acct-Delay-Time	(Accounting) Indicates how many seconds the client has been trying to send a particular record.
42	Acct-Input-Octets	(Accounting) Indicates how many octets have been received from the port over the course of this service being provided.
43	Acct-Output-Octets	(Accounting) Indicates how many octets have been sent to the port in the course of delivering this service.
44	Acct-Session-Id	(Accounting) A unique accounting identifier that makes it easy to match start and stop records in a log file. Acct-Session ID numbers restart at 1 each time the device is power-cycled or the software is reloaded. To send this attribute in access-request packets, use the **radius-server attribute 44 include-in-access-req** command in global configuration mode.
45	Acct-Authentic	(Accounting) Indicates how the user was authenticated, whether by RADIUS, the network access server itself, or another remote authentication protocol. This attribute is set to “radius” for users authenticated by RADIUS; “remote” for TACACS+ and Kerberos; or “local” for local, enable, line, and if-needed methods. For all other methods, the attribute is omitted.
46	Acct-Session-Time	(Accounting) Indicates how long (in seconds) the user has received service.

Number	IETF Attribute	Description
47	Acct-Input-Packets	(Accounting) Indicates how many packets have been received from the port over the course of this service being provided to a framed user.
48	Acct-Output-Packets	(Accounting) Indicates how many packets have been sent to the port in the course of delivering this service to a framed user.
49	Acct-Terminate-Cause	(Accounting) Reports details on why the connection was terminated. Termination causes are indicated by a numeric value as follows: **1** User request **2** Lost carrier **3** Lost service **4** Idle timeout **5** Session timeout **6** Admin reset **7** Admin reboot **8** Port error **9** NAS error **10** NAS request **11** NAS reboot **12** Port unneeded **13** Port pre-empted **14** Port suspended **15** Service unavailable **16** Callback **17** User error **18** Host request **Note** For attribute 49, Cisco supports values 1 to 6, 8, 9, 12, and 15 to 18.

Number	IETF Attribute	Description
50	Acct-Multi-Session-Id	(Accounting) A unique accounting identifier used to link multiple related sessions in a log file. Each linked session in a multilink session has a unique Acct-Session-Id value, but shares the same Acct-Multi-Session-Id.
51	Acct-Link-Count	(Accounting) Indicates the number of links known in a given multilink session at the time an accounting record is generated. The network access server can include this attribute in any accounting request that might have multiple links.
52	Acct-Input-Gigawords	Indicates how many times the Acct-Input-Octets counter has wrapped around 2^32 over the course of the provided service.
53	Acct-Output-Gigawords	Indicates how many times the Acct-Output-Octets counter has wrapped around 2^32 while delivering service.

Number	IETF Attribute	Description
55	Event-Timestamp	Records the time that the event occurred on the NAS, the timestamp sent in attribute 55 is in seconds since January 1, 1970 00:00 UTC. To send RADIUS attribute 55 in accounting packets, use the **radius-server attribute 55 include-in-acct-req** command. **Note** Before the Event-Timestamp attribute can be sent in accounting packets, you must configure the clock on the network device. (For information on setting the clock on your network device, see the "Performing Basic System Management" section in the "Basic System Management" chapter of *Network Management Configuration Guide*.) To avoid configuring the clock on the network device every time the network device is reloaded, you can enable the **clock calendar-valid** command. (For more information about this command, see the"Setting Time and Calendar Services" section in the "Basic System Management" chapter of *Network Management Configuration Guide*.
60	CHAP-Challenge	Contains the Challenge Handshake Authentication Protocol challenge sent by the network access server to a PPP CHAP user.
61	NAS-Port-Type	Indicates the type of physical port the network access server is using to authenticate the user. Physical ports are indicated by a numeric value as follows: • 0: Asynchronous • 1: Synchronous • 2: ISDN-Synchronous • 3: ISDN-Asynchronous (V.120) • 4: ISDN-Asynchronous (V.110) • 5: Virtual

Number	IETF Attribute	Description
62	Port-Limit	Sets the maximum number of ports provided to the user by the NAS.
63	Login-LAT-Port	Defines the port with which the user is to be connected by LAT.
64	Tunnel-Type[3]	Indicates the tunneling protocol(s) used. Cisco software supports one possible value for this attribute: L2TP.
65	Tunnel-Medium-Type1	Indicates the transport medium type used to create a tunnel. This attribute has only one available value for this release: IP. If no value is set for this attribute, IP is used as the default.
66	Tunnel-Client-Endpoint	Contains the address of the initiator end of the tunnel. It may be included in both Access-Request and Access-Accept packets to indicate the address from which a new tunnel is to be initiated. If the Tunnel-Client-Endpoint attribute is included in an Access-Request packet, the RADIUS server should take the value as a hint. This attribute should be included in Accounting-Request packets that contain Acct-Status-Type attributes with values of either Start or Stop, in which case it indicates the address from which the tunnel was initiated. This attribute, along with the Tunnel-Server-Endpoint and Acct-Tunnel-Connection-ID attributes, may be used to provide a globally unique method to identify a tunnel for accounting and auditing purposes. An enhancement has been added for the network access server to accept a value of 127.0.0.X for this attribute such that: 127.0.0.0 would indicate that loopback0 IP address has to be used, 127.0.0.1 would indicate that loopback1 IP address has to be used. 127.0.0.X would indicate that loopbackX IP address has to be used for the actual tunnel client endpoint IP address. This enhancement adds scalability across multiple network access servers.

Number	IETF Attribute	Description
67	Tunnel-Server-Endpoint1	Indicates the address of the server end of the tunnel. The format of this attribute varies depending on the value of Tunnel-Medium-Type. Depending on your release only IP as a tunnel medium type may be supported and the IP address or the host name of LNS is valid for this attribute.
68	Acct-Tunnel-Connection-ID	Indicates the identifier assigned to the tunnel session. This attribute should be included in Accounting-Request packets that contain an Acct-Status-Type attribute having the value Start, Stop, or any of the values described above. This attribute, along with the Tunnel-Client-Endpoint and Tunnel-Server-Endpoint attributes, may be used to provide a method to uniquely identify a tunnel session for auditing purposes.
69	Tunnel-Password1	Defines the password to be used to authenticate to a remote server. This attribute is converted into different AAA attributes based on the value of Tunnel-Type: AAA_ATTR_l2tp_tunnel_pw (L2TP), AAA_ATTR_nas_password (L2F), and AAA_ATTR_gw_password (L2F). By default, all passwords received are encrypted, which can cause authorization failures when a NAS attempts to decrypt a non-encrypted password. To enable attribute 69 to receive non-encrypted passwords, use the **radius-server attribute 69 clear** command in global configuration mode.
70	ARAP-Password	Identifies an Access-Request packet containing a Framed-Protocol of AppleTalk Remote Access Control (ARAP).
71	ARAP-Features	Includes password information that the NAS should send to the user in an ARAP feature flags packet.
72	ARAP-Zone-Access	Indicates how the ARAP zone list for the user should be used.
73	ARAP-Security	Identifies the ARAP Security Module to be used in an Access-Challenge packet.

Number	IETF Attribute	Description
74	ARAP-Security-Data	Contains the actual security module challenge or response in Access-Challenge and Access-Request packets.
75	Password-Retry	Indicates the number of times a user may attempt authentication before being disconnected.
76	Prompt	Indicates to the NAS whether it should echo the user's response as it is entered or not echo it. (0 = no echo, 1 = echo)
77	Connect-Info	Provides additional call information for modem calls. This attribute is generated in start and stop accounting records.
78	Configuration-Token	Indicates the type of user profile to be used. This attribute should be used in large distributed authentication networks based on proxy. It is sent from a RADIUS Proxy Server to a RADIUS Proxy Client in an Access-Accept; it should not be sent to a NAS.
79	EAP-Message	Encapsulates Extended Access Protocol (EAP) packets that allow the NAS to authenticate dial-in users using EAP without having to understand the EAP protocol.
80	Message-Authenticator	Prevents spoofing Access-Requests using CHAP, ARAP, or EAP authentication methods.
81	Tunnel-Private-Group-ID	Indicates the group ID for a particular tunneled session.
82	Tunnel-Assignment-ID1	Indicates to the tunnel initiator the particular tunnel to which a session is assigned.
83	Tunnel-Preference	Indicates the relative preference assigned to each tunnel. This attribute should be included if more than one set of tunneling attributes is returned by the RADIUS server to the tunnel initiator.
84	ARAP-Challenge-Response	Contains the response to the challenge of the dial-in client.

Number	IETF Attribute	Description
85	Acct-Interim-Interval	Indicates the number of seconds between each interim update in seconds for this specific session. This value can only appear in the Access-Accept message.
86	Acct-Tunnel-Packets-Lost	Indicates the number of packets lost on a given link. This attribute should be included in Accounting-Request packets that contain an Acct-Status-Type attribute having the value Tunnel-Link-Stop.
87	NAS-Port-ID	Contains a text string which identifies the port of the NAS that is authenticating the user.
88	Framed-Pool	Contains the name of an assigned address pool that should be used to assign an address for the user. If a NAS does not support multiple address pools, the NAS should ignore this attribute.
90	Tunnel-Client-Auth-ID	Specifies the name used by the tunnel initiator (also known as the NAS) when authenticating tunnel setup with the tunnel terminator. Supports L2F and L2TP protocols.
91	Tunnel-Server-Auth-ID	Specifies the name used by the tunnel terminator (also known as the Home Gateway) when authenticating tunnel setup with the tunnel initiator. Supports L2F and L2TP protocols.
200	IETF-Token-Immediate	Determines how RADIUS treats passwords received from login-users when their file entry specifies a hand-held security card server. The value for this attribute is indicated by a numeric value as follows: • 0: No—the password is ignored. • 1: Yes—the password is used for authentication.

[3] This RADIUS attribute complies with the following two IETF documents: RFC 2868, RADIUS Attributes for Tunnel Protocol Support and RFC 2867, RADIUS Accounting Modifications for Tunnel Protocol Support .

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Commands List, All Releases
Security commands	• Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z

RFCs

RFC	Title
RFC 2865	Remote Authentication Dial In User Service (RADIUS)
RFC 2866	RADIUS Accounting
RFC 2867	RADIUS Accounting Modifications for Tunnel Protocol Support
RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 2869	RADIUS Extensions

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for RADIUS Attributes Overview and RADIUS IETF Attributes

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for RADIUS Attributes Overview and RADIUS IETF Attributes

Feature Name	Releases	Feature Information
RADIUS IETF Attributes	Cisco IOS Release 11.1	This feature was introduced in Cisco IOS Release 11.1.

CHAPTER 2

RADIUS Vendor-Proprietary Attributes

The IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server. However, some vendors have extended the RADIUS attribute set for specific applications. This document provides Cisco IOS support information for these vendor-proprietary RADIUS attrubutes.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Comprehensive List of Vendor-Proprietary RADIUS Attribute Descriptions

The table below lists and describes the known vendor-proprietary RADIUS attributes:

Table 4: Vendor-Proprietary RADIUS Attributes

Number	Vendor-Proprietary Attribute	Description
17	Change-Password	Specifies a request to change the password of a user.

Number	Vendor-Proprietary Attribute	Description
21	Password-Expiration	Specifies an expiration date for a user's password in the user's file entry.
68	Tunnel-ID	(Ascend 5) Specifies the string assigned by RADIUS for each session using CLID or DNIS tunneling. When accounting is implemented, this value is used for accoutning.
108	My-Endpoint-Disc-Alias	(Ascend 5) No description available.
109	My-Name-Alias	(Ascend 5) No description available.
110	Remote-FW	(Ascend 5) No description available.
111	Multicast-GLeave-Delay	(Ascend 5) No description available.
112	CBCP-Enable	(Ascend 5) No description available.
113	CBCP-Mode	(Ascend 5) No description available.
114	CBCP-Delay	(Ascend 5) No description available.
115	CBCP-Trunk-Group	(Ascend 5) No description available.
116	Appletalk-Route	(Ascend 5) No description available.
117	Appletalk-Peer-Mode	(Ascend 5) No description available.
118	Route-Appletalk	(Ascend 5) No description available.
119	FCP-Parameter	(Ascend 5) No description available.
120	Modem-PortNo	(Ascend 5) No description available.

Number	Vendor-Proprietary Attribute	Description
121	Modem-SlotNo	(Ascend 5) No description available.
122	Modem-ShelfNo	(Ascend 5) No description available.
123	Call-Attempt-Limit	(Ascend 5) No description available.
124	Call-Block-Duration	(Ascend 5) No description available.
125	Maximum-Call-Duration	(Ascend 5) No description available.
126	Router-Preference	(Ascend 5) No description available.
127	Tunneling-Protocol	(Ascend 5) No description available.
128	Shared-Profile-Enable	(Ascend 5) No description available.
129	Primary-Home-Agent	(Ascend 5) No description available.
130	Secondary-Home-Agent	(Ascend 5) No description available.
131	Dialout-Allowed	(Ascend 5) No description available.
133	BACP-Enable	(Ascend 5) No description available.
134	DHCP-Maximum-Leases	(Ascend 5) No description available.
135	Primary-DNS-Server	Identifies a primary DNS server that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation.

Number	Vendor-Proprietary Attribute	Description
136	Secondary-DNS-Server	Identifies a secondary DNS server that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation.
137	Client-Assign-DNS	No description available.
138	User-Acct-Type	No description available.
139	User-Acct-Host	No description available.
140	User-Acct-Port	No description available.
141	User-Acct-Key	No description available.
142	User-Acct-Base	No description available.
143	User-Acct-Time	No description available.
144	Assign-IP-Client	No description available.
145	Assign-IP-Server	No description available.
146	Assign-IP-Global-Pool	No description available.
147	DHCP-Reply	No description available.
148	DHCP-Pool-Number	No description available.
149	Expect-Callback	No description available.
150	Event-Type	No description available.
151	Session-Svr-Key	No description available.
152	Multicast-Rate-Limit	No description available.
153	IF-Netmask	No description available.
154	Remote-Addr	No description available.
155	Multicast-Client	No description available.
156	FR-Circuit-Name	No description available.
157	FR-LinkUp	No description available.
158	FR-Nailed-Grp	No description available.

Number	Vendor-Proprietary Attribute	Description
159	FR-Type	No description available.
160	FR-Link-Mgt	No description available.
161	FR-N391	No description available.
162	FR-DCE-N392	No description available.
163	FR-DTE-N392	No description available.
164	FR-DCE-N393	No description available.
165	FR-DTE-N393	No description available.
166	FR-T391	No description available.
167	FR-T392	No description available.
168	Bridge-Address	No description available.
169	TS-Idle-Limit	No description available.
170	TS-Idle-Mode	No description available.
171	DBA-Monitor	No description available.
172	Base-Channel-Count	No description available.
173	Minimum-Channels	No description available.
174	IPX-Route	No description available.
175	FT1-Caller	No description available.
176	Backup	No description available.
177	Call-Type	No description available.
178	Group	No description available.
179	FR-DLCI	No description available.
180	FR-Profile-Name	No description available.
181	Ara-PW	No description available.
182	IPX-Node-Addr	No description available.

Number	Vendor-Proprietary Attribute	Description
183	Home-Agent-IP-Addr	Indicates the home agent's IP address (in dotted decimal format) when using Ascend Tunnel Management Protocol (ATMP).
184	Home-Agent-Password	With ATMP, specifies the password that the foreign agent uses to authenticate itself.
185	Home-Network-Name	With ATMP, indicates the name of the connection profile to which the home agent sends all packets.
186	Home-Agent-UDP-Port	Indicates the UDP port number the foreign agent uses to send ATMP messages to the home agent.
187	Multilink-ID	Reports the identification number of the multilink bundle when the session closes. This attribute applies to sessions that are part of a multilink bundle. The Multilink-ID attribute is sent in authentication-response packets.
188	Num-In-Multilink	Reports the number of sessions remaining in a multilink bundle when the session reported in an accounting-stop packet closes. This attribute applies to sessions that are part of a multilink bundle. The Num-In-Multilink attribute is sent in authentication-response packets and in some accounting-request packets.
189	First-Dest	Records the destination IP address of the first packet received after authentication.
190	Pre-Input-Octets	Records the number of input octets before authentication. The Pre-Input-Octets attribute is sent in accounting-stop records.
191	Pre-Output-Octets	Records the number of output octets before authentication. The Pre-Output-Octets attribute is sent in accounting-stop records.

Number	Vendor-Proprietary Attribute	Description
192	Pre-Input-Packets	Records the number of input packets before authentication. The Pre-Input-Packets attribute is sent in accounting-stop records.
193	Pre-Output-Packets	Records the number of output packets before authentication. The Pre-Output-Packets attribute is sent in accounting-stop records.
194	Maximum-Time	Specifies the maximum length of time (in seconds) allowed for any session. After the session reaches the time limit, its connection is dropped.
195	Disconnect-Cause	Specifies the reason a connection was taken offline. The Disconnect-Cause attribute is sent in accounting-stop records. This attribute also causes stop records to be generated without first generating start records if disconnection occurs before authentication is performed. For more information, refer to the table of Disconnect-Cause Attribute Values and their meanings.
196	Connect-Progress	Indicates the connection state before the connection is disconnected.
197	Data-Rate	Specifies the average number of bits per second over the course of the connection’s lifetime. The Data-Rate attribute is sent in accounting-stop records.
198	PreSession-Time	Specifies the length of time, in seconds, from when a call first connects to when it completes authentication. The PreSession-Time attribute is sent in accounting-stop records.

Number	Vendor-Proprietary Attribute	Description
199	Token-Idle	Indicates the maximum amount of time (in minutes) a cached token can remain alive between authentications.
201	Require-Auth	Defines whether additional authentication is required for class that has been CLID authenticated.
202	Number-Sessions	Specifies the number of active sessions (per class) reported to the RADIUS accounting server.
203	Authen-Alias	Defines the RADIUS server's login name during PPP authentication.
204	Token-Expiry	Defines the lifetime of a cached token.
205	Menu-Selector	Defines a string to be used to cue a user to input data.
206	Menu-Item	Specifies a single menu-item for a user-profile. Up to 20 menu items can be assigned per profile.
207	PW-Warntime	(Ascend 5) No description available.
208	PW-Lifetime	Enables you to specify on a per-user basis the number of days that a password is valid.

Number	Vendor-Proprietary Attribute	Description
209	IP-Direct	When you include this attribute in a user's file entry, a framed route is installed to the routing and bridging tables. **Note** Packet routing is dependent upon the entire table, not just this newly installed entry. The inclusion of this attribute does not guarantee that all packets should be sent to the specified IP address; thus, this attribute is not fully supported. These attribute limitations occur because the Cisco router cannot bypass all internal routing and bridging tables and send packets to a specified IP address.
210	PPP-VJ-Slot-Comp	Instructs the Cisco router not to use slot compression when sending VJ-compressed packets over a PPP link.
211	PPP-VJ-1172	Instructs PPP to use the 0x0037 value for VJ compression.
212	PPP-Async-Map	Gives the Cisco router the asynchronous control character map for the PPP session. The specified control characters are passed through the PPP link as data and used by applications running over the link.
213	Third-Prompt	Defines a third prompt (after username and password) for additional user input.
214	Send-Secret	Enables an encrypted password to be used in place of a regular password in outdial profiles.
215	Receive-Secret	Enables an encrypted password to be verified by the RADIUS server.

Number	Vendor-Proprietary Attribute	Description
216	IPX-Peer-Mode	(Ascend 5) No description available.
217	IP-Pool-Definition	Defines a pool of addresses using the following format: X a.b.c Z; where X is the pool index number, a.b.c is the pool's starting IP address, and Z is the number of IP addresses in the pool. For example, 3 10.0.0.1 5 allocates 10.0.0.1 through 10.0.0.5 for dynamic assignment.
218	Assign-IP-Pool	Tells the router to assign the user and IP address from the IP pool.
219	FR-Direct	Defines whether the connection profile operates in Frame Relay redirect mode.
220	FR-Direct-Profile	Defines the name of the Frame Relay profile carrying this connection to the Frame Relay switch.
221	FR-Direct-DLCI	Indicates the DLCI carrying this connection to the Frame Relay switch.
222	Handle-IPX	Indicates how NCP watchdog requests will be handled.
223	Netware-Timeout	Defines, in minutes, how long the RADIUS server responds to NCP watchdog packets.
224	IPX-Alias	Allows you to define an alias for IPX routers requiring numbered interfaces.
225	Metric	No description available.
226	PRI-Number-Type	No description available.
227	Dial-Number	Defines the number to dial.
228	Route-IP	Indicates whether IP routing is allowed for the user's file entry.

Number	Vendor-Proprietary Attribute	Description
229	Route-IPX	Allows you to enable IPX routing.
230	Bridge	No description available.
231	Send-Auth	Defines the protocol to use (PAP or CHAP) for username-password authentication following CLID authentication.
232	Send-Passwd	Enables the RADIUS server to specify the password that is sent to the remote end of a connection on outgoing calls.
233	Link-Compression	Defines whether to turn on or turn off "stac" compression over a PPP link. Link compression is defined as a numeric value as follows: • 0: None • 1: Stac • 2: Stac-Draft-9 • 3: MS-Stac
234	Target-Util	Specifies the load-threshold percentage value for bringing up an additional channel when PPP multilink is defined.
235	Maximum-Channels	Specifies allowed/allocatable maximum number of channels.
236	Inc-Channel-Count	No description available.
237	Dec-Channel-Count	No description available.
238	Seconds-of-History	No description available.
239	History-Weigh-Type	No description available.
240	Add-Seconds	No description available.
241	Remove-Seconds	No description available.

Number	Vendor-Proprietary Attribute	Description
242	Data-Filter	Defines per-user IP data filters. These filters are retrieved only when a call is placed using a RADIUS outgoing profile or answered using a RADIUS incoming profile. Filter entries are applied on a first-match basis; therefore, the order in which filter entries are entered is important.
243	Call-Filter	Defines per-user IP data filters. On a Cisco router, this attribute is identical to the Data-Filter attribute.
244	Idle-Limit	Specifies the maximum time (in seconds) that any session can be idle. When the session reaches the idle time limit, its connection is dropped.
245	Preempt-Limit	No description available.
246	Callback	Allows you to enable or disable callback.
247	Data-Svc	No description available.
248	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.
249	Billing Number	No description available.
250	Call-By-Call	No description available.
251	Transit-Number	No description available.
252	Host-Info	No description available.
253	PPP-Address	Indicates the IP address reported to the calling unit during PPP IPCP negotiations.
254	MPP-Idle-Percent	No description available.
255	Xmit-Rate	(Ascend 5) No description available.

For more information on vendor-propritary RADIUS attributes, refer to the section “ Configuring Router for Vendor-Proprietary RADIUS Server Communication ” in the chapter “ Configuring RADIUS .”

Feature Information for RADIUS Vendor-Proprietary Attributes

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5: Feature Information for RADIUS Vendor-Proprietary Attributes

Feature Name	Releases	Feature Information
RADIUS Vendor-Proprietary Attributes	12.2(1)XE	The IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server. However, some vendors have extended the RADIUS attribute set for specific applications. This document provides Cisco IOS support information for these vendor-proprietary RADIUS attrubutes. In 12.2(1) XE, this feature was introduced.

CHAPTER 3

RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Attribute 26 encapsulates vendor specific attributes (VSA), thereby, allowing vendors to support their own extended attributes otherwise not suitable for general use.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values

The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the 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 of the following format:

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

“Protocol” is a value of the Cisco “protocol” attribute for a particular type of authorization; protocols that can be used include IP, IPX, VPDN, VOIP, SHELL, RSVP, SIP, AIRNET, OUTBOUND. “Attribute” and “value” are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and “sep” is “=” for mandatory attributes and “*” for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes Cisco’s “multiple named ip address pools” feature to be activated during IP authorization (during PPP’s IPCP address assignment):

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

If you insert an “*”, the AV pair “ip:addr-pool=first” becomes optional. Note that 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:

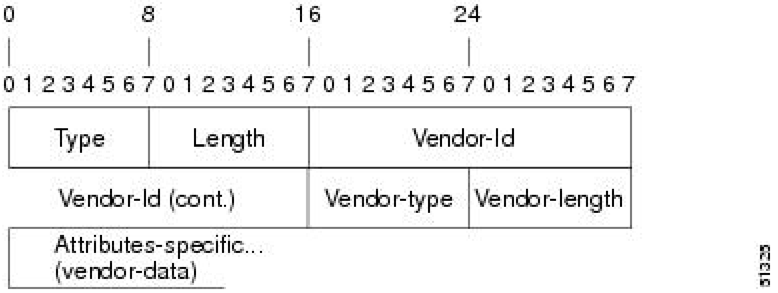
```
cisco-avpair= ”shell:priv-lvl=15“
```

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

Table 6: 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 7: 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	Contains the response value provided by a PPP MS-CHAP user in response 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	Specifies the maximum receive window size for L2TP control messages. 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.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	l2tp-hidden-avp	When enabled, sensitive AVPs in L2TP control messages are scrambled or hidden.
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	Shared secret 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.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
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.
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.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	10	Fax-Process-Abort-Flag	Indicates that the fax session was aborted or successful. True means that the session was aborted; false means that the session was successful.
26	9	11	Fax-Dsn-Address	Indicates the address to which DSNs will be sent.
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 or not message delivery notification (MDN) has been enabled. True indicates that MDN had been enabled; false means that MDN had not been 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.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
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.
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 aborts, indicates the system component that signaled the abort. Examples of system components that could trigger an abort are FAP (Fax Application Process), TIFF (the TIFF reader or the TIFF writer), fax-mail client, fax-mail server, ESMTP client, or 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.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
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) and 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.
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.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
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 has changed over time: Initially, it performed the functions now provided by both the send-name and remote-name attributes. Because the remote-name attribute has been added, the send-name attribute is restricted to its current behavior.

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
26	9	1	send-secret	PPP password authentication. The vendor-specific attributes (VSAs) “preauth:send-name” and “preauth:send-secret” will be used as the PAP username and PAP password for outbound authentication. For a CHAP outbound case, both “preauth:send-name” and “preauth:send-secret” will be used in the response packet.
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 router.)
Miscellaneous Attributes				

Number	Vendor-Specific Company Code	Sub-Type Number	Attribute	Description
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.

For more information on configuring your NAS to recognize and use VSAs, refer to the "Configuring Router to Use Vendor-Specific RADIUS Attributes" section of th e " Configuring RADIUS " module.

RADIUS Disconnect-Cause Attribute Values

Disconnect-cause attribute values specify the reason a connection was taken offline. The attribute values are sent in Accounting request packets. These values are sent at the end of a session, even if the session fails to be authenticated. If the session is not authenticated, the attribute can cause stop records to be generated without first generating start records.

The table below lists the cause codes, values, and descriptions for the Disconnect-Cause (195) attribute.

Note The Disconnect-Cause is incremented by 1000 when it is used in RADIUS AVPairs; for example, disc-cause 4 becomes 1004.

Table 8: Disconnect-Cause Attribute Values

Cause Code	Value	Description
0	No-Reason	No reason is given for the disconnect.
1	No-Disconnect	The event was not disconnected.

Cause Code	Value	Description
2	Unknown	Reason unknown.
3	Call-Disconnect	The call has been disconnected.
4	CLID-Authentication-Failure	Failure to authenticate number of the calling-party.
9	No-Modem-Available	A modem in not available to connect the call.
10	No-Carrier	No carrier detected. **Note** Codes 10, 11, and 12 can be sent if there is a disconnection during initial modem connection.
11	Lost-Carrier	Loss of carrier.
12	No-Detected-Result-Codes	Failure to detect modem result codes.
20	User-Ends-Session	User terminates a session. **Note** Codes 20, 22, 23, 24, 25, 26, 27, and 28 apply to EXEC sessions.
21	Idle-Timeout	Timeout waiting for user input. Codes 21, 100, 101, 102, and 120 apply to all session types.
22	Exit-Telnet-Session	Disconnect due to exiting Telnet session.
23	No-Remote-IP-Addr	Could not switch to SLIP/PPP; the remote end has no IP address.
24	Exit-Raw-TCP	Disconnect due to exiting raw TCP.
25	Password-Fail	Bad passwords.
26	Raw-TCP-Disabled	Raw TCP disabled.
27	Control-C-Detected	Control-C detected.
28	EXEC-Process-Destroyed	EXEC process destroyed.
29	Close-Virtual-Connection	User closes a virtual connection.
30	End-Virtual-Connection	Virtual connected has ended.
31	Exit-Rlogin	User exists Rlogin.

Cause Code	Value	Description
32	Invalid-Rlogin-Option	Invalid Rlogin option selected.
33	Insufficient-Resources	Insufficient resources.
40	Timeout-PPP-LCP	PPP LCP negotiation timed out. **Note** Codes 40 through 49 apply to PPP sessions.
41	Failed-PPP-LCP-Negotiation	PPP LCP negotiation failed.
42	Failed-PPP-PAP-Auth-Fail	PPP PAP authentication failed.
43	Failed-PPP-CHAP-Auth	PPP CHAP authentication failed.
44	Failed-PPP-Remote-Auth	PPP remote authentication failed.
45	PPP-Remote-Terminate	PPP received a Terminate Request from remote end.
46	PPP-Closed-Event	Upper layer requested that the session be closed.
47	NCP-Closed-PPP	PPP session closed because there were no NCPs open.
48	MP-Error-PPP	PPP session closed because of an MP error.
49	PPP-Maximum-Channels	PPP session closed because maximum channels were reached.
50	Tables-Full	Disconnect due to full terminal server tables.
51	Resources-Full	Disconnect due to full internal resources.
52	Invalid-IP-Address	IP address is not valid for Telnet host.
53	Bad-Hostname	Hostname cannot be validated.
54	Bad-Port	Port number is invalid or missing.
60	Reset-TCP	TCP connection has been reset. **Note** Codes 60 through 67 apply to Telnet or raw TCP sessions.
61	TCP-Connection-Refused	TCP connection has been refused by the host.
62	Timeout-TCP	TCP connection has timed out.

Cause Code	Value	Description
63	Foreign-Host-Close-TCP	TCP connection has been closed.
64	TCP-Network-Unreachable	TCP network is unreachable.
65	TCP-Host-Unreachable	TCP host is unreachable.
66	TCP-Network-Admin Unreachable	TCP network is unreachable for administrative reasons.
67	TCP-Port-Unreachable	TCP port in unreachable.
100	Session-Timeout	Session timed out.
101	Session-Failed-Security	Session failed for security reasons.
102	Session-End-Callback	Session terminated due to callback.
120	Invalid-Protocol	Call refused because the detected protocol is disabled.
150	RADIUS-Disconnect	Disconnected by RADIUS request.
151	Local-Admin-Disconnect	Administrative disconnect.
152	SNMP-Disconnect	Disconnected by SNMP request.
160	V110-Retries	Allowed V.110 retries have been exceeded.
170	PPP-Authentication-Timeout	PPP authentication timed out.
180	Local-Hangup	Disconnected by local hangup.
185	Remote-Hangup	Disconnected by remote end hangup.
190	T1-Quiesced	Disconnected because T1 line was quiesced.
195	Call-Duration	Disconnected because the maximum duration of the call was exceeded.
600	VPN-User-Disconnect	Call disconnected by client (through PPP). Code is sent if the LNS receives a PPP terminate request from the client.
601	VPN-Carrier-Loss	Loss of carrier. This can be the result of a physical line going dead. Code is sent when a client is unable to dial out using a dialer.

Cause Code	Value	Description
602	VPN-No-Resources	No resources available to handle the call. Code is sent when the client is unable to allocate memory (running low on memory).
603	VPN-Bad-Control-Packet	Bad L2TP or L2F control packets. This code is sent when an invalid control packet, such as missing mandatory Attribute-Value pairs (AVP), from the peer is received. When using L2TP, the code will be sent after six retransmits; when using L2F, the number of retransmits is user configurable. **Note** VPN-Tunnel-Shut will be sent if there are active sessions in the tunnel.
604	VPN-Admin-Disconnect	Administrative disconnect. This can be the result of a VPN soft shutdown, which is when a client reaches maximum session limit or exceeds maximum hopcount. Code is sent when a tunnel is brought down by issuing the **clear vpdn tunnel** command.
605	VPN-Tunnel-Shut	Tunnel teardown or tunnel setup has failed. Code is sent when there are active sessions in a tunnel and the tunnel goes down. **Note** This code is not sent when tunnel authentication fails.
606	VPN-Local-Disconnect	Call is disconnected by LNS PPP module. Code is sent when the LNS sends a PPP terminate request to the client. It indicates a normal PPP disconnection initiated by the LNS.
607	VPN-Session-Limit	VPN soft shutdown is enabled. Code is sent when a call has been refused due to any of the soft shutdown restrictions previously mentioned.
608	VPN-Call-Redirect	VPN call redirect is enabled.

For Q.850 cause codes and descriptions, see the *Cisco IOS Voice Troubleshooting and Monitoring Guide* , Release 12.4T.

Additional References

The following sections provide references related to RADIUS Vendor-Specific Attributes (VSA) and RADIUS Disconnect-Cause Attribute Values.

Related Documents

Related Topic	Document Title
Security Features	*Cisco IOS Security Configuration Guide: Securing User Services* , Release 15.0.
Security Server Protocols	
RADIUS Configuration	“ Configuring RADIUS ” module.

Standards

Standard	Title
Internet Engineering Task Force (IETF) Internet Draft: Network Access Servers Requirements	Network Access Servers Requirements: Extended RADIUS Practices

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2865	Remote Authentication Dial In User Service (RADIUS)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

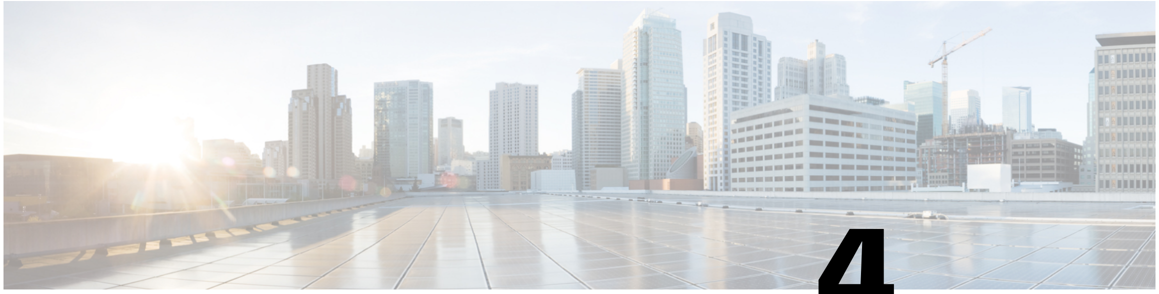
Feature Information for RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 9: Feature Information for RADIUS Vendor-Specific Attributes (VSA) and RADIUS Disconnect-Cause Attribute Values

Feature Name	Releases	Feature Information
RADIUS Vendor-Specific Attributes (VSA) and RADIUS Disconnect-Cause Attribute Values	12.0(30)S3s 12.3(11)YS1 12.2(33)SRC	This document discusses the Internet Engineering Task Force (IETF) draft standard, which specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Attribute 26 encapsulates vendor specific attributes, thereby, allowing vendors to support their own extended attributes otherwise not suitable for general use. This feature was introduced into Cisco IOS Release 12.0(30)S3s. This feature was integrated into Cisco IOS Release 12.3(11)YS1. This feature was integrated into Cisco IOS Release 12.2(33)SRC.



CHAPTER 4

Connect-Info RADIUS Attribute 77

The Connect-Info RADIUS Attribute 77 feature enables the Network Access Server (NAS) to report Connect-Info (attribute 77) in RADIUS accounting “start” and “stop” records that are sent to the RADIUS client (dial-in modem). These records allow the transmit and receive connection speeds, modulation, and compression to be compared in order to analyze a user session over a dial-in modem where speeds are often different at the end of the connection (after negotiation).

When the network access server (NAS) sends attribute 77 in accounting “start” and “stop” records, the connect rates can be measured across the platform. The “transmit” speed (the speed at which the NAS modem sends information) and “receive” speed (the speed at which the NAS receives information) can be recorded to determine whether user modem connections renegotiate to lower speeds shortly into a session. If the transmit and receive speeds are different from each other, attribute 77 reports both speeds, which allows the modem connection speeds that each customer gets from their session.

Attribute 77 is also used to send the Class string for broadband connections such as PPPoX, physical connection speeds for dial access, and the VRF string for any sessions on router interfaces defined with **ip vrf forwarding** command.

Note This feature requires no configuration.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Connect-Info RADIUS Attribute 77

For information about release and platform support, see the Feature Information for Connect-Info RADIUS Attribute 77.

Before the NAS can send attribute 77 in accounting “start” and “stop” records, you must perform the following tasks:

- Configure your NAS for authentication, authorization, and accounting (AAA) and to accept incoming modem calls.
- Enable AAA accounting by using the **aaa accounting network default start-stop group radius** command in global configuration mode.
- Change the modem poll timer by using the **modem link-info poll time** command in global configuration mode.

Note Changing the modem poll timer is required on the Cisco ASR 1000 Series Aggregation Services Routers.

Information About Connect-Info RADIUS Attribute 77

The Configurable Connect-Info Attributes feature introduces support for RADIUS attribute 77 (Connect-Info), which provides information about connection speeds, modulation, and compression for modem dial-in connections via RADIUS accounting “start” and “stop” records.

Customizing Attribute 77 for Ethernet Connections

To customize Attribute 77 for Ethernet connections, enter the connection information as the name of the service policy attached to the Ethernet subinterface. The router takes the policy name and copies it to Attribute 77.

For example, in the following configuration the outbound service policy named speed:eth:25100:5100:19/0 is attached to the QinQ Gigabit Ethernet subinterface 1/0/0.2696. The router copies the policy name to Attribute 77 and sends it to the RADIUS server in an Access-Request or Accounting-Start or Stop message.

```
interface GigabitEthernet1/0/0.2696
encapsulation dot1q 2696 second-dot1q 256
```

```
pppoe enable group global
no snmp trap link-status
service-policy input set_precedence_to_0
service-policy output speed:eth:25100:5100:19/0
```

Customizing Attribute 77 for ATM Connections

To customize Attribute 77 for ATM connections, configure the **aaa connect-info** *string* command in the following configuration modes:

- PVC (for a specific PVC)
- PVC range (for a range of PVCs)
- PVC-in-range (for a specific PVC in a range of PVCs)
- VC class (under a specific **class-vc** command)

The router takes the name of the VC class you specify under the **class-vc** command or the string you specify in the **aaa connect-info** *string* command and copies it to Attribute 77.

For example, in the following configuration the **class-vc** command is configured on both ATM PVCs 10/42 and 10/43 and the **aaa connect-info** command is configured on PVC 10/42:

```
interface ATM1/0/0.1 multipoint
description TDSL clients - default TDSL 1024 no ip mroute-cache
class-int speed:ubr:1184:160:10
range pvc 10/41 10/160
!
pvc-in-range 10/42
class-vc speed:ubr:2303:224:10
aaa connect-info speed:ubr:2303:224:10:isp-specific-descr
!
pvc-in-range 10/43
class-vc speed:ubr:2303:224:10
```

For PVC 10/42, the router takes the string (speed:ubr:2303:224:10:isp-specific-descr) specified in the **aaa connect-info** command and copies it to Attribute 77. If the **aaa connect-info** command is not configured on the subinterface, the router takes the class name (speed:ubr:2303:224:10) specified in the **class-vc** command and copies it to Attribute 77.

For PVC 10/43, the router takes the class name (speed:ubr:2303:224:10) specified in the **class-vc** command and copies it to Attribute 77.

How to Verify the Connect-Info RADIUS Attribute 77

Verifying the Connect-Info RADIUS Attribute 77

To verify attribute 77 in your accounting “start” and “stop” records, use the **debug radius** command in privileged EXEC mode.

SUMMARY STEPS

1. **enable**
2. **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug radius** **Example:** `Router# debug radius`	Displays information associated with RADIUS.

Example

The following example shows the Connect-Info [77] accounting attributes:

```
Router# debug radius
Sep 8 21:53:05.242: RADIUS/ENCODE(00007D34):Orig. component type = PPPoE
Sep 8 21:53:05.242: RADIUS: AAA Unsupported Attr: interface [208] 10
Sep 8 21:53:05.242: RADIUS: 30 2F 31 2F 30 2F 39 2E [ 0/1/0/9.]
Sep 8 21:53:05.242: RADIUS: AAA Unsupported Attr: client-mac-address[45] 14
Sep 8 21:53:05.242: RADIUS: 30 30 30 30 2E 63 30 30 31 2E 30 31 [ 0000.c001.01]
Sep 8 21:53:05.242: RADIUS(00007D34): Config NAS IP: 0.0.0.0
Sep 8 21:53:05.242: RADIUS/ENCODE(00007D34): acct_session_id: 32042
Sep 8 21:53:05.242: RADIUS(00007D34): sending
Sep 8 21:53:05.242: RADIUS/ENCODE: Best Local IP-Address 10.3.8.2 for Radius-Server 10.3.1.107

Sep 8 21:53:05.242: RADIUS(00007D34): Send Access-Request to 10.3.1.107:1645 id 1645/1, len
 116
Sep 8 21:53:05.242: RADIUS: authenticator FC 82 50 DB 65 8F 21 A9 - F3 0A A8 09 29 E5 56
65
Sep 8 21:53:05.242: RADIUS: Framed-Protocol [7] 6 PPP [1]
Sep 8 21:53:05.242: RADIUS: User-Name [1] 8 ''user1''
Sep 8 21:53:05.242: RADIUS: User-Password [2] 18 *
Sep 8 21:53:05.242: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
Sep 8 21:53:05.242: RADIUS: NAS-Port [5] 6 0
Sep 8 21:53:05.242: RADIUS: NAS-Port-Id [87] 12 ''0/1/0/9.32''
Sep 8 21:53:05.242: RADIUS: Connect-Info [77] 28 ''speed:ubr:3456:448:10/0000''
Sep 8 21:53:05.242: RADIUS: Service-Type [6] 6 Framed [2]
Sep 8 21:53:05.242: RADIUS: NAS-IP-Address [4] 6 10.3.8.2
Sep 8 21:53:05.242: RADIUS(00007D34): Started 5 sec timeout
Sep 8 21:53:05.244: RADIUS: Received from id 1645/1 10.3.1.107:1645, Access-Accept, len 32

Sep 8 21:53:05.244: RADIUS: authenticator 9A F1 29 01 66 53 17 CB - 73 FB 1B CE 7D 80 04
F2
Sep 8 21:53:05.244: RADIUS: Service-Type [6] 6 Framed [2]
Sep 8 21:53:05.244: RADIUS: Framed-Protocol [7] 6 PPP [1]
Sep 8 21:53:05.244: RADIUS(00007D34): Received from id 1645/1
Sep 8 21:53:05.248: RADIUS/ENCODE(00007D34):Orig. component type = PPPoE
Sep 8 21:53:05.248: RADIUS(00007D34): Config NAS IP: 0.0.0.0
Sep 8 21:53:05.248: RADIUS(00007D34): sending
Sep 8 21:53:05.248: RADIUS/ENCODE: Best Local IP-Address 10.3.8.2 for Radius-Server 5.3.1.107

Sep 8 21:53:05.248: RADIUS(00007D34): Send Accounting-Request to 10.3.1.107:1646 id 1646/3,
 len 126
Sep 8 21:53:05.248: RADIUS: authenticator 71 6E 73 9B FD 7E 82 81 - 10 2A CD 83 A8 BD D2
F0
```

```
Sep 8 21:53:05.248: RADIUS: Acct-Session-Id [44] 10 ''00007D2A''
Sep 8 21:53:05.248: RADIUS: Framed-Protocol [7] 6 PPP [1]
Sep 8 21:53:05.248: RADIUS: User-Name [1] 8 ''user1''
Sep 8 21:53:05.248: RADIUS: Acct-Authentic [45] 6 RADIUS [1]
Sep 8 21:53:05.248: RADIUS: Acct-Status-Type [40] 6 Start [1]
Sep 8 21:53:05.248: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
Sep 8 21:53:05.248: RADIUS: NAS-Port [5] 6 0
Sep 8 21:53:05.248: RADIUS: NAS-Port-Id [87] 12 ''0/1/0/9.32''
Sep 8 21:53:05.248: RADIUS: Connect-Info [77] 28 ''speed:ubr:3456:448:10/0000
```

Configuration Example for Connect-Info RADIUS Attribute 77

Example: Configure NAS for AAA and Incoming Modem Calls

The following example is a sample NAS configuration for AAA and incoming modem calls:

```
interface Serial0:15
  no ip address
  isdn switch-type primary-net5
  isdn incoming-voice modem
!
interface Async1
  ip address 192.0.2.2 255.255.255.0
  encapsulation ppp
  async default routing
  async mode interactive
  no peer default ip address
  ppp authentication chap
!
line 1
  modem InOu
  transport preferred none
  transport input all
  autoselect ppp
!
```

Additional References

The following sections provide references related to the Connect-Info RADIUS Attribute 77 feature.

Related Documents

Related Topic	Document Title
IOS dial technologies	Cisco IOS XE Dial Technologies Configuration Guide, Release 2
	Cisco IOS Dial Technologies Command Reference
Security commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2869	RADIUS Extensions

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

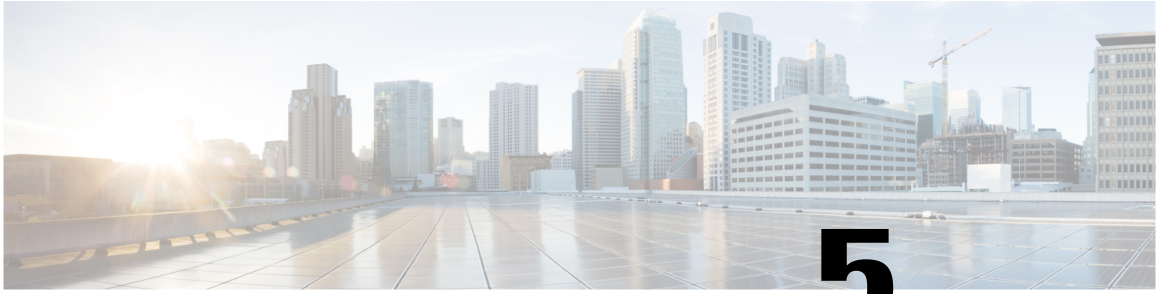
Feature Information for Connect-Info RADIUS Attribute 77

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 10: Feature Information for Connect-Info RADIUS Attribute 77

Feature Name	Releases	Feature Information
Connect-Info RADIUS Attribute 77	12.2(11)T 12.2(33)SRC	The Connect-Info RADIUS Attribute 77 feature enables the network access server (NAS) to report Connect-Info (attribute 77) in RADIUS accounting “start” and “stop” records that are sent to the RADIUS client (dial-in modem). These “start” and “stop” records allow the transmit and receive connection speeds, modulation, and compression to be compared in order to analyze a user session over a dial-in modem where speeds are often different at the end of the connection (after negotiation). This feature was introduced on Cisco IOS Release 12.2(11)T. This feature was integrated into Cisco IOS Release 12.2(33)SRC. This feature supports the following platforms: • Cisco AS5300 series • Cisco AS5400 series • Cisco AS5800 series • Cisco AS5850 series



CHAPTER 5

Encrypted Vendor-Specific Attributes

The Encrypted Vendor-Specific Attributes feature provides users with a way to centrally manage filters at a RADIUS server and supports the following types of string vendor-specific attributes (VSAs):

- Tagged String VSA, on page 72 (similar to Cisco VSA type 1 (Cisco:AVPair (1)) except that this new VSA is tagged)
- Encrypted String VSA, on page 72 (similar to Cisco VSA type 1 except that this new VSA is encrypted)
- Tagged and Encrypted String VSA, on page 73 (similar to Cisco VSA type 1 except that this new VSA is tagged and encrypted)

Cisco:AVPairs specify additional authentication and authorization information in the form an Attribute-Value Pair (AVPair) string. When Internet Engineering Task Force (IETF) RADIUS attribute 26 (Vendor-Specific) is transmitted with a vendor-Id number of "9" and a vendor-type value of "1" (which means that it is a Cisco AVPair), the RADIUS user profile format for a Cisco AVPair looks as follows: Cisco:AVPair = "protocol:attribute=value".

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Encrypted Vendor-Specific Attributes

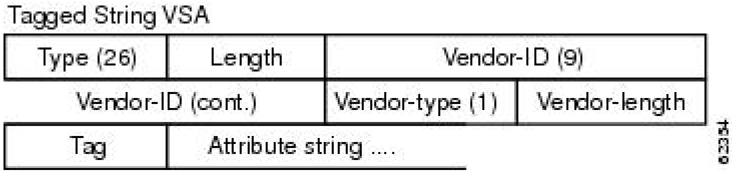
Before the RADIUS server can accept tagged and encrypted VSAs, you must configure your server for AAA authentication and authorization and to accept PPP calls. See the Prerequisites for Encrypted Vendor-Specific Attributes, on page 72 for documents that explain how to perform these tasks.

Information About Encrypted Vendor-Specific Attributes

Tagged String VSA

The figure below displays the packet format for the Tagged String VSA:

Figure 3: Tagged String VSA Format



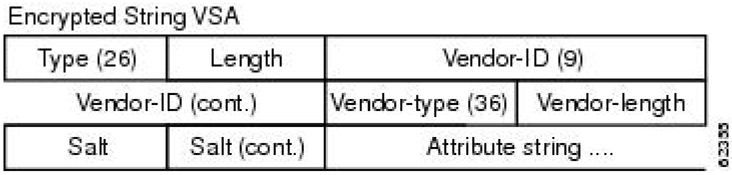
Type (26)	Length	Vendor-ID (9)	
Vendor-ID (cont.)		Vendor-type (1)	Vendor-length
Tag	Attribute string		

To retrieve the correct value, the Tag field must be parsed correctly. The value for this field can range only from 0x01 through 0x1F. If the value is not within the specified range, the RADIUS server ignores the value and considers the Tag field to be a part of the Attribute String field.

Encrypted String VSA

The figure below displays the packet format for the Encrypted String VSA:

Figure 4: Encrypted String VSA Format



Type (26)	Length	Vendor-ID (9)	
Vendor-ID (cont.)		Vendor-type (36)	Vendor-length
Salt	Salt (cont.)	Attribute string	

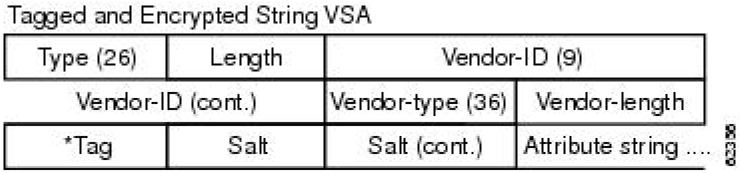
The Salt field ensures the uniqueness of the encryption key that is used to encrypt each instance of the VSA. The first and most significant bit of the Salt field must be set to 1.

Note Vendor-type (36) indicates that the attribute is an encrypted string VSA.

Tagged and Encrypted String VSA

The figure below displays the packet formats for each of the newly supported VSAs:

Figure 5: Tagged and Encrypted String VSA Format



Tagged and Encrypted String VSA

Type (26)	Length	Vendor-ID (9)	
Vendor-ID (cont.)		Vendor-type (36)	Vendor-length
*Tag	Salt	Salt (cont.)	Attribute string ....

This VSA is similar to encrypted string VSAs except this VSA has an additional Tag field. If the Tag field is not within the valid range (0x01 through 0x1F), it is considered to be part of the Salt field.

How to Verify Encrypted Vendor-Specific Attributes

The Encrypted Vendor-Specific Attributes feature requires no configuration. To verify that RADIUS-tagged and encrypted VSAs are being sent from the RADIUS server, use the following command in privileged EXEC mode:

Command	Purpose
`Router#` **debug radius**	Displays information associated with RADIUS. The output of this command shows whether tagged and encrypted VSAs are being sent from the RADIUS server.

Configuration Examples for Encrypted Vendor-Specific Attributes

NAS Configuration Example

The following example shows how to configure a network access server (NAS) with a basic configuration using tagged and encrypted VSAs. (This example assumes that the configuration required to make PPP calls is already enabled.)

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
!
radius-server host 10.2.2.2 auth-port 1645 acct-port 1646
radius-server key cisco
```

RADIUS User Profile with a Tagged and Encrypted VSA Example

The following is an example of user profile on a RADIUS server that supports tagged and encrypted string VSAs:

```
mascot   Password = "password1"
         Service-Type = NAS-Prompt,
         Framed-Protocol = PPP,
         Cisco:Cisco-Enc = "ip:route=10.0.0.0 255.0.0.0"
         Cisco.attr Cisco-Enc 36 tag-encstr(*,*)
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
RADIUS Attributes	*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2
Media-Independent PPP and Multilink PPP	Configuring Media-Independent PPP and Multilink PPP feature module.
Authentication	Configuring Authentication feature module.
Authorization	Configuring Authorization feature module.

Standards

Standard	Title
None.	--

MIBs

MIB	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2865	*Remote Authentication Dial In User Service (RADIUS)*
RFC 2868	*RADIUS Attributes for Tunnel Protocol Support*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Encrypted Vendor-Specific Attributes

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 11: Feature Information for Encrypted Vendor-Specific Attributes

Feature Name	Releases	Feature Information
Encrypted Vendor-Specific Attributes	12.2(8)T 12.2(28)SB 12.2(33)SRC	The Encrypted Vendor-Specific Attributes feature provides users with a way to centrally manage filters at a RADIUS server and supports the Tagged String, Encrypted String, and Tagged and Encrypted String vendor-specific attributes (VSAs). This feature was introduced in Cisco IOS Release 12.2(8)T. This feature was integrated into Cisco IOS Release 12.2(28)SB. This feature was integrated into Cisco IOS Release 12.2(33)SRC.

CHAPTER 6

RADIUS Attribute 5 NAS-Port Format Specified on a Per-Server Group Level

The RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level feature allows configurations to be customized for different RADIUS server groups. This flexibility allows customized network access server- (NAS-) port formats to be used instead of global formats.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for RADIUS Attribute 5 NAS-Port Format Specified on a Per-Server Group Level

- You must be running a Cisco IOS image that contains the authentication, authorization, and accounting (AAA) component.

Information About RADIUS Attribute 5 NAS-Port Format Specified on a Per-Server Group Level

RADIUS Attribute 5 Format Customization

Prior to Cisco IOS Release 12.3(14)T, Cisco IOS software allowed RADIUS attributes that were sent in access requests or accounting requests to be customized on a global basis. You could customize how each configurable attribute should function when communicating with a RADIUS server. Since the implementation of server groups, global attribute configurations were not flexible enough to address the different customizations that were required to support the various RADIUS servers with which a router might be interacting. For example, if you configured the **global radius-server attribute nas-port format command**option, every service on the router that interacted with a RADIUS server was used in the same way.

Effective with Cisco IOS Release 12.3(14)T, you can configure your router to support override flexibility for per-server groups. You can configure services to use specific named methods for different service types on a RADIUS server. The service types can be set to use their own respective service groups. This flexibility allows customized NAS-port formats to be used instead of the global formats.

How to Configure RADIUS Attribute 5 NAS-Port Format Specified on a Per-Server Group Level

Configuring the RADIUS Attribute 5 Format on a Per-Server Group Level

To configure your router to support the RADIUS Attribute 5 format on a per-server group level, perform the following steps.

Note To use this per-server group capability, you must actively use a named method list within your services. You can configure one client to use a specific named method while other clients use the default format.

Before You Begin

Before performing these steps, you should first configure method lists for AAA as is applicable for your situation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group-name*
4. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
5. **attribute nas-port format** *format-type* [*string*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa group server radius** *group-name* **Example:** `Router (config)# aaa group server radius radius1`	Groups different RADIUS server hosts into distinct lists and distinct methods and enters server-group configuration mode.
Step 4	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] **Example:** `Router (server-group)# server 172.101.159.172 auth-port 1645 acct-port 1646`	Configures the IP address of the RADIUS server for the group server.
Step 5	**attribute nas-port format** *format-type* [*string*] **Example:** `Router (server-group)# attribute nas-port format d`	Configures a service to use specific named methods for different service types. • The service types can be set to use their own respective server groups.

Monitoring and Maintaining RADIUS Attribute 5 Format on a Per-Server Group Level

To monitor and maintain RADIUS Attribute 5 Format on a Per-Server Group Level, perform the following steps (the **debug** commands may be used separately):

SUMMARY STEPS

1. **enable**
2. **debug aaa sg-server selection**
3. **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug aaa sg-server selection** **Example:** `Router# debug aaa sg-server selection`	Displays information about why the RADIUS and TACACS+ server group system in a router is choosing a particular server.
Step 3	**debug radius** **Example:** `Router# debug radius`	Displays information showing that a server group has been selected for a particular request.

Configuration Examples for RADIUS Attribute 5 NAS-Port Format Specified on a Per-Server Group Level

RADIUS Attribute 5 Format Specified on a Per-Server Level Example

The following configuration example shows a leased-line PPP client that has chosen to send no RADIUS Attribute 5 while the default is to use format F:\tips-migration

```
interface Serial2/0
```

```
 no ip address
 encapsulation ppp
 ppp accounting SerialAccounting
 ppp authentication pap
aaa accounting network default start-stop group radius
aaa accounting network SerialAccounting start-stop group group1
aaa group server radius group1
 server 10.101.159.172 auth-port 1645 acct-port 1646
 attribute nas-port none
radius-server host 10.101.159.172 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
```

Additional References

The following sections provide references related to RADIUS Vendor-Specific Attributes (VSA) and RADIUS Disconnect-Cause Attribute Values.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands	*Cisco IOS Security Command Reference*
Security Features	*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2
Security Server Protocols	Security Server Protocols section of the *Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2
RADIUS Configuration	Configuring RADIUS feature module.

Standards

Standard	Title
Internet Engineering Task Force (IETF) Internet Draft: Network Access Servers Requirements	Network Access Servers Requirements: Extended RADIUS Practices

MIBs

MIB	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2865	Remote Authentication Dial In User Service (RADIUS)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

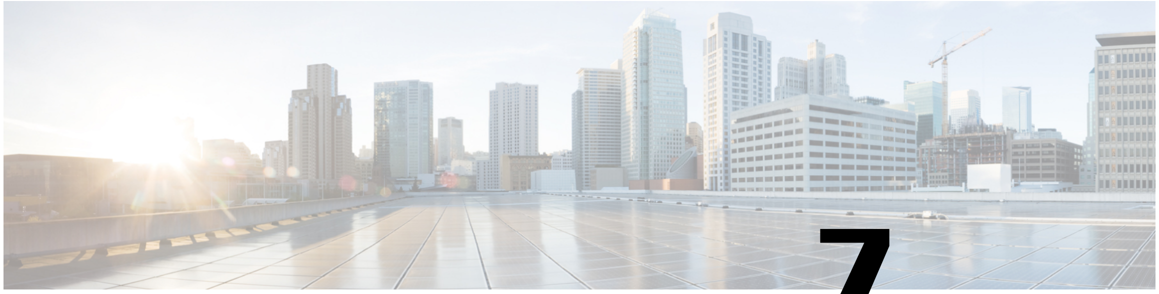
Feature Information for RADIUS Attribute 5 NAS-Port Format Specified on a Per-Server Group Level

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 12: Feature Information for RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level

Feature Name	Releases	Feature Information
RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level	12.3(14)T	The RADIUS Attribute 5 (NAS-Port) Format Specified on a Per-Server Group Level feature allows configurations to be customized for different RADIUS server groups. This flexibility allows customized network access server- (NAS-) port formats to be used instead of global formats. This feature was introduced in Cisco IOS Release 12.3(14)T. The following commands were introduced or modifieF:\tips-migration **attribute nas-port format**.



CHAPTER 7

RADIUS Attribute 8 Framed-IP-Address in Access Requests

The RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature makes it possible for a network access server (NAS) to provide the RADIUS server with a hint of the user IP address in advance of user authentication. An application can be run on the RADIUS server to use this hint and build a table (map) of user names and IP addresses. With the RADIUS server, service applications can begin preparing user login information to have available in advance of a successful user authentication with the RADIUS server.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for RADIUS Attribute 8 Framed-IP-Address in Access Requests

Sending RADIUS attribute 8 in the RADIUS access requests assumes that the login host has been configured to request its IP address from the NAS server. It also assumes that the login host has been configured to accept an IP address from the NAS.

The NAS must be configured with a pool of network addresses on the interface supporting the login hosts.

Information About RADIUS Attribute 8 Framed-IP-Address in Access Requests

When a network device dials in to a NAS that is configured for RADIUS authentication, the NAS begins the process of contacting the RADIUS server in preparation for user authentication. Typically, the IP address of the dial-in host is not communicated to the RADIUS server until after successful user authentication. Communicating the device IP address to the server in the RADIUS access request allows other applications to begin to take advantage of that information.

As the NAS is setting up communication with the RADIUS server, the NAS assigns an IP address to the dial-in host from a pool of IP addresses configured at the specific interface. The NAS sends the IP address of the dial-in host to the RADIUS server as attribute 8. At that time, the NAS sends other user information, such as the user name, to the RADIUS server.

After the RADIUS server receives the user information from the NAS, it has two options:

- If the user profile on the RADIUS server already includes attribute 8, the RADIUS server can override the IP address sent by the NAS with the IP address defined as attribute 8 in the user profile. The address defined in the user profile is returned to the NAS.
- If the user profile does not include attribute 8, the RADIUS server can accept attribute 8 from the NAS, and the same address is returned to the NAS.

The address returned by the RADIUS server is saved in memory on the NAS for the life of the session. If the NAS is configured for RADIUS accounting, the accounting start packet sent to the RADIUS server includes the same IP address as in attribute 8. All subsequent accounting packets, updates (if configured), and stop packets will also include the same IP address provided in attribute 8.

However, the RADIUS attribute 8 (Framed-IP-Address) is not included in the accounting start packets in the following two conditions. In both these conditions, use the **aaa accounting delay-start extended-time** *delay-value* command to delay the Internet Protocol Control Protocol version 6 (IPCPv6) address negotiation using the configured delay value. During the delay the IPCPv4 address is posted and the framed IPv4 address is added to the accounting “start” packet.

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

How to Configure RADIUS Attribute 8 Framed-IP-Address in Access Requests

Configuring RADIUS Attribute 8 in Access Requests

To send RADIUS attribute 8 in the access request, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute 8 include-in-access-req**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server attribute 8 include-in-access-req** **Example:** `Router(config)# radius-server attribute 8 include-in-access-req`	Sends RADIUS attribute 8 in access-request packets.

Verifying RADIUS Attribute 8 in Access Requests

To verify that RADIUS attribute 8 is being sent in access requests, perform the following steps. Attribute 8 should be present in all PPP access requests.

SUMMARY STEPS

1. **enable**
2. **more system:running-config**
3. **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**more system:running-config** **Example:** `Router# more system:running-config`	Displays the contents of the current running configuration file. (Note that the **more system:running-config** command has replaced the **show running-config** command.)
Step 3	**debug radius** **Example:** `Router# debug radius`	Displays information associated with RADIUS. The output of this command shows whether attribute 8 is being sent in access requests.

Configuration Examples for RADIUS Attribute 8 Framed-IP-Address in Access Requests

NAS Configuration That Sends the IP Address of the Dial-in Host to the RADIUS Server in the RADIUS Access Request

The following example shows a NAS configuration that sends the IP address of the dial-in host to the RADIUS server in the RADIUS access request. The NAS is configured for RADIUS authentication, authorization, and accounting (AAA). A pool of IP addresses (async1-pool) has been configured and applied at interface Async1.

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
ip address-pool local
!
```

```
interface Async1
 peer default ip address pool async1-pool
!
ip local pool async1-pool 209.165.200.225 209.165.200.229
!
radius-server host 172.31.71.146 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 8 include-in-access-req
radius-server key radhost<xxx>: Example
```

Additional References

The following sections provide references related to the RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature.

Related Documents

Related Topic	Document Title
Configuring authentication and configuring RADIUS	" Configuring Authentication " and "Configuring RADIUS " chapters, *Cisco Security Configuration Guide*
RFC 2138 (RADIUS)	RFC 2138 , Remote Authentication Dial In User Service (RADIUS)

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

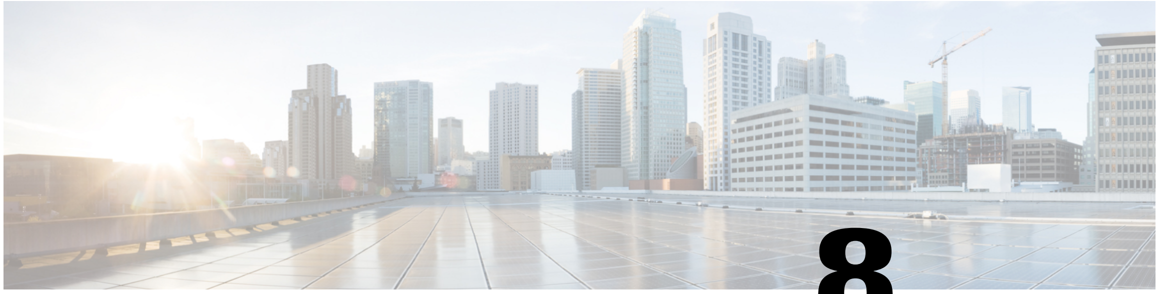
Feature Information for RADIUS Attribute 8 Framed-IP-Address in Access Requests

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 13: Feature Information for RADIUS Attribute 8 (Framed-IP-Address) in Access Requests

Feature Name	Releases	Feature Information
RADIUS Attribute 8 (Framed-IP-Address) in Access Requests	12.2(11)T 12.2(28)SB 12.2(33)SRC	The RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature makes it possible for a network access server (NAS) to provide the RADIUS server with a hint of the user IP address in advance of user authentication. An application can be run on the RADIUS server to use this hint and build a table (map) of user names and IP addresses. With the RADIUS server, service applications can begin preparing user login information to have available in advance of a successful user authentication with the RADIUS server. The following commands were introduced or modified: **radius-server attribute 8 include-in-access-req**.



CHAPTER 8

RADIUS Attribute 82 Tunnel Assignment ID

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for RADIUS Attribute 82 Tunnel Assignment ID

You must be using a Cisco platform that supports VPDN to use this feature.

Restrictions for Radius Attribute 82 Tunnel Assignment ID

This feature is designed only for VPDN dial-in applications. It does not support VPDN dial-out.

Information about RADIUS Attribute 82 Tunnel Assignment ID

The RADIUS Attribute 82: Tunnel Assignment ID feature allows the Layer 2 Transport Protocol access concentrator (LAC) to group users from different per-user or domain RADIUS profiles into the same active tunnel. The RADIUS Attribute 82: Tunnel Assignment ID feature defines a new avpair, Tunnel-Assignment-ID, which allows the LAC to group users from different RADIUS profiles into the same tunnel if the chosen endpoint, tunnel type, and Tunnel-Assignment-ID are identical. This feature introduces new software functionality. No new commands are introduced with this feature.

How to Verify if RADIUS Attribute 82 is Being Used by the LAC

There are no configuration steps for the RADIUS Attribute 82: Tunnel Assignment ID feature. This task verifies the RADIUS attribute 82 used by the LAC during tunnel authorization.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Router# **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	Router# **debug radius** **Example:** `Router# debug radius`	Displays information associated with RADIUS. The output of this command shows whether attribute 82 is being sent in access requests.

Configuration Examples for RADIUS Attribute 82 Tunnel Assignment ID

LAC Configuration Example

The following example shows a sample LAC configuration when the VPDN group is defined on the router:

```
aaa new-model
aaa authentication ppp default local
aaa authorization network default local
!
bba-group pppoe bba_group1
virtual-template 1
!
interface Loopback1
no ip address
vpdn-group VPDN_LAC1
request-dialin
protocol l2tp
local name tb162_LAC1
domain isp1.com
initiate-to ip 10.0.0.2
source-ip 10.0.0.1
l2tp tunnel receive-window 100
l2tp tunnel nosession-timeout 30
l2tp tunnel retransmit retries 5
l2tp tunnel retransmit timeout min 2
l2tp tunnel retransmit timeout max 8
l2tp tunnel hello 60
l2tp tunnel password tunnel1
!
!
interface virtual-template 1
no snmp trap link-status
no keepalive
ip unnumbered loopback1
ppp mtu adaptive
ppp authentication pap
no logging event link-status
!
```

The following example shows a sample LAC configuration when the VPDN group is defined in RADIUS:

```
aaa authentication ppp default group radius
aaa authorization network default radius
!
bba-group pppoe bba_group1
virtual-template 1
!
interface Loopback1
no ip address
interface virtual-template 1
no snmp trap link-status
no keepalive
ip unnumbered loopback1
ppp mtu adaptive
ppp authentication pap
no logging event link-status
```

LNS Configuration Example

The following example configures VPDN on the LNS:

```
hostname lns
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
vpdn enable
vpdn-group VPDN_LNS1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname tb162_LAC1
 local name LNS1
 l2tp tunnel hello 90
 l2tp tunnel password 0 hello1
interface Loopback0
 ip address 10.1.1.3 255.255.255.0
interface Virtual-Template1
 ip unnumbered Loopback0
 no keepalive
 peer default ip address pool mypool
 ppp authentication chap
ip local pool mypool 10.1.1.10 10.1.1.50
radius-server host lns-radiusd  auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
```

RADIUS Configuration Example

The following examples configure the RADIUS server to group sessions in a tunnel:

Per-User Configuration

```
user@router.com Password = "cisco" Service-Type = Outbound,
       Tunnel-Type = :1:L2TP,
       Tunnel-Server-Endpoint = :1:"10.14.10.54",
       Tunnel-Assignment-Id = :1:"router"
client@router.com Password = "cisco" Service-Type = Outbound,
       Tunnel-Type = :1:L2TP,
       Tunnel-Server-Endpoint = :1:"10.14.10.54",
       Tunnel-Assignment-Id = :1:"router"
```

Domain Configuration

```
eng.router.com Password = "cisco" Service-Type = Outbound,
        Tunnel-Type = :1:L2TP,
        Tunnel-Server-Endpoint = :1:"10.14.10.54",
        Tunnel-Assignment-Id = :1:"router"
sales.router.com Password = "cisco" Service-Type = Outbound,
        Tunnel-Type = :1:L2TP,
        Tunnel-Server-Endpoint = :1:"10.14.10.54",
        Tunnel-Assignment-Id = :1:"router"
```

Additional References

The following sections provide references related to RADIUS Tunnel Attribute Extensions.

Related Documents

Related Topic	Document Title
Authentication	“ Configuring Authentication ” module.
RADIUS Attributes	“ RADIUS Attributes Overview and RADIUS IETF Attributes ” module.
Virtual private dialup networks (VPDN)	*Cisco IOS VPDN Configuration Guide* , Release 15.0.

Standards

Standard	Title
None.	--

MIBs

MIB	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2868	RADIUS Attributes for Tunnel Protocol Support

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for RADIUS Attribute 82 Tunnel Assignment ID

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 14: Feature Information for RADIUS Attribute 82: Tunnel Assignment ID

Feature Name	Releases	Feature Information
RADIUS Attribute 82: Tunnel Assignment Id	12.2(4)T 12.2(4)T3 12.2(11)T 12.2(27)SB	The RADIUS Attribute 82: Tunnel Assignment ID feature allows the Layer 2 Transport Protocol access concentrator (LAC) to group users from different per-user or domain RADIUS profiles into the same active tunnel. This feature was introduced in 12.2(4)T. In 12.2(4)T3, support for the Cisco 7500 series routers was added. This feature was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800 and Cisco AS5850 platforms. This feature was integrated into Cisco IOS Release 12.2(27)SB.

CHAPTER 9

RADIUS Attribute 104

The RADIUS Attribute 104 feature allows private routes (attribute 104) to be specified in a RADIUS authorization profile. The private routes affect only packets that are received on an individual interface. The routes are stored apart from the global routing table and are not injected into any routing protocols for redistribution.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for RADIUS Attribute 104

- You must be using a Cisco RADIUS server.
- You should be familiar with configuring RADIUS.
- You should be familiar with policy-based routing (PBR) and private routes.

- You should be familiar with configuring access control lists (ACLs).
- Before using the RADIUS Attribute 104 feature, you must configure RADIUS AAA authorization and RADIUS route download.
- The following memory bytes are requireF:\tips-migration
    - One route map--50 bytes.
    - One match-set clause--600 bytes.
    - One extended ACL--366 bytes.
    - For N number of attribute 104s, the memory requirement is (600+366)*N+50=1000*N(approximate) per user.

Restrictions for RADIUS Attribute 104

- If you already have PBR locally (statically) configured under the interface, and you specify attribute 104, the locally configured PBR will be disabled.
- If a pseudo next-hop address is involved, there must be a route available in the routing table for the next-hop address. If a route is not available, the packet will not be policy routed.
- Policy routing does not order the match-set clauses and relies on the first match, so you should specify the attributes in the order in which you want them to be matched.
- Metric numbers cannot be used in the attribute.

Information About RADIUS Attribute 104

Policy-Based Routing Background

PBR provides a mechanism for the forwarding, or routing of, data packets on the basis of defined policies. The policies are not wholly dependent on the destination address but rather on other factors, such as type of service, source address, precedence, port numbers, or protocol type.

Policy-based routing is applied to incoming packets. All packets that are received on an interface that has policy-based routing enabled are considered for policy-based routing. The router passes the packets through enhanced packet filters called route maps. On the basis of the criteria that are defined in the route maps, the packets are forwarded to the appropriate next hop.

Each entry in a route map statement contains a combination of match clauses and set clauses or commands. The match clauses define the criteria for whether appropriate packets meet the particular policy (that is, whether the conditions are met). The set clauses provide instruction for how the packets should be routed after they have met the match criteria. The match clause specifies which set of filters a packet must match for the corresponding set clause to be applied.

Attribute 104 and the Policy-Based Route Map

This section discusses the attribute 104 feature and how it works with policy-based route maps.

RADIUS Attribute 104 Overview

Using the RADIUS Attribute 104 feature, you can specify private routes in your RADIUS authorization profile. The private routes you specify will affect only packets that are received on an individual interface. The routes are stored apart from the global routing table and are not injected into any routing protocols for redistribution.

Permit Route Map

Route map statements can be marked as "permit" or "deny." If the statement is marked "permit," the set clause is applied to the packets that match the match criteria. For attribute 104, when you are configuring the route map, you need to mark the route map as "permit," as follows. See Related Documents, on page 107 for where to find information on configuring a route map.

Default Private Route

The policy routing process proceeds through the route map until a match is found. If no match is found in the route map, the global routing table is consulted. If you have specified a default route in your user profile, any further routes beyond the default route are effectively ignored.

Route Map Order

You need to specify route maps on the server in the order that you want them to be applied.

How to Apply RADIUS Attribute 104

Applying RADIUS Attribute 104 to Your User Profile

You can apply RADIUS attribute 104 to your user profile by adding the following to the RADIUS server database.

SUMMARY STEPS

1. Apply RADIUS attribute 104 to your user profile.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Apply RADIUS attribute 104 to your user profile.	`Ascend-Private-Route=”dest_addr/netmask next_hop”` The destination network address of the router is “dest_addr/netmask”, and the address of the next-hop router is “next_hop.”

Examples

The following is a sample user profile that creates three private routes that are associated with the caller:

```
username Password="ascend"; User-Service=Framed-User
   Framed-Protocol=PPP,
   Framed-Address=10.1.1.1,
   Framed-Netmask=255.0.0.0,
   Ascend-Private-Route="172.16.1.1/16 10.10.10.1"
   Ascend-Private-Route="192.168.1.1/32 10.10.10.2"
   Ascend-Private-Route="10.20.0.0/1 10.10.10.3"
   Ascend-Private-Route="10.0.0.0/0 10.10.10.4"
```

Using the above profile, the private routing table for the connection contains the following routes, including a default route:

```
Destination/Mask     Gateway
172.16.1.1/16         10.10.10.1
192.168.1.1/32         10.10.10.2
10.20.20.20/1       10.10.10.3
10.0.0.0/0            10.10.10.4
```

Verifying Route Maps

You can use the following **show** commands to verify the route maps that have been configured.

SUMMARY STEPS

1. **enable**
2. **show ip policy**
3. **show route-map** [*map-name* | **dynamic** [*dynamic-map-name* | **application** [*application-name*]] | **all**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show ip policy** **Example:** `Router# show ip policy`	Displays the route map that is used for policy routing.
Step 3	**show route-map** [*map-name* | **dynamic** [*dynamic-map-name* | **application** [*application-name*]] | **all**] **Example:** `Router# show route-map`	Displays all route maps that are configured or only the one that is specified.

Troubleshooting the RADIUS Profile

If your private route configuration is not working properly, you may want to reread the section "Policy-Based Routing Background, on page 102." This section may help you determine what is happening to the packets. In addition, the following **debug** commands can be used to troubleshoot your RADIUS profile.

SUMMARY STEPS

1. **enable**
2. **debug radius**
3. **debug aaa per-user**
4. debug ip policy

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug radius** **Example:** `Router# debug radius`	Displays information associated with RADIUS.

	Command or Action	Purpose
Step 3	**debug aaa per-user** **Example:** `Router# debug aaa per-user`	Displays the attributes that are applied to each user as the user authenticates.
Step 4	debug ip policy **Example:** `Router# debug ip policy`	Displays IP routing packet activity.

Configuration Examples for RADIUS Attribute 104

Route-Map Configuration in Which Attribute 104 Has Been Applied Example

The following output is a typical route-map configuration to which attribute 104 has been applieF:\tips-migration

```
Router# show route-map dynamic
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 0, identifier 1639994476
  Match clauses:
    ip address (access-lists): PBR#1 PBR#2
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 1, identifier 1640264784
  Match clauses:
    ip address (access-lists): PBR#3 PBR#4
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 2, identifier 1645563704
  Match clauses:
    ip address (access-lists): PBR#5 PBR#6
    length 10 100
  Set clauses:
    ip next-hop 10.1.1.1
    ip gateway10.1.1.1
  Policy routing matches: 0 packets, 0 bytes
 Current active dynamic routemaps = 1
```

Additional References

The following sections provide references related to RADIUS NAS-IP-Address Attribute Configurability.

Related Documents

Related Topic	Document Title
Configuring AAA	“Authentication, Authorization, and Accounting (AAA)” section of *Cisco IOS Security Configuration Guide: Securing User Services*
Configuring RADIUS	“ Configuring RADIUS ” module.
RADIUS commands	*Cisco IOS Security Command Reference*

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for RADIUS Attribute 104

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 15: Feature Information for RADIUS Attribute 104

Feature Name	Releases	Feature Information
RADIUS Attribute 104	12.3(7)T	The RADIUS Attribute 104 feature allows private routes (attribute 104) to be specified in a RADIUS authorization profile. The private routes affect only packets that are received on an individual interface. The routes are stored apart from the global routing table and are not injected into any routing protocols for redistribution. This feature was introduced in Cisco IOS Release 12.3(7)T. The following commands were introduced or modifieF:\tips-migration **show ip policy**, **show route-map**.

CHAPTER 10

RADIUS Tunnel Attribute Extensions

The RADIUS Tunnel Attribute Extensions feature allows a name to be specified (other than the default) for the tunnel initiator and the tunnel terminator in order to establish a higher level of security when setting up VPN tunneling.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for RADIUS Tunnel Attribute Extensions

To use RADIUS attributes 90 and 91, you must complete the following tasks:

- Configure your NAS to support AAA.

- Configure your NAS to support RADIUS.
- Configure your NAS to support VPN.

Restrictions for RADIUS Tunnel Attribute Extensions

Your RADIUS server must support tagged attributes to use RADIUS tunnel attributes 90 and 91.

Information About RADIUS Tunnel Attribute Extensions

The RADIUS Tunnel Attribute Extensions feature introduces RADIUS attribute 90 (Tunnel-Client-Auth-ID) and RADIUS attribute 91 (Tunnel-Server-Auth-ID). Both attributes help support the provision of compulsory tunneling in virtual private networks (VPNs) by allowing the user to specify authentication names for the network access server (NAS) and the RADIUS server.

How RADIUS Tunnel Attribute Extensions Work

Once a NAS has set up communication with a RADIUS server, you can enable a tunneling protocol. Some applications of tunneling protocols are voluntary, but others involve compulsory tunneling; that is, a tunnel is created without any action from the user and without allowing the user any choice in the matter. In those cases, new RADIUS attributes are needed to carry the tunneling information from the NAS to the RADIUS server to establish authentication. These new RADIUS attributes are listed in the table below.

Note In compulsory tunneling, any security measures in place apply only to traffic between the tunnel endpoints. Encryption or integrity protection of tunneled traffic must not be considered as a replacement for end-to-end security.

Table 16: RADIUS Tunnel Attributes

Number	IETF RADIUS Tunnel Attribute	Equivalent TACACS+ Attribute	Supported Protocols	Description
90	Tunnel-Client-Auth-ID	tunnel-id	• Layer 2 Forwarding (L2F) • Layer 2 Tunneling Protocol (L2TP)	Specifies the name used by the tunnel initiator (also known as the NAS[4]) when authenticating tunnel setup with the tunnel terminator.

Number	IETF RADIUS Tunnel Attribute	Equivalent TACACS+ Attribute	Supported Protocols	Description
91	Tunnel-Server-Auth-ID	gw-name	• Layer 2 Forwarding (L2F) • Layer 2 Tunneling Protocol (L2TP)	Specifies the name used by the tunnel terminator (also known as the Home Gateway[5]) when authenticating tunnel setup with the tunnel initiator.

[4] When L2TP is used, the NAS is referred to as an L2TP access concentrator (LAC).

[5] When L2TP is used, the Home Gateway is referred to as an L2TP network server (LNS).

RADIUS attribute 90 and RADIUS attribute 91 are included in the following situations:

- If the RADIUS server accepts the request and the desired authentication name is different from the default, they must be included it.
- If an accounting request contains Acct-Status-Type attributes with values of either start or stop and pertains to a tunneled session, they should be included in.

How to Verify RADIUS Attribute 90 and RADIUS Attribute 91

To verify that RADIUS attribute 90 and RADIUS attribute 91 are being sent in access accepts and accounting requests, use the following command in privileged EXEC mode:

Command	Purpose
`Router#` **debug radius**	Displays information associated with RADIUS. The output of this command shows whether attribute 90 and attribute 91 are being sent in access accepts and accounting requests.

Configuration Examples for RADIUS Tunnel Attribute Extensions

L2TP Network Server Configuration Example

The following example shows how to configure the LNS with a basic L2F and L2TP configuration using RADIUS tunneling attributes 90 and 91:

```
aaa new-model
aaa authentication login default none
aaa authentication login console none
aaa authentication ppp default local group radius
aaa authorization network default group radius if-authenticated
!
```

```
username l2f-cli-auth-id password 0 l2f-cli-pass
username l2f-svr-auth-id password 0 l2f-svr-pass
username l2tp-svr-auth-id password 0 l2tp-tnl-pass
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
accept-dialin
protocol l2f
virtual-template 1
terminate-from hostname l2f-cli-auth-id
local name l2f-svr-auth-id
!
vpdn-group 2
accept-dialin
protocol l2tp
virtual-template 2
terminate-from hostname l2tp-cli-auth-id
local name l2tp-svr-auth-id
!
interface Ethernet1/0
ip address 10.0.0.3 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface Virtual-Template1
ip unnumbered Ethernet1/0
ppp authentication pap
!
interface Virtual-Template2
ip unnumbered Ethernet1/0
ppp authentication pap
!
radius-server host 1.1.1.1 auth-port 1645 acct-port 1646
radius-server key <deleted>
!
```

RADIUS User Profile with RADIUS Tunneling Attributes 90 and 91 Example

The following is an example of a RADIUS user profile that includes RADIUS tunneling attributes 90 and 91. This entry supports two tunnels, one for L2F and the other for L2TP. The tag entries with :1 support L2F tunnels, and the tag entries with :2 support L2TP tunnels.

```
cisco.com Password = "cisco", Service-Type = Outbound
Service-Type = Outbound,
Tunnel-Type = :1:L2F,
Tunnel-Medium-Type = :1:IP,
Tunnel-Client-Endpoint = :1:"10.0.0.2",
Tunnel-Server-Endpoint = :1:"10.0.0.3",
Tunnel-Client-Auth-Id = :1:"l2f-cli-auth-id",
Tunnel-Server-Auth-Id = :1:"l2f-svr-auth-id",
Tunnel-Assignment-Id = :1:"l2f-assignment-id",
Cisco-Avpair = "vpdn:nas-password=l2f-cli-pass",
Cisco-Avpair = "vpdn:gw-password=l2f-svr-pass",
Tunnel-Preference = :1:1,
Tunnel-Type = :2:L2TP,
Tunnel-Medium-Type = :2:IP,
Tunnel-Client-Endpoint = :2:"10.0.0.2",
Tunnel-Server-Endpoint = :2:"10.0.0.3",
Tunnel-Client-Auth-Id = :2:"l2tp-cli-auth-id",
Tunnel-Server-Auth-Id = :2:"l2tp-svr-auth-id",
Tunnel-Assignment-Id = :2:"l2tp-assignment-id",
Cisco-Avpair = "vpdn:l2tp-tunnel-password=l2tp-tnl-pass",
Tunnel-Preference = :2:2
```

Additional References

The following sections provide references related to RADIUS Tunnel Attribute Extensions.

Related Documents

Related Topic	Document Title
Authentication	" Configuring Authentication " module.
RADIUS Attributes	" RADIUS Attributes Overview and RADIUS IETF Attributes " module.
Virtual private dialup networks (VPDN)	*Cisco IOS VPDN Configuration Guide* , Release 15.0.

Standards

Standard	Title
None.	--

MIBs

MIB	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2868	RADIUS Attributes for Tunnel Protocol Support

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for RADIUS Tunnel Attribute Extensions

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 17: Feature Information for RADIUS Tunnel Attribute Extensions

Feature Name	Releases	Feature Information
Feature Information for RADIUS Tunnel Attribute Extensions	12.1(5)T 12.2(4)B3 12.2(13)T	The RADIUS Tunnel Attribute Extensions feature allows a name to be specified (other than the default) for the tunnel initiator and the tunnel terminator in order to establish a higher level of security when setting up VPN tunneling. This feature was introduced in Cisco IOS Release 12.1(5)T. This feature was integrated into Cisco IOS Release 12.2(4)B3. This feature was integrated into Cisco IOS Release 12.2(13)T.

Glossary

Layer 2 Forwarding (L2F) --A Layer 2 tunneling protocol that enables an ISP or other access service to create a virtual tunnel to link customer remote sites or remote users with corporate home networks. In particular, a network access server (NAS) at the ISP point of presence (POP) exchanges PPP messages with the remote users and communicates by L2F or L2TP requests and responses with the customer tunnel server to set up tunnels.

Layer 2 Tunnel Protocol (L2TP) --A Layer 2 tunneling protocol that enables an ISP or other access service to create a virtual tunnel to link customer remote sites or remote users with corporate home networks. In particular, a network access server (NAS) at the ISP point of presence (POP) exchanges PPP messages with the remote users and communicates by L2F or L2TP requests and responses with the customer tunnel server to set up tunnels.

L2TP access concentrator (LAC) --A network access server (NAS) to which the client directly connects and through which PPP frames are tunneled to the L2TP network server (LNS). The LAC need only implement the media over which L2TP is to operate to pass traffic to one or more LNSs. The LAC may tunnel any protocol carried within PPP. The LAC initiates incoming calls and receives outgoing calls. A LAC is analogous to an L2F network access server.

L2TP network server (LNS) --A termination point for L2TP tunnels, and an access point where PPP frames are processed and passed to higher-layer protocols. An LNS can operate on any platform that terminates PPP. The LNS handles the server side of the L2TP protocol. L2TP relies only on the single medium over which L2TP tunnels arrive. The LNS initiates outgoing calls and receives incoming calls. An LNS is analogous to a home gateway in L2F technology.

network access server (NAS) --A Cisco platform, or collection of platforms, such as an AccessPath system, that interfaces between the packet world (such as the Internet) and the circuit-switched world (such as the PSTN).

tunnel--A virtual pipe between the L2TP access concentrator (LAC) and L2TP network server (LNS) that can carry multiple PPP sessions.

virtual private network (VPN)--A system that permits dial-in networks to exist remotely to home networks, while giving the appearance of being directly connected. VPNs use L2TP and L2F to terminate the Layer 2 and higher parts of the network connection at the L2TP network server (LNS) instead of the L2TP access concentrator (LAC).

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CHAPTER 11

V.92 Reporting Using RADIUS Attribute v.92-info

The V.92 Reporting Using RADIUS Attribute v.92-info feature provides the ability to track V.92 call information, such as V.92 features that are supported, the Quick Connect feature set that was attempted, the duration for which the original call was put on hold, and how many times Modem On Hold was initiated. The vendor-specific attribute (VSA) v.92-info is included in accounting "start" and "stop" records when modems negotiate a V.92 connection.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for V.92 Reporting Using RADIUS Attribute v.92-info

Before the network access server (NAS) can send attribute v.92-info information in accounting "start" and "stop" records, you must perform the following tasks:

- Configure your NAS for authentication, authorization, and accounting (AAA) and to accept incoming modem calls.
- Enable AAA accounting by using the **aaa accounting network default start-stop group radius** command in global configuration mode.
- Familiarize yourself with the V.92 Quick Connect and V.92 Modem on Hold features. See Related Documents, on page 129.

Restrictions for V.92 Reporting Using RADIUS Attribute v.92-info

- If V.92 is not negotiated on your server, V.92 information will not be included in the accounting record.
- Because the attribute v.92-info information is sent as a Cisco VSA, if you configure your RADIUS server as nonstandard (using a non-Cisco server), the V.92 call information will not be sent by default. However, you can still get the V.92 call information by first configuring the **radius-server vsa send**command with the **accounting** keyword (that is, **radius-server vsa send accounting**).

Information About V.92 Reporting Using RADIUS Attribute v.92-info

V.92 Standard Overview

The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) V.92 standard encompasses a number of specifications, including Quick Connect (QC), which dramatically improves how quickly users can connect with their Internet service provider (ISP), and Modem on Hold (MoH), which enables users to suspend and reactivate their dial-up connection to either receive or initiate a telephone call. V.92 also includes pulse code modulation (PCM) upstream, which boosts the upstream data rates from the user to the ISP to reduce transfer times for large files and e-mail attachments sent by the user.

VSA v.92-info

The VSA v.92-info information in RADIUS accounting “start” and “stop” records can help you track V.92 feature set information. The VSA is enabled by default for all sessions that reside over a modem call that is connected using V.92 model modulation.

The VSA information is displayed in the “start” and “stop” records as follows:

v92-info=<V.92 features supported>/<QC Exchange>/<Total MOH time>/<MOH count>

The VSA v92-info has the following four subfields:

- V.92 features supported--All features that are available for the V.92 modem user who is dialing in. These features include QC, MoH, and PCM Upstream.
- QC Exchange--If QC was initiated, this subfield states what feature set (within QC) was attempted.

- Total MOH time--If MoH was initiated, this subfield indicates the duration for which the original call was put on hold.
- MOH count--If MOH was initiated, this field indicates how many times the MOH was initiated.

The following is an example of VSA v92-info information displayed in an accounting recorF:\tips-migration

v92-info=V.92 QC MOH/QC Requested/60/1

How to Monitor and Verify V.92 Call Information

Monitoring V.92 Call Information

To monitor the V.92 information in the accounting “start” and “stop” records, you can perform the following task using some or all of the debug commands that are listeF:\tips-migration

SUMMARY STEPS

1. **enable**
2. **debug aaa accounting**
3. **debug aaa authentication**
4. **debug aaa authorization**
5. debug isdn event
6. debug modem csm [*slot*/*port* | **group** *group-number*]
7. debug ppp {**negotiation** | **authentication**}
8. **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug aaa accounting** **Example:** `Router# debug aaa accounting`	Displays information about accountable events as they occur.
Step 3	**debug aaa authentication** **Example:** `Router# debug aaa authentication`	Displays information about AAA authentication.

	Command or Action	Purpose
Step 4	**debug aaa authorization** **Example:** `Router# debug aaa authorization`	Displays information about AAA and TACACS+ authorization.
Step 5	debug isdn event **Example:** `Router# debug isdn event`	Displays ISDN events occurring on the user side (on the router) of the ISDN interface.
Step 6	debug modem csm [*slot*/*port* | **group** *group-number*] **Example:** `Router# debug modem csm 1/0 group 1`	Displays call switching module (CSM) modem call information.

Step 7	debug ppp {**negotiation** | **authentication**}
	Example:
	`Router# debug ppp authentication`
		Displays information on traffic and exchanges in an internetwork that is implementing the PPP.

Step 8	**debug radius** **Example:** `Router# debug radius`	Displays information associated with RADIUS.

Examples

The following sample debug outputs display information about a V.92 reporting situation:

Debug Output 1

```
01:39:19: ISDN Se7/6:23: RX <-  SETUP pd = 8  callref = 0x42A0
01:39:19:         Bearer Capability i = 0x9090A2
01:39:19:         Channel ID i = 0xA18396
01:39:19:         Progress Ind i = 0x8183 - Origination address is non-ISDN
01:39:19:         Calling Party Number i = 0xA1, '60112', Plan:ISDN, Type:National
01:39:19:         Called Party Number i = 0xA1, '50138', Plan:ISDN, Type:National
01:39:19:         Locking Shift to Codeset 6
01:39:19:         Codeset 6 IE 0x28  i = 'ANALOG,savitha'
01:39:19: ISDN Se7/6:23: Incoming call id = 0x0038, dsl 0
01:39:19: ISDN Se7/6:23: NegotiateBchan: bchan 22 intid 0 serv_st 0 chan_st 0 callid 0x0000
 ev 0x90 n/w? 0
01:39:19: Negotiated int_id 0 bchan 0 cr=0xC2A0 callid=0x0038 lo_chan 22 final int_id/bchan
 0/22 cause 0x0
01:39:19: ISDN Se7/6:23: LIF_EVENT: ces/callid 1/0x38 CALL_INCOMING
01:39:19: ISDN Se7/6:23: CALL_INCOMING dsl 0 bchan 21
01:39:19: voice_parse_intf_name: Using the old NAS_PORT string
01:39:19: AAA/ACCT/EVENT/(00000007): CALL START
```

```
01:39:19: AAA/ACCT(00000000): add node, session 9
01:39:19: AAA/ACCT/NET(00000007): add, count 1
01:39:19: AAA/ACCT/EVENT/(00000007): ATTR REPLACE
01:39:19: ISDN Se7/6:23: CALL_INCOMING: call type is VOICE ULAW, bchan = 21
01:39:19: ISDN Se7/6:23: Event:  Received a VOICE call from 60112 on B21 at 64 Kb/s Tone
Value 0
01:39:19: AAA/ACCT/DS0: channel=21, ds1=6, t3=0, slot=7, ds0=117465109
01:39:19: AAA/ACCT/DS0: channel=21, ds1=6, t3=0, slot=7, ds0=117465109
01:39:19: VDEV_ALLOCATE: 1/5 is allocated
01:39:19: ISDN Se7/6:23: RM returned call_type 1 resource type 0 response 2
01:39:19: EVENT_FROM_ISDN: dchan_idb=0x63B3D334, call_id=0x38, ces=0x0
   bchan=0x15, event=0x1, cause=0x0
01:39:19:  dev in call to isdn : set dnis_collected & fap_notify
01:39:19: EVENT_FROM_ISDN:(0038): DEV_INCALL at slot 1 and port 5
01:39:19: EVENT_FROM_ISDN: decode:calling oct3 0xA1, called oct3 0xA1, oct3a 0x0,mask 0x3D
01:39:19: EVENT_FROM_ISDN: csm_call_info:calling oct3 0xA1, called oct3 0xA1, oct3a 0x0,mask
 0x3D
01:39:19: CSM_PROC_IDLE: CSM_EVENT_ISDN_CALL at slot 1, port 5
01:39:19: CSM DSPLIB(1/5/csm_flags=0x12): np_dsplib_prepare_modem
01:39:19: csm_connect_pri_vdev: TS allocated at bp_stream 0, bp_Ch 5, vdev_common 0x62EAD8F4
 1/5
01:39:19: ISDN Se7/6:23: EVENT to CSM:DEV_INCALL: calltype=VOICE, bchan=21
01:39:19: ISDN Se7/6:23: TX ->  CALL_PROC pd = 8  callref = 0xC2A0
01:39:19:         Channel ID i = 0xA98396
01:39:19: ISDN Se7/6:23: TX ->  ALERTING pd = 8  callref = 0xC2A0
01:39:19: CSM DSPLIB(1/5):DSPLIB_MODEM_INIT: Modem session transition to IDLE
01:39:19: CSM DSPLIB(1/5): Modem went offhook
01:39:19: CSM_PROC_IC2_RING: CSM_EVENT_MODEM_OFFHOOK at slot 1, port 5
01:39:19: ISDN Se7/6:23: VOICE_ANS Event:  call id 0x38, bchan 21, ces 0
01:39:19: ISDN Se7/6:23: isdn_send_connect(): msg 74, call id 0x38, ces 0 bchan 21, call
type VOICE
01:39:19: ISDN Se7/6:23: TX ->  CONNECT pd = 8  callref = 0xC2A0
01:39:19: ISDN Se7/6:23: RX <-  CONNECT_ACK pd = 8  callref = 0x42A0
01:39:19: ISDN Se7/6:23: LIF_EVENT: ces/callid 1/0x38 CALL_PROGRESS
01:39:19: ISDN Se7/6:23: event CALL_PROGRESS dsl 0
01:39:19: ISDN Se7/6:23: CALL_PROGRESS: CALL_CONNECTED call id 0x38, bchan 21, dsl 0
01:39:19: EVENT_FROM_ISDN: dchan_idb=0x63B3D334, call_id=0x38, ces=0x0
   bchan=0x15, event=0x4, cause=0x0
01:39:19: EVENT_FROM_ISDN:(0038): DEV_CONNECTED at slot 1 and port 5
01:39:19: CSM_PROC_IC6_WAIT_FOR_CONNECT: CSM_EVENT_ISDN_CONNECTED at slot 1, port 5
01:39:19: CSM DSPLIB(1/5): np_dsplib_call_accept
01:39:19: ISDN Se7/6:23: EVENT to CSM:DEV_CONNECTEF:\tips-migration calltype=VOICE, bchan=21
01:39:19: CSM DSPLIB(1/5):DSPLIB_MODEM_WAIT_ACTIVE: Modem session transition to ACTIVE
01:39:19: CSM DSPLIB(1/5): Modem state changed to (CONNECT_STATE)
01:39:22: CSM DSPLIB(1/5): Modem state changed to (V8BIS_EXCHANGE_STATE)
01:39:24: CSM DSPLIB(1/5): Modem state changed to (LINK_STATE)
01:39:28: CSM DSPLIB(1/5): Modem state changed to (RANGING_STATE)
01:39:30: CSM DSPLIB(1/5): Modem state changed to (HALF_DUPLEX_TRAIN_STATE)
01:39:45: CSM DSPLIB(1/5): Modem state changed to (TRAINUP_STATE)
01:39:45: CSM DSPLIB(1/5): Modem state changed to (EC_NEGOTIATING_STATE)
01:39:46: CSM DSPLIB(1/5): Modem state changed to (STEADY_STATE)
01:39:46: TTY1/05: DSR came up
01:39:46: tty1/05: Modem: IDLE->(unknown)
01:39:46: TTY1/05: EXEC creation
01:39:46: CHAT1/05: Attempting line activation script
01:39:46: CHAT1/05: Asserting DTR
01:39:50: voice_parse_intf_name: Using the old NAS_PORT string
01:39:50: voice_parse_intf_name: Using the old NAS_PORT string
01:39:50: AAA/AUTHEN/LOGIN (00000007): Pick method list 'default'
01:39:50: RADIUS/ENCODE(00000007): ask "Username: "
01:39:50: RADIUS/ENCODE(00000007): send packet; GET_USER
01:39:50: TTY1/05: set timer type 10, 30 seconds
01:39:50: TTY1/05: Autoselect(2) sample 7E
01:39:50: TTY1/05: Autoselect(2) sample 7EFF
01:39:50: TTY1/05: Autoselect(2) sample 7EFF7D
01:39:50: TTY1/05: Autoselect(2) sample 7EFF7D23
01:39:50: TTY1/05 Autoselect cmF:\tips-migration  ppp negotiate
01:39:50: TTY1/05: EXEC creation
01:39:50: CHAT1/05: Attempting line activation script
01:39:50: CHAT1/05: Asserting DTR
01:39:54: voice_parse_intf_name: Using the old NAS_PORT string
01:39:54: voice_parse_intf_name: Using the old NAS_PORT string
01:39:54: TTY1/05: no timer type 1 to destroy
```

```
01:39:54: TTY1/05: no timer type 0 to destroy
01:39:54: As1/05 LCP: I CONFREQ [Closed] id 0 len 50
01:39:54: As1/05 LCP:    ACCM 0x00000000 (0x020600000000)
01:39:54: As1/05 LCP:    MagicNumber 0x00002EB8 (0x050600002EB8)
01:39:54: As1/05 LCP:    PFC (0x0702)
01:39:54: As1/05 LCP:    ACFC (0x0802)
01:39:54: As1/05 LCP:    Callback 6  (0x0D0306)
01:39:54: As1/05 LCP:    MRRU 1614 (0x1104064E)
01:39:54: As1/05 LCP:    EndpointDisc 1 Local
01:39:54: As1/05 LCP:     (0x131701CC7F60A0E7A211D6B549000102)
01:39:54: As1/05 LCP:     (0x2BC43900000000)
01:39:54: As1/05 LCP: Lower layer not up, Fast Starting
01:39:54: voice_parse_intf_name: Using the old NAS_PORT string
01:39:54: voice_parse_intf_name: Using the old NAS_PORT string
01:39:54: As1/05 PPP: Treating connection as a callin
01:39:54: As1/05 PPP: Phase is ESTABLISHING, Passive Open
01:39:54: As1/05 LCP: State is Listen
01:39:54: As1/05 PPP: Authorization required
01:39:54: As1/05 LCP: O CONFREQ [Listen] id 1 len 25
01:39:54: As1/05 LCP:    ACCM 0x000A0000 (0x0206000A0000)
01:39:54: As1/05 LCP:    AuthProto CHAP (0x0305C22305)
01:39:54: As1/05 LCP:    MagicNumber 0x099EBCBA (0x0506099EBCBA)
01:39:54: As1/05 LCP:    PFC (0x0702)
01:39:54: As1/05 LCP:    ACFC (0x0802)
01:39:54: As1/05 LCP: O CONFREJ [Listen] id 0 len 11
01:39:54: As1/05 LCP:    Callback 6  (0x0D0306)
01:39:54: As1/05 LCP:    MRRU 1614 (0x1104064E)
01:39:54: As1/05 LCP: I CONFACK [REQsent] id 1 len 25
01:39:54: As1/05 LCP:    ACCM 0x000A0000 (0x0206000A0000)
01:39:54: As1/05 LCP:    AuthProto CHAP (0x0305C22305)
01:39:54: As1/05 LCP:    MagicNumber 0x099EBCBA (0x0506099EBCBA)
01:39:54: As1/05 LCP:    PFC (0x0702)
01:39:54: As1/05 LCP:    ACFC (0x0802)
01:39:54: As1/05 LCP: I CONFREQ [ACKrcvd] id 1 len 43
01:39:54: As1/05 LCP:    ACCM 0x00000000 (0x020600000000)
01:39:54: As1/05 LCP:    MagicNumber 0x00002EB8 (0x050600002EB8)
01:39:54: As1/05 LCP:    PFC (0x0702)
01:39:54: As1/05 LCP:    ACFC (0x0802)
01:39:54: As1/05 LCP:    EndpointDisc 1 Local
01:39:54: As1/05 LCP:     (0x131701CC7F60A0E7A211D6B549000102)
01:39:54: As1/05 LCP:     (0x2BC43900000000)
01:39:54: As1/05 LCP: O CONFACK [ACKrcvd] id 1 len 43
01:39:54: As1/05 LCP:    ACCM 0x00000000 (0x020600000000)
01:39:54: As1/05 LCP:    MagicNumber 0x00002EB8 (0x050600002EB8)
01:39:54: As1/05 LCP:    PFC (0x0702)
01:39:54: As1/05 LCP:    ACFC (0x0802)
01:39:54: As1/05 LCP:    EndpointDisc 1 Local
01:39:54: As1/05 LCP:     (0x131701CC7F60A0E7A211D6B549000102)
01:39:54: As1/05 LCP:     (0x2BC43900000000)
01:39:54: As1/05 LCP: State is Open
01:39:54: As1/05 PPP: Phase is AUTHENTICATING, by this end
01:39:54: As1/05 CHAP: O CHALLENGE id 1 len 26 from "s5400"
01:39:54: As1/05 LCP: I IDENTIFY [Open] id 2 len 18 magic 0x00002EB8 MSRASV4.00
01:39:54: As1/05 LCP: I IDENTIFY [Open] id 3 len 23 magic 0x00002EB8 MSRAS-1-PTE-PC1
01:39:54: As1/05 CHAP: I RESPONSE id 1 len 34 from "Administrator"
01:39:54: As1/05 PPP: Phase is FORWARDING, Attempting Forward
01:39:54: As1/05 PPP: Phase is AUTHENTICATING, Unauthenticated User
01:39:54: AAA/AUTHEN/PPP (00000007): Pick method list 'default'
01:39:54: As1/05 PPP: Sent CHAP LOGIN Request
01:39:54: RADIUS/ENCODE(00000007): Unsupported AAA attribute parent-interface
01:39:54: RADIUS/ENCODE(00000007): Unsupported AAA attribute parent-interface-type
01:39:54: RADIUS/ENCODE(00000007): acct_session_iF:\tips-migration 9
01:39:54: RADIUS(00000007): sending
01:39:54: RADIUS: Send to unknown id 2 10.107.164.120:1645, Access-Request, len 128
01:39:54: RADIUS:  authenticator 13 E4 F2 9F BC 3E CE 52 - CC 93 0C E0 01 0C 73 7B
01:39:54: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
01:39:54: RADIUS:  User-Name           [1]   15  "Administrator"
01:39:54: RADIUS:  CHAP-Password       [3]   19  *
01:39:54: RADIUS:  Called-Station-Id   [30]  7   "50138"
01:39:54: RADIUS:  Calling-Station-Id  [31]  7   "60112"
01:39:54: RADIUS:  Vendor, Cisco       [26]  30
01:39:54: RADIUS:   cisco-nas-port     [2]   24  "Async1/05*Serial7/6:21"
01:39:54: RADIUS:  NAS-Port            [5]   6   221
```

```
01:39:54: RADIUS:  NAS-Port-Type       [61]  6   Async                     [0]
01:39:54: RADIUS:  Service-Type        [6]   6   Framed                    [2]
01:39:54: RADIUS:  NAS-IP-Address      [4]   6   10.0.58.107
01:39:54: RADIUS: Received from id 2 10.107.164.120:1645, Access-Accept, len 62
01:39:54: RADIUS:  authenticator EF 45 A3 D4 A7 EE D0 65 - 03 50 B4 3E 07 87 2E 2F
01:39:54: RADIUS:  Vendor, Cisco       [26]  30
01:39:54: RADIUS:   cisco-nas-port     [2]   24  "Async1/05*Serial7/6:21"
01:39:54: RADIUS:  Service-Type        [6]   6   Framed                    [2]
01:39:54: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
01:39:54: RADIUS: Received from id 7
01:39:54: As1/05 PPP: Received LOGIN Response PASS
01:39:54: As1/05 PPP/AAA: Check Attr: interface
01:39:54: As1/05 PPP/AAA: Check Attr: service-type
01:39:54: As1/05 PPP/AAA: Check Attr: Framed-Protocol
01:39:54: As1/05 PPP: Phase is FORWARDING, Attempting Forward
01:39:54: As1/05 PPP: Phase is AUTHENTICATING, Authenticated User
01:39:54: As1/05 AAA/AUTHOR/LCP: Process Author
01:39:54: As1/05 AAA/AUTHOR/LCP: Process Attr: service-type
01:39:54: As1/05 CHAP: O SUCCESS id 1 len 4
01:39:54: AAA/ACCT/NET(00000007): Pick method list 'default'
01:39:54: AAA/ACCT/SETMLIST(00000007): Handle FFFFFFFF, mlist 630B11E4, Name default
01:39:54: AAA/ACCT/EVENT/(00000007): NET UP
01:39:54: AAA/ACCT/NET(00000007): Queueing record is START
01:39:54: As1/05 PPP: Phase is UP
01:39:54: As1/05 AAA/AUTHOR/IPCP: FSM authorization not needed
01:39:54: As1/05 AAA/AUTHOR/FSM: We can start IPCP
01:39:54: As1/05 IPCP: O CONFREQ [Closed] id 1 len 10
01:39:54: As1/05 IPCP:    Address 10.1.1.2 (0x030646010102)
01:39:54: AAA/ACCT(00000007): Accouting method=radius (radius)
01:39:54: RADIUS/ENCODE(00000007): Unsupported AAA attribute timezone
01:39:54: RADIUS/ENCODE(00000007): Unsupported AAA attribute parent-interface
01:39:54: RADIUS/ENCODE(00000007): Unsupported AAA attribute parent-interface-type
01:39:54: RADIUS(00000007): sending
01:39:54: RADIUS: Send to unknown id 8 10.107.164.120:1646, Accounting-Request, len 243
01:39:54: RADIUS:  authenticator 41 87 FA 03 EB F9 94 62 - B2 3A 24 B8 27 4C A4 BC
01:39:54: RADIUS:  Acct-Session-Id     [44]  10  "00000009"
01:39:54: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
01:39:54: RADIUS:  Connect-Info        [77]  26  "52000/28800 V90/V44/LAPM"
01:39:54: RADIUS:  Vendor, Cisco       [26]  48
01:39:54: RADIUS:   Cisco AVpair      [1]   42  "v92-info=V.92 QC MOH/No QC Requested/0/0"
01:39:54: RADIUS:  Vendor, Cisco       [26]  32
01:39:54: RADIUS:   Cisco AVpair       [1]   26  "connect-progress=Call Up"
01:39:54: RADIUS:  Authentic           [45]  6   RADIUS                    [1]
01:39:54: RADIUS:  User-Name           [1]   15  "Administrator"
01:39:54: RADIUS:  Acct-Status-Type    [40]  6   Start                     [1]
01:39:54: RADIUS:  Called-Station-Id   [30]  7   "50138"
01:39:54: RADIUS:  Calling-Station-Id  [31]  7   "60112"
01:39:54: RADIUS:  Vendor, Cisco       [26]  30
01:39:54: RADIUS:   cisco-nas-port     [2]   24  "Async1/05*Serial7/6:21"
01:39:54: RADIUS:  NAS-Port            [5]   6   221
01:39:54: RADIUS:  NAS-Port-Type       [61]  6   Async                     [0]
01:39:54: RADIUS:  Service-Type        [6]   6   Framed                    [2]
01:39:54: RADIUS:  NAS-IP-Address      [4]   6   10.0.58.107
01:39:54: RADIUS:  Acct-Delay-Time     [41]  6   0
01:39:54: RADIUS: Received from id 8 10.107.164.120:1646, Accounting-response, len 20
01:39:54: RADIUS:  authenticator E5 5C D3 69 88 D5 2E 8E - 49 AF 63 22 01 53 33 7B
01:39:54: AAA/ACCT/NET(00000007): START protocol reply PASS
01:39:54: As1/05 CCP: I CONFREQ [Not negotiated] id 4 len 211
01:39:54: As1/05 CCP:    Type254
01:39:54: As1/05 CCP:     (0xFEC90100000000000000000000000000)
01:39:54: As1/05 CCP:     (0x000074FFC7000000000068000000A000)
01:39:54: As1/05 CCP:     (0x00006C20563905000000C0000000A400)
01:39:54: As1/05 CCP:     (0x0000BC00000186400007000E80018C8)
01:39:54: As1/05 CCP:     (0x130017CCF177000000000001000000E8FE)
01:39:54: As1/05 CCP:     (0xC70076CDF177060000000000000000000)
01:39:54: As1/05 CCP:     (0x00000000000000000000000000000000)
01:39:54: As1/05 CCP:     (0x00000000000000000000000000000000)
01:39:54: As1/05 CCP:     (0x00000000000000000000000000000000)
01:39:54: As1/05 CCP:     (0x00000000000000000000220020000001)
01:39:54: As1/05 CCP:     (0x0800000000005016B1CBA2E7D611B549)
01:39:54: As1/05 CCP:     (0x0001022BC439C8000000000000000C800)
01:39:54: As1/05 CCP:     (0x00004D000000281FB8)
01:39:54: As1/05 CCP:    MS-PPC supported bits 0x00000006 (0x120600000006)
```

```
01:39:54: As1/05 LCP: O PROTREJ [Open] id 2 len 217 protocol CCP
01:39:54: As1/05 LCP:  (0x80FD010400D3FEC90100000000000000)
01:39:54: As1/05 LCP:  (0x000000000000000074FFC70000000000)
01:39:54: As1/05 LCP:  (0x68000000A00000006C20563905000000)
01:39:54: As1/05 LCP:  (0xC0000000A4000000BC00000018640000)
01:39:54: As1/05 LCP:  (0x7000E80018C8130017CCF17700000000)
01:39:54: As1/05 LCP:  (0x01000000E8FEC70076CDF17706000000)
01:39:54: As1/05 LCP:  (0x00000000000000000000000000000000)
01:39:54: As1/05 LCP:  (0x00000000000000000000000000000000)
01:39:54: As1/05 LCP:  (0x00000000000000000000000000000000)
01:39:54: As1/05 LCP:  (0x00000000000000000000000000000000)
01:39:54: As1/05 LCP:  (0x22002000000010800000000005016B1CB)
01:39:54: As1/05 LCP:  (0xA2E7D611B5490001022BC439C8000000)
01:39:54: As1/05 LCP:  (0x00000000C80000004D000000281FB812)
01:39:54: As1/05 LCP:  (0x0600000006)
01:39:54: As1/05 IPCP: I CONFREQ [REQsent] id 5 len 34
01:39:54: As1/05 IPCP:    Address 0.0.0.0 (0x030600000000)
01:39:54: As1/05 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
01:39:54: As1/05 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
01:39:54: As1/05 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
01:39:54: As1/05 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
01:39:54: As1/05 AAA/AUTHOR/IPCP: Start.  Her address 0.0.0.0, we want 10.2.2.6
01:39:54: As1/05 AAA/AUTHOR/IPCP: Authorization succeeded
01:39:54: As1/05 AAA/AUTHOR/IPCP: Done.  Her address 0.0.0.0, we want 10.2.2.6
01:39:54: As1/05 AAA/AUTHOR/IPCP: no author-info for primary dns
01:39:54: As1/05 AAA/AUTHOR/IPCP: no author-info for primary wins
01:39:54: As1/05 AAA/AUTHOR/IPCP: no author-info for seconday dns
01:39:54: As1/05 AAA/AUTHOR/IPCP: no author-info for seconday wins
01:39:54: As1/05 IPCP: O CONFREJ [REQsent] id 5 len 28
01:39:54: As1/05 IPCP:    PrimaryDNS 0.0.0.0 (0x810600000000)
01:39:54: As1/05 IPCP:    PrimaryWINS 0.0.0.0 (0x820600000000)
01:39:54: As1/05 IPCP:    SecondaryDNS 0.0.0.0 (0x830600000000)
01:39:54: As1/05 IPCP:    SecondaryWINS 0.0.0.0 (0x840600000000)
01:39:54: As1/05 IPCP: I CONFACK [REQsent] id 1 len 10
01:39:54: As1/05 IPCP:    Address 70.1.1.2 (0x030646010102)
01:39:54: As1/05 IPCP: I CONFREQ [ACKrcvd] id 6 len 10
01:39:54: As1/05 IPCP:    Address 0.0.0.0 (0x030600000000)
01:39:54: As1/05 IPCP: O CONFNAK [ACKrcvd] id 6 len 10
01:39:54: As1/05 IPCP:    Address 70.2.2.6 (0x030646020206)
01:39:55: As1/05 IPCP: I CONFREQ [ACKrcvd] id 7 len 10
01:39:55: As1/05 IPCP:    Address 70.2.2.6 (0x030646020206)
01:39:55: As1/05 IPCP: O CONFACK [ACKrcvd] id 7 len 10
01:39:55: As1/05 IPCP:    Address 70.2.2.6 (0x030646020206)
01:39:55: As1/05 IPCP: State is Open
01:39:55: AAA/ACCT/EVENT/(00000007): IPCP_PASS
01:39:55: As1/05 IPCP: Install route to 10.2.2.6
01:39:55: As1/05 IPCP: Add link info for cef entry 10.2.2.6
```

Debug Output 2

```
01:40:50: ISDN Se7/6:23: RX <-  DISCONNECT pd = 8  callref = 0x42A0
01:40:50:         Cause i = 0x8190 - Normal call clearing
01:40:50: ISDN Se7/6:23: LIF_EVENT: ces/callid 1/0x38 CALL_DISC
01:40:50: EVENT_FROM_ISDN: dchan_idb=0x63B3D334, call_id=0x38, ces=0x0
   bchan=0x15, event=0x0, cause=0x10
01:40:50: EVENT_FROM_ISDN:(0038): DEV_IDLE at slot 1 and port 5
01:40:50: CSM_PROC_IC7_OC6_CONNECTEF:\tips-migration CSM_EVENT_ISDN_DISCONNECTED at slot
1, port 5
01:40:50: CSM DSPLIB(1/5): np_dsplib_call_hangup reason 14
01:40:50: CSM(1/5): Enter csm_enter_disconnecting_state
01:40:50: VDEV_DEALLOCATE: slot 1 and port 5 is deallocated
01:40:50: ISDN Se7/6:23: EVENT to CSM:DEV_IDLE: calltype=VOICE, bchan=21
01:40:50: ISDN Se7/6:23: process_disc_ack(): call id 0x38, ces 0, call type VOICE cause
0x10
01:40:50: ISDN Se7/6:23: TX ->  RELEASE pd = 8  callref = 0xC2A0
01:40:50: AAA/ACCT/EVENT/(00000007): CALL STOP
01:40:50: AAA/ACCT/CALL STOP(00000007): Sending stop requests
01:40:50: AAA/ACCT(00000007): Send all stops
01:40:50: AAA/ACCT/NET(00000007): STOP
01:40:50: AAA/ACCT/NET(00000007): Queueing record is STOP osr 1
01:40:50: AAA/ACCT(00000007): Accouting method=radius (radius)
```

```
01:40:50: RADIUS/ENCODE(00000007): Unsupported AAA attribute timezone
01:40:50: RADIUS/ENCODE(00000007): Unsupported AAA attribute parent-interface
01:40:50: RADIUS/ENCODE(00000007): Unsupported AAA attribute parent-interface-type
01:40:50: RADIUS(00000007): sending
01:40:50: RADIUS: Send to unknown id 9 10.107.164.120:1646, Accounting-Request, len 315
01:40:50: RADIUS:  authenticator 2E 6A 04 D0 04 9A D3 D5 - F7 DD 99 E0 C3 99 27 60
01:40:50: RADIUS:  Acct-Session-Id     [44]  10  "00000009"
01:40:50: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
01:40:50: RADIUS:  Framed-IP-Address   [8]   6   70.2.2.6
01:40:50: RADIUS:  Acct-Terminate-Cause[49]  6   lost-carrier              [2]
01:40:50: RADIUS:  Vendor, Cisco       [26]  33
01:40:50: RADIUS:   Cisco AVpair       [1]   27  "disc-cause-ext=No Carrier"
01:40:50: RADIUS:  Vendor, Cisco       [26]  35
01:40:50: RADIUS:   Cisco AVpair       [1]   29  "connect-progress=LAN Ses Up"
01:40:50: RADIUS:  Acct-Session-Time   [46]  6   56
01:40:50: RADIUS:  Connect-Info        [77]  26  "52000/28800 V90/V44/LAPM"
01:40:50: RADIUS:  Vendor, Cisco       [26]  48
01:40:50: RADIUS:   Cisco AVpair       [1]   42  "v92-info=V.92 QC MOH/No QC Requested/0/0"
01:40:50: RADIUS:  Acct-Input-Octets   [42]  6   285
01:40:50: RADIUS:  Acct-Output-Octets  [43]  6   295
01:40:50: RADIUS:  Acct-Input-Packets  [47]  6   5
01:40:50: RADIUS:  Acct-Output-Packets [48]  6   5
01:40:50: RADIUS:  User-Name           [1]   15  "Administrator"
01:40:50: RADIUS:  Acct-Status-Type    [40]  6   Stop                      [2]
01:40:50: RADIUS:  Called-Station-Id   [30]  7   "50138"
01:40:50: RADIUS:  Calling-Station-Id  [31]  7   "60112"
01:40:50: RADIUS:  Vendor, Cisco       [26]  30
01:40:50: RADIUS:   cisco-nas-port     [2]   24  "Async1/05*Serial7/6:21"
01:40:50: RADIUS:  NAS-Port            [5]   6   221
01:40:50: RADIUS:  NAS-Port-Type       [61]  6   Async                     [0]
01:40:50: RADIUS:  Service-Type        [6]   6   Framed                    [2]
01:40:50: RADIUS:  NAS-IP-Address      [4]   6   10.0.58.107
01:40:50: RADIUS:  Acct-Delay-Time     [41]  6   0
01:40:50: RADIUS: Received from id 9 10.107.164.120:1646, Accounting-response, len 20
01:40:50: RADIUS:  authenticator D0 3F 32 D7 7C 8C 5E 22 - 9A 69 EF 17 AC 32 81 21
01:40:50: AAA/ACCT/NET(00000007): STOP protocol reply PASS
01:40:50: AAA/ACCT/NET(00000007): Cleaning up from Callback osr 0
01:40:50: AAA/ACCT(00000007): del node, session 9
01:40:50: AAA/ACCT/NET(00000007): free_rec, count 0
01:40:50: AAA/ACCT/NET(00000007) reccnt 0, csr TRUE, osr 0
01:40:50: AAA/ACCT/NET(00000007): Last rec in db, intf not enqueued
01:40:50: ISDN Se7/6:23: RX <-  RELEASE_COMP pd = 8  callref = 0x42A0
01:40:50: ISDN Se7/6:23: CCPRI_ReleaseCall(): bchan 22, call id 0x38, call type VOICE
01:40:50: CCPRI_ReleaseChan released b_dsl 0 B_Chan 22
01:40:50: ISDN Se7/6:23: LIF_EVENT: ces/callid 1/0x38 CALL_CLEARED
01:40:50: ISDN Se7/6:23: received CALL_CLEARED  call_id 0x38
01:40:50: no resend setup, no redial
01:40:50: no resend setup, no redial
01:40:50: AAA/ACCT/DS0: channel=21, ds1=6, t3=0, slot=7, ds0=117465109
01:40:50: EVENT_FROM_ISDN: dchan_idb=0x63B3D334, call_id=0x38, ces=0x1
   bchan=0x15, event=0x0, cause=0x0
01:40:50: ISDN Se7/6:23: EVENT to CSM:DEV_IDLE: calltype=VOICE, bchan=21
01:40:51: CSM DSPLIB(1/5): Modem state changed to (TERMINATING_STATE)
01:40:51: CSM DSPLIB(1/5): Modem went onhook
01:40:51: CSM_PROC_IC8_OC8_DISCONNECTING: CSM_EVENT_MODEM_ONHOOK at slot 1, port 5
01:40:51: CSM(1/5): Enter csm_enter_idle_state
01:40:51: CSM DSPLIB(1/5):DSPLIB_IDLE: Modem session transition to FLUSHING
01:40:51: CSM DSPLIB(1/5):DSPLIB_IDLE: Modem session transition to IDLE
01:40:51: TTY1/05: DSR was dropped
01:40:51: tty1/05: Modem: READY->(unknown)
01:40:52: TTY1/05: dropping DTR, hanging up
01:40:52: DSPLIB(1/5): np_dsplib_process_dtr_notify()
01:40:52: CSM DSPLIB(1/5): Modem went onhook
01:40:52: CSM_PROC_IDLE: CSM_EVENT_MODEM_ONHOOK at slot 1, port 5
01:40:52: TTY1/05: Async Int reset: Dropping DTR
01:40:52: tty1/05: Modem: HANGUP->(unknown)
01:40:52: AAA/ACCT/EVENT/(00000007): NET DOWN
01:40:52: As1/05 IPCP: Remove link info for cef entry 70.2.2.6
01:40:52: As1/05 IPCP: State is Closed
01:40:52: As1/05 PPP: Phase is TERMINATING
01:40:52: As1/05 LCP: State is Closed
01:40:52: As1/05 PPP: Phase is DOWN
01:40:52: As1/05 IPCP: Remove route to 70.2.2.6
```

```
01:40:52: As1/05 LCP: State is Closed
01:40:53: TTY1/05: cleanup pending. Delaying DTR
01:40:54: TTY1/05: cleanup pending. Delaying DTR
01:40:55: TTY1/05: cleanup pending. Delaying DTR
01:40:56: TTY1/05: cleanup pending. Delaying DTR
01:40:57: TTY1/05: no timer type 0 to destroy
01:40:57: TTY1/05: no timer type 1 to destroy
01:40:57: TTY1/05: no timer type 3 to destroy
01:40:57: TTY1/05: no timer type 4 to destroy
01:40:57: TTY1/05: no timer type 2 to destroy
01:40:57: Async1/05: allowing modem_process to continue hangup
01:40:57: TTY1/05: restoring DTR
01:40:57: TTY1/05: autoconfigure probe started
01:40:57: As1/05 LCP: State is Closed
```

Verifying V.92 Call Information

To verify that the V.92 call was correctly established, use the following **show** commands:

SUMMARY STEPS

1. **show modem** [*slot*/*port* | **group** *number*]
2. **show port modem log** [**reverse** *slot*/*port*] [*slot* | *slot*/*port*]
3. **show users** [**all**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show modem** [*slot*/*port* | **group** *number*] **Example:** `Router# show modem 1/0 group 1`	Displays a high-level performance report for all the modems or a single modem inside Cisco access servers.
Step 2	**show port modem log** [**reverse** *slot*/*port*] [*slot* | *slot*/*port*] **Example:** `Router# show port modem log`	Displays the events generated by the modem sessions.
Step 3	**show users** [**all**] **Example:** `Router# show users`	Displays information about the active lines on the router.

Examples

The following V.92 reporting outputs are from the **show port modem log** and **show users** commands:

Show Output 1

```
Router# show port modem log 1/05
Port 1/05 Events Log
  01:46:19: Service Type: DATA_FAX_MODEM
  01:46:19: Service Mode: DATA_FAX_MODEM
  01:46:19: Session State: IDLE
  01:46:19: incoming caller number: 60112
  01:46:19: incoming called number: 50138
  01:46:19: Service Type: DATA_FAX_MODEM
  01:46:19: Service Mode: DATA_FAX_MODEM
  01:46:19: Session State: IDLE
  01:46:19: Service Type: DATA_FAX_MODEM
  01:46:19: Service Mode: DATA_FAX_MODEM
  01:46:19: Session State: ACTIVE
  01:46:19: Modem State event:
            State: Connect
  01:46:20: Modem State event:
            State: V.8bis Exchange
  01:46:20: Modem State event:
            State: Link
  01:46:20: Modem State event:
            State: Ranging
  01:46:20: Modem State event:
            State: Half Duplex Train
  01:46:20: Modem State event:
            State: Train Up
  01:46:20: Modem State event:
            State: EC Negotiating
  01:46:20: Modem State event:
            State: Steady
  01:46:20: Modem Static event:
    Connect Protocol                        :   LAP-M
    Compression                             :   V.44
    Connected Standard                      :   V.90
    TX,RX Symbol Rate                       :   8000, 3200
    TX,RX Carrier Frequency                 :   0, 1829
    TX,RX Trellis Coding                    :   16/No trellis
    Frequency Offset                        :   0  Hz
    Round Trip Delay                        :   0  msecs
    TX,RX Bit Rate                          :   52000, 28800
    Robbed Bit Signalling (RBS) pattern     :   255
    Digital Pad                             :   6 dB
    Digital Pad Compensation                :   Enabled
    MNP10EC                                 :   Off-None
    QC Exchange                             :   No QC Requested
    TX,RX Negotiated String Length          :   255, 255
    DC TX,RX Negotiated Codewords           :   1024, 1024
    DC TX,RX Negotiated History Size        :   4096, 5120
01:46:21: ISDN Se7/6:23: RX <-  SERVICE pd = 3  callref = 0x0000
01:46:21:         Change Status i = 0xC0 - in-service
01:46:21:         Channel ID i = 0xA98381
01:46:21: ISDN Se7/6:23: Incoming call id = 0x003A, dsl 0
01:46:21: ISDN Se7/6:23: LIF_EVENT: ces/callid 1/0x0 CHAN_STATUS
01:46:21: ISDN Se7/6:23: CHAN_STATUS B-chan=1, action=2; Maintenance.
01:46:21: ISDN Se7/6:23: TX ->  SERVICE ACKNOWLEDGE pd = 3  callref = 0x8000
01:46:21:         Change Status i = 0xC0 - in-service
01:46:21:         Channel ID i =       1
s5400#sh port modem log 1/05
Port 1/05 Events Log
  01:46:30: Service Type: DATA_FAX_MODEM
  01:46:30: Service Mode: DATA_FAX_MODEM
  01:46:30: Session State: IDLE
  01:46:30: incoming caller number: 60112
  01:46:30: incoming called number: 50138
  01:46:30: Service Type: DATA_FAX_MODEM
  01:46:30: Service Mode: DATA_FAX_MODEM
  01:46:30: Session State: IDLE
  01:46:30: Service Type: DATA_FAX_MODEM
  01:46:30: Service Mode: DATA_FAX_MODEM
  01:46:30: Session State: ACTIVE
  01:46:30: Modem State event:
          State: Connect
01:46:30: Modem State event:
          State: V.8bis Exchange
01:46:30: Modem State event:
          State: Link
01:46:30: Modem State event:
          State: Ranging
01:46:30: Modem State event:
          State: Half Duplex Train
01:46:30: Modem State event:
          State: Train Up
01:46:31: Modem State event:
          State: EC Negotiating
01:46:31: Modem State event:
          State: Steady
01:46:31: Modem Static event:
  Connect Protocol                        :   LAP-M
  Compression                             :   V.44
  Connected Standard                      :   V.90
  TX,RX Symbol Rate                       :   8000, 3200
  TX,RX Carrier Frequency                 :   0, 1829
  TX,RX Trellis Coding                    :   16/No trellis
  Frequency Offset                        :   0  Hz
  Round Trip Delay                        :   0  msecs
  TX,RX Bit Rate                          :   52000, 28800
  Robbed Bit Signalling (RBS) pattern     :   255
  Digital Pad                             :   6 dB
  Digital Pad Compensation                :   Enabled
  MNP10EC                                 :   Off-None
  QC Exchange                             :   No QC Requested
  TX,RX Negotiated String Length          :   255, 255
  DC TX,RX Negotiated Codewords           :   1024, 1024
  DC TX,RX Negotiated History Size        :   4096, 5120
  Diagnostic Code                         :   00 00 00 00 00 00 00 00
  V.92 Status                             :   V.92 QC MOH
01:46:32: Modem Dynamic event:
  Sq Value                                :   6
  Signal Noise Ratio                      :   38  dB
  Receive Level                           :   -11  dBm
  Phase Jitter Frequency                  :   0  Hz
  Phase Jitter Level                      :   0  degrees
  Far End Echo Level                      :   0  dBm
  Phase Roll                              :   0  degrees
  Total Retrains                          :   0
  EC Retransmission Count                 :   0
  Characters transmitted, received        :   0, 0
  Characters received BAD                 :   0
  PPP/SLIP packets transmitted, received  :   0, 0
  PPP/SLIP packets received (BAD/ABORTED) :   0
  EC packets transmitted, received OK     :   0, 0
  EC packets (Received BAD/ABORTED)       :   0
  Total Speedshifts                       :   0
  Total MOH Time                          :   0  secs
  Current MOH Time                        :   0  secs
  MOH Status                              :   Modem is Not on Hold
  MOH Count                               :   0
  MOH Request Count                       :   0
  Retrains due to Call Waiting            :   0
  DC Encoder,Decoder State                :   compressed/compressed
  DC TX,RX Compression Ratio              :   not calculated/not calculated
  DC TX,RX Dictionary Reset Count         :   0, 0
  Diagnostic Code                         :   00 00 00 00 00 00 00 00
01:46:35: Modem State event:
          State: Terminate
01:46:35: Service Type: DATA_FAX_MODEM
01:46:35: Service Mode: DATA_FAX_MODEM
01:46:35: Session State: FLUSHING
01:46:35: Service Type: DATA_FAX_MODEM
01:46:35: Service Mode: DATA_FAX_MODEM
01:46:35: Session State: IDLE
01:46:35: Modem End Connect event:
  Call Timer                              :   65  secs
  Disconnect Reason Info                  :   0x220
```

```
        Type (=0  ):  <unknown>
       Class (=2  ):  EC condition - locally detected
      Reason (=32 ):  received DISC frame -- normal LAPM termination
    Total Retrains                          :   0
    EC Retransmission Count                 :   0
    Characters transmitted, received        :   677, 817
    Characters received BAD                 :   0
    PPP/SLIP packets transmitted, received  :   10, 10
    PPP/SLIP packets received (BAD/ABORTED) :   0
    EC packets transmitted, received OK     :   10, 21
    EC packets (Received BAD/ABORTED)       :   0
    TX,RX Bit Rate                          :   52000, 28800
    Total Speedshifts                       :   0
    Total MOH Time                          :   0  secs
    Current MOH Time                        :   0  secs
    MOH Status                              :   Modem is Not on Hold
    MOH Count                               :   0
    MOH Request Count                       :   0
    Retrains due to Call Waiting            :   0
    DC Encoder,Decoder State                :   compressed/compressed
    DC TX,RX Compression Ratio              :   1.67:1/1.65:1
    DC TX,RX Dictionary Reset Count         :   0, 1
    Diagnostic Code                         :   00 00 00 00 00 00 00 00
  01:46:37:Modem Link Rate event:
```

Show Output 2

```
Router# show users
    Line       User       Host(s)              Idle       Location
*  0 con 0                idle                 00:00:00
  tty 1/05     Administra Async interface      00:00:29   PPP: 70.2.2.6
  Interface      User        Mode                     Idle     Peer Address
```

Troubleshooting Tips

If you see that V.92 call information is not being reported by AAA, ensure that the call is a V.92 call by using the **show modem** command or by looking at the modem logs by using the **show modem log**command.

Additional References

The following sections provide references related to theV.92 Reporting Using RADIUS Attribute v.92-info feature.

Related Documents

Related Topic	Document Title
AAA accounting	“ AAA Accounting ” module.
AAA accounting commands	*Cisco IOS Security Command Reference*
V.92 Quick Connect feature	*V.92 Quick Connect for Cisco AS5300 and Cisco AS5800 Universal Access Servers*

Related Topic	Document Title
V.92 Modem on Hold feature	*V.92 Modem on Hold for Cisco AS5300 and Cisco AS5800 Universal Access Servers*

Standards

Standards	Title
None.	--

MIBs

MIBs	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for V.92 Reporting Using RADIUS Attribute v.92-info

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 18: Feature Information for V.92 Reporting Using RADIUS Attribute v.92-info

Feature Name	Releases	Feature Information
V.92 Reporting Using RADIUS Attribute v.92-info	12.3(1)	The V.92 Reporting Using RADIUS Attribute v.92-info feature provides the ability to track V.92 call information, such as V.92 features that are supported, the Quick Connect feature set that was attempted, the duration for which the original call was put on hold, and how many times Modem On Hold was initiated. The vendor-specific attribute (VSA) v.92-info is included in accounting “start” and “stop” records when modems negotiate a V.92 connection. This feature was introduced in Cisco IOS Release 12.3(1).

CHAPTER 12

RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements

The RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements feature allows the hostname of the network access server (NAS) to be specified--rather than the IP address of the NAS--in RADIUS attribute 66 (Tunnel-Client-Endpoint). This feature makes it easier for users to remember a hostname instead of a numerical IP address, and helps disguise the numerical IP address of the NAS.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements

A Cisco platform that supports VPDN is required. See the Glossary, on page 137 for more information about VPDN.

Restrictions for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements

Your Cisco device must be running a Cisco software image that supports virtual private dialup networks (VPDNs).

Information About RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements

How the RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements are Used

Virtual Private Networks (VPNs) use Layer 2 Forwarding (L2F) or Layer 2 Tunnel Protocol (L2TP) tunnels to tunnel the link layer of high-level protocols (for example, PPP or asynchronous High-Level Data Link Control (HDLC)). Internet service providers (ISPs) configure their NASs to receive calls from users and forward the calls to the customer tunnel server. Usually, the ISP maintains only information about the tunnel server--the tunnel endpoint. The customer maintains the IP addresses, routing, and other user database functions of the tunnel server users. RADIUS attribute 66 provides the customer with the ability to specify the hostname of the NAS instead of the IP address of the NAS.

Note L2F is not supported on the Cisco ASR 1000 Series Aggregation Services Routers.

How to Configure RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements

There are no configuration tasks associated with support for the RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements.

Configuration Examples for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements

Setting Up the RADIUS Profile for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements Example

The following example shows a configuration that allows the user to specify the hostname of the NAS using RADIUS attribute 66 (Tunnel-Client-Endpoint) in the RADIUS profile:

```
cisco-avpair = vpdn:l2tp-cm-local-window-size=1024
cisco-avpair = vpdn:l2tp-nosession-timeout=30
cisco-avpair = vpdn:l2tp-cm-retransmit-retries=10
cisco-avpair = vpdn:l2tp-cm-min-timeout=2
cisco-avpair = vpdn:l2tp-hello-interval=60
Service-Type = outbound
Tunnel-Assignment-Id_tag1 = ISP1
Tunnel-Client-Auth-Id_tag1 = LAC1
Tunnel-Client-Endpoint_tag1 = 10.0.0.2
Tunnel-Medium-Type_tag1 = IPv4
Tunnel-Password_tag1 = tunnel1
Tunnel-Server-Auth-Id_tag1 = LNS1
Tunnel-Server-Endpoint_tag1 = 10.0.0.1
Tunnel-Type_tag1 = l2tp
```

Additional References

The following sections provide references related to the RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements feature.

Related Documents

Related Topic	Document Title
RADIUS attribute 66	*Cisco IOS XE Security Configuration Guide: Configuring User Services* , Release 2
Security commands	*Cisco IOS Security Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 19: Feature Information for RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements

Feature Name	Releases	Feature Information
RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements	12.1(5)T 12.2(28)SB	The RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements feature allows the hostname of the network access server (NAS) to be specified—rather than the IP address of the NAS—in RADIUS attribute 66 (Tunnel-Client-Endpoint). This feature makes it easier for users to remember a hostname instead of a numerical IP address, and helps disguise the numerical IP address of the NAS. This feature was introduced in Cisco IOS Release 12.1(5)T. This feature was integrated into Cisco IOS Release12.2(28)SB.

Glossary

L2F--Layer 2 Forwarding Protocol. Protocol that supports the creation of secure virtual private dialup networks over the Internet.

L2TP--Layer 2 Tunnel Protocol. Protocol that is one of the key building blocks for virtual private networks in the dial access space and is endorsed by Cisco and other internetworking industry leaders. This protocol combines the best of Cisco's Layer 2 Forwarding (L2F) protocol and Microsoft's Point-to-Point Tunneling Protocol (PPTP).

Layer 2 Forwarding Protocol--See L2F.

Layer 2 Tunnel Protocol--See L2TP.

Point-to-Point Protocol--See PPP.

PPP--Point-to-Point Protocol. Successor to SLIP that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Whereas SLIP was designed to work with IP, PPP was designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: LCP and NCP.

RADIUS--Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

Remote Authentication Dial-In User Service--See RADIUS.

virtual private dialup network--See VPDN.

VPDN--virtual private dialup network. A system that permits dial-in networks to exist remotely to home networks, while giving the appearance of being directly connected. VPDNs use L2TP and L2F to terminate the Layer 2 and higher parts of the network connection at the L2TP network server (LNS), instead of the L2TP access concentrator (LAC).

CHAPTER 13

RADIUS Attribute Screening

The RADIUS Attribute Screening feature allows users to configure a list of "accept" or "reject" RADIUS attributes on the network access server (NAS) for purposes such as authorization or accounting.

If a NAS accepts and processes all RADIUS attributes received in an Access-Accept packet, unwanted attributes may be processed, creating a problem for wholesale providers who do not control their customers' authentication, authorization, and accounting (AAA) servers. For example, there may be attributes that specify services to which the customer has not subscribed, or there may be attributes that may degrade service for other wholesale dial users. The ability to configure the NAS to restrict the use of specific attributes has therefore become a requirement for many users.

The RADIUS Attribute Screening feature should be implemented in one of the following ways:

- To allow the NAS to accept and process all standard RADIUS attributes for a particular purpose, except for those on a configured reject list
- To allow the NAS to reject (filter out) all standard RADIUS attributes for a particular purpose, except for those on a configured accept list

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for RADIUS Attribute Screening

Before configuring a RADIUS accept or reject list, you must enable AAA by using the **aaa new-model**command in global configuration mode.

Restrictions for RADIUS Attribute Screening

NAS Requirements

To enable this feature, your NAS should be configured for authorization with RADIUS groups.

Accept or Reject Lists Limitations

The two filters used to configure accept or reject lists are mutually exclusive; therefore, a user can configure only one access list or one reject list for each purpose, per server group.

Vendor-Specific Attributes

This feature does not support vendor-specific attribute (VSA) screening; however, a user can specify attribute 26 (Vendor-Specific) in an accept or reject list, which accepts or reject all VSAs.

Required Attributes Screening Recommendation

It is recommended that users do not reject the following required attributes:

- For authorization:
  - 6 (Service-Type)
  - 7 (Framed-Protocol)
- For accounting:
  - 4 (NAS-IP-Address)
  - 40 (Acct-Status-Type)
  - 41 (Acct-Delay-Time)
  - 44 (Acct-Session-ID)

If an attribute is required, the rejection is refused, and the attribute is allowed to pass through.

Note The user does not receive an error at the point of configuring a reject list for required attributes because the list does not specify a purpose--authorization or accounting. The server determines whether an attribute is required when it is known what the attribute is to be used for.

Information About RADIUS Attribute Screening

The RADIUS Attribute Screening feature provides the following benefits:

- Users can configure an accept or reject list consisting of a selection of attributes on the NAS for a specific purpose so unwanted attributes are not accepted and processed.
- Users may wish to configure an accept list that includes only relevant accounting attributes, thereby reducing unnecessary traffic and allowing users to customize their accounting data.

How to Screen RADIUS Attributes

Configuring RADIUS Attribute Screening

To configure a RADIUS attribute accept or reject list for authorization or accounting, use the following commands:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authentication ppp default**
4. **aaa authorization network default group** *group-name*
5. **aaa group server radius** *group-name*
6. **server** *ip-address*
7. **authorization** [**accept** | **reject**] *listname*
8. Router(config-sg-radius)# **exit**
9. **radius-server host** {*hostname* | *ip-address*} [**key** *string*
10. **radius-server attribute list** *listname*
11. **attribute** *number number* [*number...*]]

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa authentication ppp default** **Example:** **group** *group-name* **Example:** `Router(config)# aaa authentication ppp default group radius-sg`	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
Step 4	**aaa authorization network default group** *group-name* **Example:** `Router(config)# aaa authorization network default group radius-sg`	Sets parameters that restrict network access to the user.
Step 5	**aaa group server radius** *group-name* **Example:** `Router(config)# aaa group server radius radius-sg`	Groups different RADIUS server hosts into distinct lists and distinct methods.
Step 6	**server** *ip-address* **Example:** `Router(config-sg-radius)# server 10.1.1.1`	Configures the IP address of the RADIUS server for the group server,
Step 7	**authorization** [**accept** | **reject**] *listname* **Example:** `and/or`	Specifies a filter for the attributes that are returned in an Access-Accept packet from the RADIUS server. and/or Specifies a filter for the attributes that are to be sent to the RADIUS server in an accounting request.

	Command or Action	Purpose
	Example: **accounting** [**accept** | **reject**] *listname* **Example:** `Router(config-sg-radius)# authorization accept min-author`	**Note** The **accept** keyword indicates that all attributes are rejected except for the attributes specified in the *listname*. The **reject** keyword indicates that all attributes are accepted except for the attributes specified in the *listname* and all standard attributes.
Step 8	Router(config-sg-radius)# **exit**	Exits server-group configuration mode.
Step 9	**radius-server host** {*hostname* | *ip-address*} [**key** *string* **Example:** `Router(config)# radius-server host 10.1.1.1 key mykey1`	Specifies a RADIUS server host.
Step 10	**radius-server attribute list** *listname* **Example:** `Router(config)# radius-server attribute list min-author`	Defines the list name given to the set of attributes defined in the **attribute** command and enters server-group configuration mode. **Note** The *listname* must be the same as the *listname* defined in Step 5.
Step 11	**attribute** *number* *number* [*number...*]] **Example:** `Router(config-sg-radius)# attribute 6-7`	Adds RADIUS attributes to the configured accept or reject list. See the " RADIUS Attributes Overview and RADIUS IETF Attributes " feature module for more information. **Note** This command can be used multiple times to add attributes to an accept or reject list. **Note** The user-password (RADIUS attribute 2) and nas-ip (RADIUS attribute 4) attributes can be filtered together successfully in the access request if they are configured to be filtered. An access request must contain either a user-password or a CHAP password or a state. Also, either a NAS IP address or NAS identifier must be present in a RADIUS accounting request.

Verifying RADIUS Attribute Screening

To verify an accept or reject list, use one of the following commands in privileged EXEC mode:

Command	Purpose
`Router#` **debug aaa accounting**	Displays information on accountable events as they occur.
`Router#` **debug aaa authentication**	Displays information on AAA authentication.
`Router#` **show radius statistics**	Displays the RADIUS statistics for accounting and authentication packets.

Configuration Examples for RADIUS Attribute Screening

Authorization Accept Example

The following example shows how to configure an accept list for attribute 6 (Service-Type) and attribute 7 (Framed-Protocol); all other attributes (including VSAs) are rejected for RADIUS authorization.

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 10.1.1.1
authorization accept min-author
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list min-author
attribute 6-7
```

Accounting Reject Example

The following example shows how to configure a reject list for attribute 66 (Tunnel-Client-Endpoint) and attribute 67 (Tunnel-Server-Endpoint); all other attributes (including VSAs) are accepted for RADIUS accounting.

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 10.1.1.1
accounting reject tnl-x-endpoint
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list tnl-x-endpoint
attribute 66-67
```

Authorization Reject and Accounting Accept Example

The following example shows how to configure a reject list for RADIUS authorization and configure an accept list for RADIUS accounting. Although you cannot configure more than one accept or reject list per server group for authorization or accounting, you can configure one list for authorization and one list for accounting per server group.

```
aaa new-model
aaa authentication ppp default group radius-sg
aaa authorization network default group radius-sg
aaa group server radius radius-sg
server 10.1.1.1
authorization reject bad-author
accounting accept usage-only
!
radius-server host 10.1.1.1 key mykey1
radius-server attribute list usage-only
attribute 1,40,42-43,46
!
radius-server attribute list bad-author
attribute 22,27-28,56-59
```

Rejecting Required Attributes Example

The following example shows debug output for the **debug aaa accounting** command. In this example, required attributes 44, 40, and 41 have been added to the reject list “standard.”

```
Router# debug aaa authorization
AAA/ACCT(6): Accounting method=radius-sg (radius)
RADIUS: attribute 44 cannot be rejected
RADIUS: attribute 61 rejected
RADIUS: attribute 31 rejected
RADIUS: attribute 40 cannot be rejected
RADIUS: attribute 41 cannot be rejected
```

Additional References

The following sections provide references related to the RADIUS Attribute Screening feature.

Related Documents

Related Topic	Document Title
IOS AAA security features	*Cisco IOS Security Configuration Guide: Securing User Services* , Release 12.4T.
Cisco IOS Security Commands	*Cisco IOS Security Command Reference*
RADIUS	“ Configuring RADIUS ” module.

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this release.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for RADIUS Attribute Screening

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 20: Feature Information for RADIUS Attribute Screening

Feature Name	Releases	Feature Information
RADIUS Attribute Screening	12.2(1)DX 12.2(2)DD 12.2(4)B 12.2(4)T 12.2(13)T 12.2(33)SRC	The RADIUS Attribute Screening feature allows users to configure a list of "accept" or "reject" RADIUS attributes on the network access server (NAS) for purposes such as authorization or accounting. This feature was introduced in 12.2(1)DX. This feature was integrated into Cisco IOS Release 12.2(2)DD. This feature was integrated into Cisco IOS Release 12.2(4)B. This feature was integrated into 12.2(4)T. This feature was integrated into Cisco IOS Release 12.2(33)SRC. Platform support was added for the Cisco 7401 ASR router. The Cisco 7200 series platform applies to the Cisco IOS Releases 12.2(1)DX, 12.2(2)DD, 12.2(4)B, 12.2(4)T, and 12.2(13)T. The Cisco 7401 ASR platform applies to Cisco IOS Release 12.2(13)T only. The following commands were introduced or modified by this feature: **accounting (server-group configuration), authorization (server-group configuration), attribute (server-group configuration), radius-server attribute list**

Glossary

AAA --authentication, authorization, and accounting. Suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server.

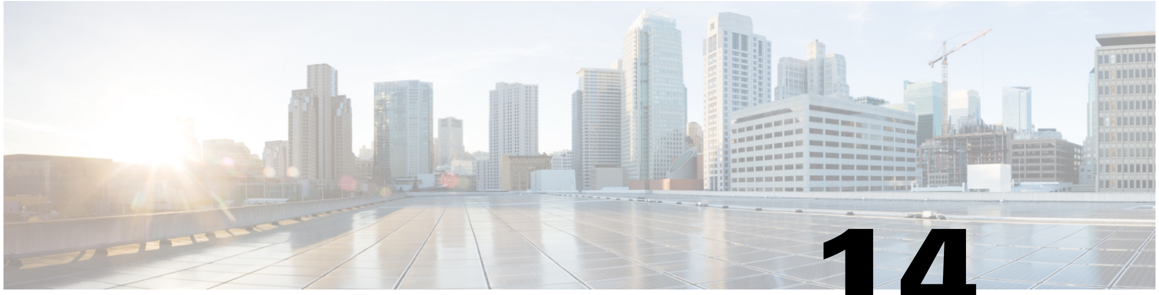
attribute --RADIUS Internet Engineering Task Force (IETF) attributes are the original set of 255 standard attributes that are used to communicate AAA information between a client and a server. Because IETF attributes are standard, the attribute data is predefined and well known; thus all clients and servers who exchange AAA information via IETF attributes must agree on attribute data such as the exact meaning of the attributes and the general bounds of the values for each attribute.

NAS --network access server. A Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the Public Switched Telephone Network).

RADIUS --Remote Authentication Dial-In User Service. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

VSA --vendor-specific attribute. VSAs are derived from one IETF attribute--vendor-specific (attribute 26). Attribute 26 allows a vendor to create and implement an additional 255 attributes. That is, a vendor can create an attribute that does not match the data of any IETF attribute and encapsulate it behind attribute 26: essentially, Vendor-Specific ="protocol:attribute=value".

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



CHAPTER 14

RADIUSNAS-IP-AddressAttributeConfigurability

The RADIUS NAS-IP-Address Attribute Configurability feature allows an arbitrary IP address to be configured and used as RADIUS attribute 4, NAS-IP-Address, without changing the source IP address in the IP header of the RADIUS packets. This feature may be used for situations in which service providers are using a cluster of small network access servers (NASs) to simulate a large NAS to improve scalability. This feature allows the NASs to behave as a single RADIUS client from the perspective of the RADIUS server.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for RADIUS NAS-IP-Address Attribute Configurability

The following requirements are necessary before configuring this feature:

- Experience with IP Security (IPSec) and configuring both RADIUS servers and authentication, authorization, and accounting (AAA) is necessary.
- RADIUS server and AAA lists must be configured.

Restrictions for RADIUS NAS-IP-Address Attribute Configurability

The following restrictions apply if a cluster of RADIUS clients are being used to simulate a single RADIUS client for scalability. Solutions, or workarounds, to the restrictions are also provided.

- RADIUS attribute 44, Acct-Session-Id, may overlap among sessions from different NASs.

There are two solutions. Either the **radius-server attribute 44 extend-with-addr** or **radius-server unique-ident** command can be used on NAS routers to specify different prepending numbers for different NAS routers.

- RADIUS server-based IP address pool for different NASs must be managed.

The solution is to configure different IP address pool profiles for different NASs on the RADIUS server. Different NASs use different pool usernames to retrieve them.

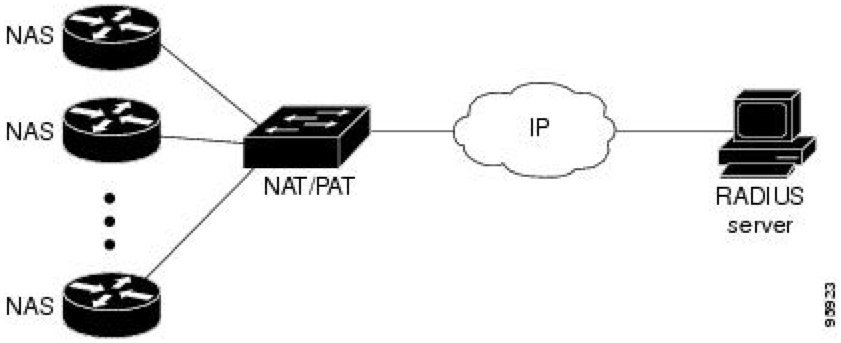
- RADIUS request message for sessions from different NASs must be differentiated.

One of the solutions is to configure different format strings for RADIUS attribute 32, NAS-Identifier, using the **radius-server attribute 32 include-in-access-req** command on different NASs.

Information About RADIUS NAS-IP-Address Attribute Configurability

To simulate a large NAS RADIUS client using a cluster of small NAS RADIUS clients, as shown in Information About RADIUS NAS-IP-Address Attribute Configurability, a Network Address Translation (NAT) or Port Address Translation (PAT) device is inserted in a network. The device is placed between a cluster of NASs and the IP cloud that is connected to a RADIUS server. When RADIUS traffic from different NASs goes through the NAT or PAT device, the source IP addresses of the RADIUS packets are translated to a single IP address, most likely an IP address on a loopback interface on the NAT or PAT device. Different User Datagram Protocol (UDP) source ports are assigned to RADIUS packets from different NASs. When the RADIUS reply comes back from the server, the NAT or PAT device receives it, uses the destination UDP port to translate the destination IP address back to the IP address of the NAS, and forwards the reply to the corresponding NAS.

The figure below demonstrates how the source IP addresses of several NASs are translated to a single IP address as they pass through the NAT or PAT device on the way to the IP cloud.



RADIUS servers normally check the source IP address in the IP header of the RADIUS packets to track the source of the RADIUS requests and to maintain security. The NAT or PAT solution satisfies these requirements because only a single source IP address is used even though RADIUS packets come from different NAS routers.

However, when retrieving accounting records from the RADIUS database, some billing systems use RADIUS attribute 4, NAS-IP-Address, in the accounting records. The value of this attribute is recorded on the NAS routers as their own IP addresses. The NAS routers are not aware of the NAT or PAT that runs between them and the RADIUS server; therefore, different RADIUS attribute 4 addresses will be recorded in the accounting records for users from the different NAS routers. These addresses eventually expose different NAS routers to the RADIUS server and to the corresponding billing systems.

Using the RADIUS NAS-IP-Address Attribute Configurability Feature

The RADIUS NAS-IP-Address Attribute Configurability feature allows you to freely configure an arbitrary IP address as RADIUS NAS-IP-Address, RADIUS attribute 4. By manually configuring the same IP address, most likely the IP address on the loopback interface of the NAT or PAT device, for all the routers, you can hide a cluster of NAS routers behind the NAT or PAT device from the RADIUS server.

How to Configure RADIUS NAS-IP-Address Attribute Configurability

Configuring RADIUS NAS-IP-Address Attribute Configurability

Before configuring the RADIUS NAS-IP-Address Attribute Configurability feature, you must have configured the RADIUS servers or server groups and AAA method lists.

To configure the RADIUS NAS-IP-Address Attribute Configurability feature, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server attribute 4** *ip-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server attribute 4** *ip-address* **Example:** `Router (config)# radius-server attribute 4 10.2.1.1`	Configures an IP address to be used as the RADIUS NAS-IP-Address, attribute 4.

Monitoring and Maintaining RADIUS NAS-IP-Address Attribute Configurability

To monitor the RADIUS attribute 4 address that is being used inside the RADIUS packets, use the **debug radius** command.

SUMMARY STEPS

1. **enable**
2. **debug radius**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug radius** **Example:** `Router# debug radius`	Displays information associated with RADIUS.

Example

The following sample output is from the **debug radius** command:

```
Router# debug radius
RADIUS/ENCODE(0000001C): acct_session_id: 29
RADIUS(0000001C): sending
RADIUS(0000001C): Send Access-Request to 10.0.0.10:1645 id 21645/17, len 81
RADIUS:  authenticator D0 27 34 C0 F0 C4 1C 1B - 3C 47 08 A2 7E E1 63 2F
RADIUS:  Framed-Protocol     [7]   6   PPP                      [1]
RADIUS:  User-Name           [1]   18  "shashi@pepsi.com"
RADIUS:  CHAP-Password       [3]   19  *
RADIUS:  NAS-Port-Type       [61]  6   Virtual                  [5]
RADIUS:  Service-Type        [6]   6   Framed                   [2]
RADIUS:  NAS-IP-Address      [4]   6   10.0.0.21
UDP: sent src=10.1.1.1(21645), dst=10.0.0.10(1645), length=109
UDP: rcvd src=10.0.0.10(1645), dst=10.1.1.1(21645), length=40
RADIUS: Received from id 21645/17 10.0.0.10:1645, Access-Accept, len 32
RADIUS:  authenticator C6 99 EC 1A 47 0A 5F F2 - B8 30 4A 4C FF 4B 1D F0
RADIUS:  Service-Type        [6]   6   Framed                   [2]
RADIUS:  Framed-Protocol     [7]   6   PPP                      [1]
RADIUS(0000001C): Received from id 21645/17
```

Configuration Examples for RADIUS NAS-IP-Address Attribute Configurability

Configuring a RADIUS NAS-IP-Address Attribute Configurability Example

The following example shows that IP address 10.0.0.21 has been configured as the RADIUS NAS-IP-Address attribute:

```
radius-server attribute 4 10.0.0.21
radius-server host 10.0.0.10 auth-port 1645 acct-port 1646 key cisco
```

Additional References

The following sections provide references related to RADIUS NAS-IP-Address Attribute Configurability.

Related Documents

Related Topic	Document Title
Configuring AAA	"Authentication, Authorization, and Accounting (AAA)" section of *Cisco IOS Security Configuration Guide: Securing User Services*
Configuring RADIUS	" Configuring RADIUS " module.

Related Topic	Document Title
RADIUS commands	*Cisco IOS Security Command Reference*

Standards

Standards	Title
No new or modified standards are supported by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for RADIUS NAS-IP-Address Attribute Configurability

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 21: Feature Information for RADIUS NAS-IP-Address Attribute Configurability

Feature Name	Releases	Feature Information
RADIUS NAS-IP-Address Attribute Configurability	12.3(3)B 12.3(7)T 12.2(28)SB 12.2(33)SRC	This feature allows an arbitrary IP address to be configured and used as RADIUS attribute 4, NAS-IP-Address, without changing the source IP address in the IP header of the RADIUS packets. This feature was introduced into Cisco IOS Release 12.3(3)B. This feature was integrated into Cisco IOS Release 12.3(7)T. This feature was integrated into Cisco IOS Release 12.2(28)SB. This feature was integrated into Cisco IOS Release 12.2(33)SRC. The **radius-server attribute 4** command was introduced this feature.

CHAPTER 15

AAA Per VC QoS Policy Support

The AAA Per VC QoS Policy Support feature provides the ability to modify an existing quality of service (QoS) profile applied to a session while that session remains active using new Cisco attribute-value (AV) pairs that specify service policy output and service policy input.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for AAA Per VC QoS Policy Support

You should be familiar with defining policy maps for managing subscriber sessions, and with configuring QoS traffic conditioning. See the Additional References, on page 89 section for information on these topics.

Restrictions for AAA Per VC QoS Policy Support

Although there are no specific restrictions for using the AAA Per VC QoS Policy Support feature, defect report CSCef69140 describes a problem whereby in PPPoA sessions, an input service policy cannot be applied at the ATM virtual circuit (VC) level. Instead, an input service policy, and therefore an input policy AV pair, must be applied under interface virtual template mode.

Also, read through the configuration guidelines in the Interface Policy Map AAA Attributes section before using the attributes described in this document.

Information About AAA Per VC QoS Policy Support

RADIUS Push and Pull

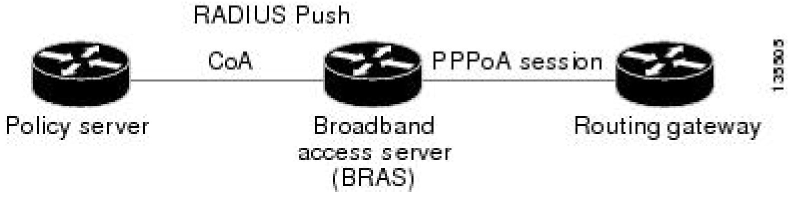
Cisco Systems software offers applications for the DSL aggregation market and service providers that make powerful use of dynamic policy maps. Policy maps govern user services to be deployed in the network and are triggered by a service or by a user--concepts referred to as push and pull. Pull refers to a policy applied during authentication. Push refers to the dynamic change of policy on the session using Change of Authorization (CoA) message. Before the AAA Per VC QoS Policy Support feature introduced in Cisco IOS Release 12.4(2)T, there was no RADIUS push and pull capability for a policy map at the ATM VC level. RADIUS only supported dynamic bandwidth selection and virtual access interface policy maps applied during the establishment of a PPP session. The AAA Per VC QoS Policy Support feature provides support for RADIUS push and pull capability for a policy map at the ATM VC level.

RADIUS pull of policy maps on a VC means that a policy map can be applied on the VC while a PPP over ATM (PPPoA) session is being established. PPPoA sessions are established between a policy server and a routing gateway.

Service policies are applied only when a subscriber first authenticates the VC. Software creates an identifier that is used as the session unique identifier between the router and the RADIUS server using RADIUS Internet Engineering Task Force (IETF) attribute 44. This identifier is sent with an Access Request message and all accounting records for that session.

RADIUS push functionality provides the ability to modify an existing QoS profile applied to a session while that session remains active. A policy server governs the authorization of active sessions with its ability to send a Change of Authorization (CoA) message (see the figure below). Specific events can trigger the CoA message and allow modification of the QoS configuration. Implementation of RADIUS push eliminates the need to preprovision subscribers, allowing QoS policies to be transparently applied where and when required without the disruption of session reauthentication.

Figure 6: RADIUS Push



These abilities provide a high degree of flexibility, smaller configuration files, and more efficient use of queueing resources. And perhaps more importantly, RADIUS push and pull eliminates the need to statically configure a policy map on every VC or VLAN.

This feature is implemented by Cisco AV pairs that identify QoS policies configured on the router from a RADIUS server by defining service policy output and service policy input. The AV pairs place the appropriate policy map, which is identified by name, directly on the interface. The interface can be either an ATM VC or Ethernet VLAN.

After the initial subscriber authentication, authorization process, RADIUS returns the appropriate AV name for the policy maps to be applied at the VC and virtual-access interface level. The QoS policy maps define the subscriber user experience for broadband service and can be leveraged to deliver higher value services such as VoIP and video.

Interface Policy Map AAA Attributes

Two new generic Cisco RADIUS VSA attributes are introduced by the AAA Per VC QoS Policy Support feature, as follows:

```
cisco-avpair = “atm:vc-qos-policy-in=in-policy-name
”
cisco-avpair = “atm:vc-qos-policy-out=out-policy-name
”
```

Use these attributes in the RADIUS server profile to define service policy output and service policy input. The AV pairs place the appropriate policy map, which is identified by name, directly on the interface. The interface can be either an ATM VC or Ethernet VLAN.

The AAA Per VC QoS Policy Support feature also replaces the following generic Cisco RADIUS vendor-specific attribute (VSA) attributes:

```
cisco-avpair = “ip:sub-policy-In=in-policy-name
”
cisco-avpair = “ip:sub-policy-Out=out-policy-name
”
```

with the following new attributes:

```
cisco-avpair = "ip:sub-qos-policy-in=in-policy-name
”
cisco-avpair = "ip:sub-qos-policy-out=out-policy-name
”
```

The replaced attributes will be supported for several more software releases, but profiles should be updated with the new attributes as soon as it is feasible to do so.

Remember the following guidelines as you configure these attributes:

- A policy map pulled or pushed from the RADIUS server has a higher precedence than a policy map configured under a permanent virtual circuit (PVC).
- The Cisco IOS **show policy-map interface**EXEC command will display the policy map pushed or pulled from the RADIUS server. This policy map is actually used by the driver, even though the policy map was configured using the **service-policy** command under PVC configuration mode.
- Once a policy map is pushed or pulled on the VC and successfully installed or updated, any configuration or removal of the configuration would affect only the running configuration, and not the driver and actual policy map used by the VC.

- You must enable dynamic bandwidth selection using the **dbs enable**command. Dynamic policies that are pulled and pushed from the RADIUS server must be specifically disabled using the **no dbs enable** command.

Configuration Examples for AAA Per VC QoS Policy Support

RADIUS Interface Policy Map Profile Example

Following is an example of a RADIUS profile defining an input service policy named test_vc:

```
radius subscriber 2
 vsa cisco generic 1 string “atm:vc-qos-policy-in=test_vc”
 attribute 1 string “user@cisco.com”
 attribute 44 string “00000002”
!
radius client 192.168.1.4 access-ports 1645 1645 accounting-ports 1646 1646
radius host 192.168.1.3 auth-port 1645 acct-port 1646 key 0 cisco
radius host 192.168.1.4 auth-port 1645 acct-port 1646
radius retransmit 0
radius timeout 15
radius key 0 cisco
radius server 192.168.1.4
 client 192.168.1.3 shared-secret word
```

Define the Policy Map on the Router Example

The following example shows the Cisco IOS commands that are used to define the service policy on the router:

```
!
interface ATM4/0
 no ip address
 no atm ilmi-keepalive
 pvc 1/101
  dbs enable
  service-policy input test_vc
 !
end
```

Display the Service Policy Example

The following example shows the report from the **show policy-map interface**command when the policy map named test_vc has been pushed on PVC 1/101:

```
Router# show policy interface atm 4/0
 ATM4/0: VC 1/101 -
  Service-policy input: test_vc
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Additional References

The following sections provide references related to the RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature.

Related Documents

Related Topic	Document Title
Configuring authentication and configuring RADIUS	“ Configuring Authentication ” and “Configuring RADIUS ” chapters, *Cisco Security Configuration Guide*
RFC 2138 (RADIUS)	RFC 2138 , Remote Authentication Dial In User Service (RADIUS)

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for AAA Per VC QoS Policy Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 22: Feature Information for AAA Per VC QoS Policy Support

Feature Name	Releases	Feature Information
AAA Per VC QoS Policy Support	12.4(2)T 12.2(33)SRE	The AAA Per VC QoS Policy Support feature provides the ability to modify an existing quality of service (QoS) profile applied to a session while that session remains active using new Cisco attribute-value (AV) pairs that specify service policy output and service policy input. In 12.4(2)T, this feature was introduced on the Cisco 10000. In Cisco IOS Release 12.2(33)SRE, the AAA Per VC QoS Policy Support feature was added for the Cisco 7600 series router.