



## **RADIUS Attributes Configuration Guide Cisco IOS XE Release 2**

### **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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2012 Cisco Systems, Inc. All rights reserved.



## **CONTENTS**

### **RADIUS Attributes Overview and RADIUS IETF Attributes 1**

Finding Feature Information 1

RADIUS Attributes Overview 1

IETF Attributes Versus VSAs 1

RADIUS Packet Format 2

RADIUS Packet Types 3

RADIUS Files 3

Dictionary File 3

Clients File 4

Users File 4

RADIUS IETF Attributes 5

Supported RADIUS IETF Attributes 5

Comprehensive List of RADIUS Attribute Descriptions 8

Additional References 24

Feature Information for RADIUS Attributes Overview and RADIUS IETF Attributes 26

### **RADIUS Vendor-Proprietary Attributes 33**

Finding Feature Information 33

Supported Vendor-Proprietary RADIUS Attributes 33

Comprehensive List of Vendor-Proprietary RADIUS Attribute Descriptions 39

Feature Information for RADIUS Vendor-Proprietary Attributes 50

### **RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values 51**

Finding Feature Information 51

Information About RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values 51

RADIUS Disconnect-Cause Attribute Values 59

Additional References 61

Feature Information for RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values 63

### **Connect-Info RADIUS Attribute 77 65**

|  |           |
|--|-----------|
| Finding Feature Information  | 65        |
| Prerequisites for Connect-Info RADIUS Attribute 77                                 | 66        |
| Information About Connect-Info RADIUS Attribute 77                                 | 66        |
| Customizing Attribute 77 for Ethernet Connections                                  | 66        |
| Customizing Attribute 77 for ATM Connections                                       | 66        |
| How to Verify the Connect-Info RADIUS Attribute 77                                 | 67        |
| Verifying the Connect-Info RADIUS Attribute 77                                     | 67        |
| Additional References  | 69        |
| Feature Information for Connect-Info RADIUS Attribute 77                           | 70        |
| <b>Encrypted Vendor-Specific Attributes</b>  | <b>73</b> |
| Finding Feature Information  | 73        |
| Prerequisites for Encrypted Vendor-Specific Attributes                             | 73        |
| Information About Encrypted Vendor-Specific Attributes                             | 74        |
| Tagged String VSA  | 74        |
| Encrypted String VSA   | 74        |
| Tagged and Encrypted String VSA  | 75        |
| How to Verify Encrypted Vendor-Specific Attributes                                 | 75        |
| Configuration Examples for Encrypted Vendor-Specific Attributes                    | 75        |
| NAS Configuration Example  | 75        |
| RADIUS User Profile with a Tagged and Encrypted VSA Example                        | 76        |
| Additional References  | 76        |
| Feature Information for Encrypted Vendor-Specific Attributes                       | 77        |
| <b>RADIUS Attribute 8 Framed-IP-Address in Access Requests</b>                     | <b>79</b> |
| Finding Feature Information  | 79        |
| Prerequisites for RADIUS Attribute 8 Framed-IP-Address in Access Requests          | 79        |
| Information About RADIUS Attribute 8 Framed-IP-Address in Access Requests          | 80        |
| How This Feature Works   | 80        |
| Benefits   | 80        |
| How to Configure RADIUS Attribute 8 Framed-IP-Address in Access Requests           | 80        |
| Configuring RADIUS Attribute 8 in Access Requests                                  | 81        |
| Verifying RADIUS Attribute 8 in Access Requests                                    | 81        |
| Configuration Examples for RADIUS Attribute 8 Framed-IP-Address in Access Requests | 82        |
| NAS Configuration That Sends the IP Address of the Dial-in Host Example            | 82        |
| Additional References  | 83        |
| Feature Information for RADIUS Attribute 8 Framed-IP-Address in Access Requests    | 84        |

|   |            |
|---|------------|
| <b>RADIUS Attribute 82 Tunnel Assignment ID</b>                           | <b>87</b>  |
| Finding Feature Information   | 87         |
| Restrictions for Radius Attribute 82 Tunnel Assignment ID                 | 87         |
| Information about RADIUS Attribute 82 Tunnel Assignment ID                | 87         |
| Benefits  | 87         |
| How to Configure RADIUS Attribute 82 Tunnel Assignment ID                 | 88         |
| Verifying RADIUS Attribute 82   | 88         |
| Configuration Examples for RADIUS Attribute 82 Tunnel Assignment ID       | 88         |
| LAC Configuration Example   | 88         |
| LNS Configuration Example   | 89         |
| RADIUS Configuration Example  | 89         |
| Additional References   | 90         |
| Feature Information for RADIUS Attribute 82 Tunnel Assignment ID          | 91         |
| <b>RADIUS Tunnel Attribute Extensions</b>                                 | <b>93</b>  |
| Finding Feature Information   | 93         |
| Prerequisites   | 93         |
| Restrictions  | 93         |
| Information About RADIUS Tunnel Attribute Extensions                      | 94         |
| RADIUS Tunnel Attribute Extension Benefits                                | 94         |
| RADIUS Tunnel Attribute Extension Description                             | 94         |
| How to Configure RADIUS Tunnel Attribute Extensions                       | 95         |
| Verifying RADIUS Attribute 90 and RADIUS Attribute 91                     | 95         |
| Configuration Examples for RADIUS Tunnel Attribute Extensions             | 95         |
| L2TP Network Server Configuration Example                                 | 95         |
| RADIUS User Profile with RADIUS Tunneling Attributes 90 and 91 Example    | 96         |
| Additional References   | 96         |
| Feature Information for RADIUS Tunnel Attribute Extensions                | 97         |
| Glossary  | 98         |
| <b>RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements</b>            | <b>101</b> |
| Finding Feature Information   | 101        |
| Prerequisites for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements | 101        |
| Restrictions for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements  | 102        |
| Information About RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements | 102        |
| How the RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements are Used  | 102        |
| How to Configure RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements  | 102        |

|   |            |
|---|------------|
| Configuration Examples for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements                | 102        |
| Setting Up the RADIUS Profile for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements Example | 103        |
| Additional References   | 103        |
| Feature Information for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements                   | 104        |
| Glossary  | 105        |
| <b>RADIUS Attribute Value Screening</b>   | <b>107</b> |
| Finding Feature Information   | 107        |
| Prerequisites for RADIUS Attribute Value Screening  | 107        |
| Restrictions for RADIUS Attribute Value Screening   | 108        |
| Information About RADIUS Attribute Value Screening  | 108        |
| How to Screen RADIUS Attributes   | 109        |
| Configuring RADIUS Attribute Value Screening  | 109        |
| Verifying RADIUS Attribute Value Screening  | 110        |
| Configuration Examples for RADIUS Attribute Value Screening                                       | 111        |
| Authorization Accept Example  | 111        |
| Accounting Reject Example   | 111        |
| Authorization Reject and Accounting Accept Example  | 112        |
| Rejecting Required Attributes Example   | 112        |
| Additional References   | 112        |
| Feature Information for RADIUS Attribute Value Screening  | 113        |



# 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 is stored on the RADIUS daemon. This chapter lists the RADIUS attributes currently supported.

- [Finding Feature Information, page 1](#)
- [RADIUS Attributes Overview, page 1](#)
- [RADIUS IETF Attributes, page 5](#)
- [Additional References, page 24](#)
- [Feature Information for RADIUS Attributes Overview and RADIUS IETF Attributes, page 26](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

## RADIUS Attributes Overview

- [IETF Attributes Versus VSAs, page 1](#)
- [RADIUS Packet Format, page 2](#)
- [RADIUS Files, page 3](#)

## 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. 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.

RADIUS vendor-specific attributes (VSAs) derived from one IETF attribute--vendor-specific (attribute 26). Attribute 26 allows a vendor to create an additional 255 attributes however they wish. That is, a vendor can

create an attribute that does not match the data of any IETF attribute and encapsulate it behind attribute 26; thus, the newly created attribute is accepted if the user accepts attribute 26.

For more information on VSAs, refer to “Chapter 1, “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.

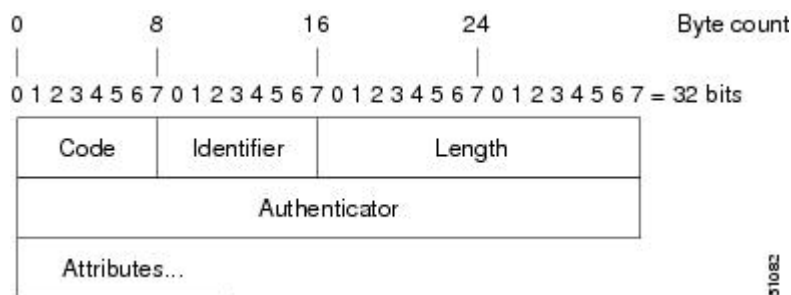
The figure below shows the fields within a RADIUS packet.



### Note

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

**Figure 1 RADIUS Packet Diagram**



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. Two types of authenticators are as follows:
  - 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, page 3](#)



## RADIUS Packet Types

The following list defines the various types of RADIUS packet types that can 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. Any user performing authentication must submit an Access-Request packet. Once an Access-Request packet is received, the RADIUS server must forward a reply.

**Access-Accept**-- Once 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**-- Once 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**-- Once 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 should 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; the users file defines which user requests the RADIUS server will authenticate based on security and configuration data.

- [Dictionary File, page 3](#)
- [Clients File, page 4](#)
- [Users File, page 4](#)

## Dictionary File

A dictionary file provides a list of attributes that are dependent upon which attributes your NAS supports. However, you can add your own set of attributes to your dictionary for custom solutions. It defines attribute values, thereby allowing you to 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 follow 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 is important because it 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 the client sends the server must be an exact match with the data contained in 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 referred to 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, please note the 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 cisco.com, the password is cisco, and the user can access five tunnel attributes.

```
# This user profile includes RADIUS tunneling attributes
cisco.com Password="cisco" 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

In Cisco IOS XE Release 2.1 for RADIUS tunnel attributes, 32 tagged tunnel sets are supported for L2TP.

- [Supported RADIUS IETF Attributes, page 5](#)
- [Comprehensive List of RADIUS Attribute Descriptions, page 8](#)

## Supported RADIUS IETF Attributes

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

Refer to the RADIUS IETF Attributes table for a description of each listed attribute.

**Table 1**      **Supported RADIUS IETF Attributes**

| Number | IETF Attribute     | XE 2.1 | XE 2.3 Changes |
|--------|--------------------|--------|----------------|
| 1      | User-Name          | yes    | --             |
| 2      | User-Password      | yes    | --             |
| 3      | CHAP-Password      | yes    | --             |
| 4      | NAS-IP Address     | yes    | --             |
| 5      | NAS-Port           | yes    | --             |
| 6      | Service-Type       | yes    | --             |
| 7      | Framed-Protocol    | yes    | --             |
| 8      | Framed-IP-Address  | yes    | --             |
| 9      | Framed-IP-Netmask  | yes    | --             |
| 10     | Framed-Routing     | yes    | --             |
| 11     | Filter-Id          | yes    | --             |
| 12     | Framed-MTU         | yes    | --             |
| 13     | Framed-Compression | yes    | --             |
| 14     | Login-IP-Host      | yes    | --             |
| 15     | Login-Service      | yes    | --             |

| Number | IETF Attribute           | XE 2.1 | XE 2.3 Changes |
|--------|--------------------------|--------|----------------|
| 16     | Login-TCP-Port           | yes    | --             |
| 18     | Reply-Message            | yes    | --             |
| 19     | Callback-Number          | yes    | --             |
| 20     | Callback-ID              | no     | --             |
| 22     | Framed-Route             | yes    | --             |
| 23     | Framed-IPX-Network       | no     | --             |
| 24     | State                    | yes    | --             |
| 25     | Class                    | yes    | --             |
| 26     | Vendor-Specific          | yes    | --             |
| 27     | Session-Timeout          | yes    | --             |
| 28     | Idle-Timeout             | yes    | --             |
| 29     | Termination-Action       | no     | --             |
| 30     | Called-Station-Id        | yes    | --             |
| 31     | Calling-Station-Id       | yes    | --             |
| 32     | NAS-Identifier           | yes    | --             |
| 33     | Proxy-State              | no     | --             |
| 34     | Login-LAT-Service        | yes    | --             |
| 35     | Login-LAT-Node           | yes    | --             |
| 36     | Login-LAT-Group          | no     | --             |
| 37     | Framed-AppleTalk-Link    | no     | --             |
| 38     | Framed-AppleTalk-Network | no     | --             |
| 39     | Framed-AppleTalk-Zone    | no     | --             |
| 40     | Acct-Status-Type         | yes    | --             |
| 41     | Acct-Delay-Time          | yes    | --             |
| 42     | Acct-Input-Octets        | yes    | --             |
| 43     | Acct-Output-Octets       | yes    | --             |
| 44     | Acct-Session-Id          | yes    | --             |

| Number | IETF Attribute            | XE 2.1 | XE 2.3 Changes |
|--------|---------------------------|--------|----------------|
| 45     | Acct-Authentic            | yes    | --             |
| 46     | Acct-Session-Time         | yes    | --             |
| 47     | Acct-Input-Packets        | yes    | --             |
| 48     | Acct-Output-Packets       | yes    | --             |
| 49     | Acct-Terminate-Cause      | yes    | --             |
| 50     | Acct-Multi-Session-Id     | yes    | --             |
| 51     | Acct-Link-Count           | yes    | --             |
| 52     | Acct-Input-Gigawords      | yes    | --             |
| 53     | Acct-Output-Gigawords     | yes    | --             |
| 55     | Event-Timestamp           | yes    | --             |
| 60     | CHAP-Challenge            | yes    | --             |
| 61     | NAS-Port-Type             | yes    | --             |
| 62     | Port-Limit                | yes    | --             |
| 63     | Login-LAT-Port            | no     | --             |
| 64     | Tunnel-Type <sup>1</sup>  | yes    | --             |
| 65     | Tunnel-Medium-Type1       | yes    | --             |
| 66     | Tunnel-Client-Endpoint    | no     | yes            |
| 67     | Tunnel-Server-Endpoint1   | yes    | --             |
| 68     | Acct-Tunnel-Connection-ID | yes    | --             |
| 69     | Tunnel-Password1          | yes    | --             |
| 70     | ARAP-Password             | no     | --             |
| 71     | ARAP-Features             | no     | --             |
| 72     | ARAP-Zone-Access          | no     | --             |
| 73     | ARAP-Security             | no     | --             |
| 74     | ARAP-Security-Data        | no     | --             |

<sup>1</sup> 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.

| Number | IETF Attribute                     | XE 2.1 | XE 2.3 Changes |
|--------|------------------------------------|--------|----------------|
| 75     | Password-Retry                     | no     | --             |
| 76     | Prompt                             | yes    | --             |
| 77     | Connect-Info                       | yes    | --             |
| 78     | Configuration-Token                | no     | --             |
| 79     | EAP-Message                        | no     | --             |
| 80     | Message-Authenticator              | no     | --             |
| 81     | Tunnel-Private-Group-ID            | no     | --             |
| 82     | Tunnel-Assignment-ID1              | yes    | --             |
| 83     | Tunnel-Preference                  | yes    | --             |
| 84     | ARAP-Challenge-Response            | no     | --             |
| 85     | Acct-Interim-Interval              | yes    | --             |
| 86     | Acct-Tunnel-Packets-Lost           | no     | --             |
| 87     | NAS-Port-ID                        | no     | --             |
| 88     | Framed-Pool                        | no     | --             |
| 90     | Tunnel-Client-Auth-ID <sup>2</sup> | yes    | --             |
| 91     | Tunnel-Server-Auth-ID              | yes    | --             |
| 200    | IETF-Token-Immediate               | no     | --             |

## 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. |

<sup>2</sup> This RADIUS attribute complies with RFC 2865 and RFC 2868.

| Number | IETF Attribute | Description  |
|--------|----------------|--|
| 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.   |
| 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       | <p>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 <b>radius-server extended-portnames</b> command). Each 16-bit number should be viewed as a 5-digit decimal integer for interpretation as follows:</p> <p>For asynchronous terminal lines, async network interfaces, and virtual async interfaces, the value is <b>00ttt</b>, where <b>ttt</b> is the line number or async interface unit number.</p> <p>For ordinary synchronous network interface, the value is <b>10xxx</b>.</p> <p>For channels on a primary rate ISDN interface, the value is <b>2ppcc</b>.</p> <p>For channels on a basic rate ISDN interface, the value is <b>3bb0c</b>.</p> <p>For other types of interfaces, the value is <b>6nnss</b>.</p> |

| Number | IETF Attribute    | Description   |
|--------|-------------------|---|
| 6      | Service-Type      | <p>Indicates the type of service requested or the type of service to be provided.</p> <ul style="list-style-type: none"> <li>• In a request:           <p>Framed for known PPP or SLIP connection. Administrative-user for <b>enable</b> command.</p> <ul style="list-style-type: none"> <li>• In response:               <p>Login--Make a connection. Framed--Start SLIP or PPP. Administrative User--Start an EXEC or <b>enable ok</b>.</p> <p>Exec User--Start an EXEC session.</p> <p>Service type is indicated by a particular numeric value as follows:</p> <ul style="list-style-type: none"> <li>• 1: Login</li> <li>• 2: Framed</li> <li>• 3: Callback-Login</li> <li>• 4: Callback-Framed</li> <li>• 5: Outbound</li> <li>• 6: Administrative</li> <li>• 7: NAS-Prompt</li> <li>• 8: Authenticate Only</li> <li>• 9: Callback-NAS-Prompt</li> </ul> </li> </ul> </li> </ul> |
| 7      | Framed-Protocol   | <p>Indicates the framing to be used for framed access. No other framing is allowed.</p> <p>Framing is indicated by a numeric value as follows:</p> <ul style="list-style-type: none"> <li>• 1: PPP</li> <li>• 2: SLIP</li> <li>• 3: ARA</li> <li>• 4: Gandalf-proprietary single-link/multilink protocol</li> <li>• 5: Xylogics-proprietary IPX/SLIP</li> </ul>   |
| 8      | Framed-IP-Address | <p>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 <b>radius-server attribute 8 include-in-access-req</b> command in global configuration mode.</p>   |



| Number | IETF Attribute     | Description   |
|--------|--------------------|---|
| 9      | Framed-IP-Netmask  | Indicates the IP netmask to be configured for the user when the user is a router to 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 a router to a network. Only “None” and “Send and Listen” values are supported for this attribute.<br><br>Routing method is indicated by a numeric value as follows: <ul style="list-style-type: none"> <li>• 0: None</li> <li>• 1: Send routing packets</li> <li>• 2: Listen for routing packets</li> <li>• 3: Send routing packets and listen for routing packets</li> </ul>              |
| 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 or some other means.  |
| 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. Not currently implemented for non-EXEC authorization.<br><br>Compression protocol is indicated by a numeric value as follows: <ul style="list-style-type: none"> <li>• 0: None</li> <li>• 1: VJ-TCP/IP header compression</li> <li>• 2: IPX header compression</li> </ul> |

| Number | IETF Attribute     | Description   |
|--------|--------------------|---|
| 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.<br>Service is indicated by a numeric value as follows: <ul style="list-style-type: none"> <li>• 0: Telnet</li> <li>• 1: Rlogin</li> <li>• 2: TCP-Clear</li> <li>• 3: PortMaster</li> <li>• 4: LAT</li> </ul>   |
| 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 via 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.   |
| 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 router 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.   |

| <b>Number</b> | <b>IETF Attribute</b> | <b>Description</b>   |
|---------------|-----------------------|--|
| 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 | <p>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:</p> <pre>protocol : attribute sep value</pre> <p>"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:</p> <pre>cisco-avpair= "ip:addr-pool=first" cisco-avpair= "shell:priv-lvl=15"</pre> <p>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.</p> <p>Table 1 lists supported vendor-specific RADIUS attributes (IETF attribute 26). The "TACACS+ Attribute-Value Pairs" appendix provides a complete list of supported TACACS+ attribute-value (AV) pairs that can be used with IETF attribute 26. (RFC 2865)</p> |
| 27     | Session-Timeout | <p>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."</p>   |

| Number | IETF Attribute     | Description  |
|--------|--------------------|--|
| 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: <ul style="list-style-type: none"> <li>• 0: Default</li> <li>• 1: RADIUS request</li> </ul>  |
| 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 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 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 <b>radius-server attribute 32 include-in-access-req</b> global configuration command to send RADIUS attribute 32 in an Access-Request or Accounting-Request. By default, the 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.   |

| Number | IETF Attribute            | Description  |
|--------|---------------------------|--|
| 34     | Login-LAT-Service         | Indicates the system with which the user is to be connected by LAT. This attribute is only available in the EXEC mode.   |
| 35     | Login-LAT-Node            | Indicates the node with which the user is to be automatically connected by LAT.  |
| 36     | Login-LAT-Group           | Identifies the LAT group codes that this user is authorized to use.  |
| 37     | Framed-AppleTalk-Link     | Indicates the AppleTalk network number that should be used for serial links to the user, which is another AppleTalk router.  |
| 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 this 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 router is power cycled or the software is reloaded. To send this attribute in access-request packets, use the <b>radius-server attribute 44 include-in-access-req</b> command in global configuration mode. |

| Number | IETF Attribute      | Description  |
|--------|---------------------|--|
| 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.  |
| 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.  |

| Number | IETF Attribute        | Description   |
|--------|-----------------------|---|
| 49     | Acct-Terminate-Cause  | <p>(Accounting) Reports details on why the connection was terminated. Termination causes are indicated by a numeric value as follows:</p> <ol style="list-style-type: none"> <li>1 User request</li> <li>2 Lost carrier</li> <li>3 Lost service</li> <li>4 Idle timeout</li> <li>5 Session timeout</li> <li>6 Admin reset</li> <li>7 Admin reboot</li> <li>8 Port error</li> <li>9 NAS error</li> <li>10 NAS request</li> <li>11 NAS reboot</li> <li>12 Port unneeded</li> <li>13 Port pre-empted</li> <li>14 Port suspended</li> <li>15 Service unavailable</li> <li>16 Callback</li> <li>17 User error</li> <li>18 Host request</li> </ol> <p><b>Note</b> For attribute 49, Cisco IOS XE supports values 1 to 6, 9, 12, and 15 to 18.</p> |
| 50     | Acct-Multi-Session-Id | <p>(Accounting) A unique accounting identifier used to link multiple related sessions in a log file.</p> <p>Each linked session in a multilink session has a unique Acct-Session-Id value, but shares the same Acct-Multi-Session-Id.</p>   |
| 51     | Acct-Link-Count       | <p>(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.</p>  |
| 52     | Acct-Input-Gigawords  | <p>Indicates how many times the Acct-Input-Octets counter has wrapped around <math>2^{32}</math> over the course of the provided service.</p>   |



| Number | IETF Attribute        | Description  |
|--------|-----------------------|--|
| 53     | Acct-Output-Gigawords | Indicates how many times the Acct-Output-Octets counter has wrapped around 2 <sup>32</sup> while delivering service.   |
| 55     | Event-Timestamp       | <p>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 <b>radius-server attribute 55 include-in-acct-req</b> command.</p> <p><b>Note</b> Before the Event-Timestamp attribute can be sent in accounting packets, you <i>must</i> configure the clock on the router. (For information on setting the clock on your router, refer to section “Performing Basic System Management” in the chapter “System Management” of the <i>Cisco IOS XE Configuration Fundamentals Configuration Guide</i>, Release 2.) To avoid configuring the clock on the router every time the router is reloaded, you can enable the <b>clock calendar-valid</b> command. (For information on this command, refer to the chapter “Basic System Management Commands” in the <i>Cisco IOS Configuration Fundamentals Command Reference</i> .</p> |
| 60     | CHAP-Challenge        | Contains the Challenge Handshake Authentication Protocol challenge sent by the network access server to a PPP CHAP user.   |

| Number | IETF Attribute           | Description  |
|--------|--------------------------|--|
| 61     | NAS-Port-Type            | <p>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:</p> <ul style="list-style-type: none"> <li>• 0: Asynchronous</li> <li>• 1: Synchronous</li> <li>• 2: ISDN-Synchronous</li> <li>• 3: ISDN-Asynchronous (V.120)</li> <li>• 4: ISDN-Asynchronous (V.110)</li> <li>• 5: Virtual</li> </ul> |
| 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 <sup>3</sup> | Indicates the tunneling protocol(s) used. Cisco IOS XE software supports one possible values for this attribute: L2TP.   |
| 65     | Tunnel-Medium-Type1      | Indicates the transport medium type to use 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.   |

<sup>3</sup> 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 .

| Number | IETF Attribute          | Description   |
|--------|-------------------------|---|
| 66     | Tunnel-Client-Endpoint  | <p>Contains the address of the initiator end of the tunnel. It <i>may</i> 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; the server is not obligated to honor the hint, however. This attribute <i>should</i> 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 means to identify a tunnel for accounting and auditing purposes.</p> <p>An enhancement has been added for the network access server to accept a value of 127.0.0.X for this attribute such that:</p> <p>127.0.0.0 would indicate that loopback0 IP address is to be used 127.0.0.1 would indicate that loopback1 IP address is to be used ... 127.0.0.X would indicate that loopbackX IP address is to be used for the actual tunnel client endpoint IP address. This enhancement adds scalability across multiple network access servers.</p> |
| 67     | Tunnel-Server-Endpoint1 | <p>Indicates the address of the server end of the tunnel. The format of this attribute varies depending on the value of Tunnel-Medium-Type. Because this release only supports IP as a tunnel medium type, the IP address or the host name of LNS is valid for this attribute.</p>  |

| Number | IETF Attribute            | Description  |
|--------|---------------------------|--|
| 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 means to uniquely identify a tunnel session for auditing purposes.   |
| 69     | Tunnel-Password1          | <p>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).</p> <p>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 <b>radius-server attribute 69 clear</b> global configuration command.</p> |
| 70     | ARAP-Password             | Identifies an Access-Request packet containing a Framed-Protocol of 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.  |
| 74     | ARAP-Security-Data        | Contains the actual security module challenge or response. It can be found in Access-Challenge and Access-Request packets.   |
| 75     | Password-Retry            | Indicates how many times a user may attempt authentication before being disconnected.  |

| Number | IETF Attribute          | Description   |
|--------|-------------------------|---|
| 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 a 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 via 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.   |
| 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.  |

| Number | IETF Attribute           | Description   |
|--------|--------------------------|---|
| 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     | <p>Determines how RADIUS treats passwords received from login-users when their file entry specifies a hand-held security card server.</p> <p>The value for this attribute is indicated by a numeric value as follows:</p> <ul style="list-style-type: none"> <li>• 0: No, meaning that the password is ignored.</li> <li>• 1: Yes, meaning that the password is used for authentication.</li> </ul> |

## Additional References

### Related Documents

| Related Topic                                 | Document Title                      |
|---|-------------------------------------|
| RADIUS IETF and vendor-proprietary attributes | Cisco AAA Implementation Case Study |

| Related Topic   | Document Title  |
|---|---|
| RADIUS with AAA   | The following chapters in the <i>Cisco IOS XE Security Configuration Guide: Securing User Services</i> , Release 2: <ul style="list-style-type: none"> <li>• “Configuring RADIUS ”</li> <li>• “Configuring Authentication ”</li> <li>• “Configuring Authorization ”</li> <li>• “Configuring Accounting ”</li> </ul> |
| RADIUS attribute implementation   | RADIUS Vendor-Specific Attributes Voice Implementation Guide  |
| <b>Standards</b>  |   |
| Standard  | Title   |
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | --  |
| <b>MIBs</b>   |   |
| 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:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>  |
| <b>RFCs</b>   |   |
| RFC   | Title   |
| RFC 2865  | <a href="#">Remote Authentication Dial In User Service (RADIUS)</a>   |
| RFC 2866  | <a href="#">RADIUS Accounting</a>   |
| RFC 2867  | <a href="#">RADIUS Accounting Modifications for Tunnel Protocol Support</a>   |
| RFC 2868  | <a href="#">RADIUS Attributes for Tunnel Protocol Support</a>   |
| RFC 2869  | <a href="#">RADIUS Extensions</a>   |

### Technical Assistance

| Description   | Link   |
|---|--|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

## 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](http://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 Attribute 8 (Framed-IP-Address) in Access Requests<br>(also called Sticky IP) | Cisco IOS XE Release 2.1 | <p>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.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified: <b>radius-server attribute 8 include-in-access-req</b>.</p> <p>For more details on this feature, see also “RADIUS Attribute 8 Framed-IP-Address in Access Requests” .</p> |
| RADIUS Attribute 44 (Accounting Session ID) in Access Requests                       | Cisco IOS XE Release 2.1 | <p>A unique accounting identifier that makes it easy to match start and stop records in a log file.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified: <b>radius-server attribute 44 include-in-access-req</b>.</p>   |

| Feature Name                                | Releases                 | Feature Information  |
|---|--------------------------|--|
| RADIUS Attribute 52 and 53 Gigaword Support | Cisco IOS XE Release 2.1 | <p>The RADIUS Attribute 52 and Attribute 53 Gigaword Support feature introduces support for Attribute 52 (Acct-Input-Gigawords) and Attribute 53 (Acct-Output-Gigawords) in accordance with RFC 2869. Attribute 52 keeps track of the number of times the Acct-Input-Octets counter has rolled over the 32-bit integer throughout the course of the provided service; attribute 53 keeps track of the number of times the Acct-Output-Octets counter has rolled over the 32-bit integer throughout the delivery of service. Both attributes can be present only in Accounting-Request records where the Acct-Status-Type is set to “Stop” or “Interim-Update.” These attributes can be used to keep accurate track of and bill for usage.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> |

| Feature Name  | Releases                 | Feature Information   |
|---|--------------------------|---|
| RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements | Cisco IOS XE Release 2.3 | <p>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.</p> <p>In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>For more details on this feature, see also “RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements” .</p>  |
| RADIUS Attribute 77 for DSL                               | Cisco IOS XE Release 2.1 | <p>The RADIUS Attribute 77 for DSL feature introduces support for attribute 77 (Connect-Info) to carry the textual name of the virtual circuit class associated with the given permanent virtual circuit (PVC). (Although attribute 77 does not carry the unspecified bit rate (UBR), the UBR can be inferred from the classname used if one UBR is set up on each class.) Attribute 77 is sent from the network access server (NAS) to the RADIUS server via Accounting-Request and Accounting-Response packets.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>For more details on this feature, see also “Connect-Info RADIUS Attribute 77” .</p> |

| Feature Name   | Releases                 | Feature Information  |
|--|--------------------------|--|
| RADIUS Attribute 82: Tunnel Assignment Id            | Cisco IOS XE Release 2.1 | <p>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.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>For more details on this feature, see also “RADIUS Attribute 82: Tunnel Assignment ID” .</p> |
| RADIUS Attribute 91 Encrypted and Tagged VSA Support | Cisco IOS XE Release 2.1 | <p>The RADIUS attribute 91 feature allows you to specify a name (other than the default) of the tunnel terminator. By allowing the user to specify authentication names for the RADIUS server, attribute 91 supports the provision of compulsory tunneling in virtual private networks (VPNs). Also by specifying a name, you can establish a higher level of security when setting up VPN tunneling.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p>   |

| Feature Name                       | Releases                 | Feature Information   |
|------------------------------------|--------------------------|---|
| RADIUS Tunnel Attribute Extensions | Cisco IOS XE Release 2.1 | <p>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.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>For more details on this feature, see also “RADIUS Tunnel Attribute Extensions” .</p> |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.





## 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 XE support information for these vendor-proprietary RADIUS attributes.

- [Finding Feature Information, page 33](#)
- [Supported Vendor-Proprietary RADIUS Attributes, page 33](#)
- [Comprehensive List of Vendor-Proprietary RADIUS Attribute Descriptions, page 39](#)
- [Feature Information for RADIUS Vendor-Proprietary Attributes, page 50](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

### Supported Vendor-Proprietary RADIUS Attributes

The table below lists Cisco-supported vendor-proprietary RADIUS attributes and the Cisco IOS XE release in which they are implemented. In cases where the attribute has a security server-specific format, the format is specified. Refer to Refer to Vendor-Proprietary RADIUS Attributes table for a list of descriptions.

**Table 4**      **Supported Vendor-Proprietary RADIUS Attributes**

| Number | Vendor-Proprietary Attribute | IOS XE 2.1 |
|--------|------------------------------|------------|
| 17     | Change-Password              | yes        |
| 21     | Password-Expiration          | yes        |
| 68     | Tunnel-ID                    | yes        |
| 108    | My-Endpoint-Disc-Alias       | no         |

| <b>Number</b> | <b>Vendor-Proprietary Attribute</b> | <b>IOS XE 2.1</b> |
|---------------|-------------------------------------|-------------------|
| 109           | My-Name-Alias                       | no                |
| 110           | Remote-FW                           | no                |
| 111           | Multicast-GLeave-Delay              | no                |
| 112           | CBCP-Enable                         | no                |
| 113           | CBCP-Mode                           | no                |
| 114           | CBCP-Delay                          | no                |
| 115           | CBCP-Trunk-Group                    | no                |
| 116           | Appletalk-Route                     | no                |
| 117           | Appletalk-Peer-Mode                 | no                |
| 118           | Route-Appletalk                     | no                |
| 119           | FCP-Parameter                       | no                |
| 120           | Modem-PortNo                        | no                |
| 121           | Modem-SlotNo                        | no                |
| 122           | Modem-ShelfNo                       | no                |
| 123           | Call-Attempt-Limit                  | no                |
| 124           | Call-Block-Duration                 | no                |
| 125           | Maximum-Call-Duration               | no                |
| 126           | Router-Preference                   | no                |
| 127           | Tunneling-Protocol                  | no                |
| 128           | Shared-Profile-Enable               | no                |
| 129           | Primary-Home-Agent                  | no                |
| 130           | Secondary-Home-Agent                | no                |
| 131           | Dialout-Allowed                     | no                |
| 133           | BACP-Enable                         | no                |
| 134           | DHCP-Maximum-Leases                 | no                |
| 135           | Primary-DNS-Server                  | yes               |
| 136           | Secondary-DNS-Server                | yes               |
| 137           | Ascend-Client-Assign-DNS            | no                |



| Number | Vendor-Proprietary Attribute | IOS XE 2.1 |
|--------|------------------------------|------------|
| 138    | User-Acct-Type               | no         |
| 139    | User-Acct-Host               | no         |
| 140    | User-Acct-Port               | no         |
| 141    | User-Acct-Key                | no         |
| 142    | User-Acct-Base               | no         |
| 143    | User-Acct-Time               | no         |
| 144    | Assign-IP-Client             | no         |
| 145    | Assign-IP-Server             | no         |
| 146    | Assign-IP-Global-Pool        | no         |
| 147    | DHCP-Reply                   | no         |
| 148    | DHCP-Pool-Number             | no         |
| 149    | Expect-Callback              | no         |
| 150    | Event-Type                   | no         |
| 151    | Ascend-Session-Svr-Key       | yes        |
| 152    | Ascend-Multicast-Rate-Limit  | yes        |
| 153    | IF-Netmask                   | no         |
| 154    | h323-Remote-Address          | no         |
| 155    | Ascend-Multicast-Client      | yes        |
| 156    | FR-Circuit-Name              | no         |
| 157    | FR-LinkUp                    | no         |
| 158    | FR-Nailed-Grp                | no         |
| 159    | FR-Type                      | no         |
| 160    | FR-Link-Mgt                  | no         |
| 161    | FR-N391                      | no         |
| 162    | FR-DCE-N392                  | no         |
| 163    | FR-DTE-N392                  | no         |
| 164    | FR-DCE-N393                  | no         |
| 165    | FR-DTE-N393                  | no         |

| Number | Vendor-Proprietary Attribute | IOS XE 2.1 |
|--------|------------------------------|------------|
| 166    | FR-T391                      | no         |
| 167    | FR-T392                      | no         |
| 168    | Bridge-Address               | no         |
| 169    | TS-Idle-Limit                | no         |
| 170    | TS-Idle-Mode                 | no         |
| 171    | DBA-Monitor                  | no         |
| 172    | Base-Channel-Count           | no         |
| 173    | Minimum-Channels             | no         |
| 174    | IPX-Route                    | no         |
| 175    | FT1-Caller                   | no         |
| 176    | Ipssec-Backup-Gateway        | yes        |
| 177    | rm-Call-Type                 | yes        |
| 178    | Group                        | no         |
| 179    | FR-DLCI                      | no         |
| 180    | FR-Profile-Name              | no         |
| 181    | Ara-PW                       | no         |
| 182    | IPX-Node-Addr                | no         |
| 183    | Home-Agent-IP-Addr           | no         |
| 184    | Home-Agent-Password          | no         |
| 185    | Home-Network-Name            | no         |
| 186    | Home-Agent-UDP-Port          | no         |
| 187    | Multilink-ID                 | yes        |
| 188    | Ascend-Num-In-Multilink      | yes        |
| 189    | First-Dest                   | no         |
| 190    | Pre-Bytes-In                 | yes        |
| 191    | Pre-Bytes-Out                | yes        |
| 192    | Pre-Paks-In                  | yes        |
| 193    | Pre-Paks-Out                 | yes        |

| Number | Vendor-Proprietary Attribute | IOS XE 2.1 |
|--------|------------------------------|------------|
| 194    | Maximum-Time                 | yes        |
| 195    | Disconnect-Cause             | yes        |
| 196    | Connect-Progress             | yes        |
| 197    | Data-Rate                    | yes        |
| 198    | PreSession-Time              | yes        |
| 199    | Token-Idle                   | no         |
| 201    | Require-Auth                 | no         |
| 202    | Number-Sessions              | no         |
| 203    | Authen-Alias                 | no         |
| 204    | Token-Expiry                 | no         |
| 205    | Menu-Selector                | no         |
| 206    | Menu-Item                    | no         |
| 207    | PW-Warntime                  | no         |
| 208    | PW-Lifetime                  | yes        |
| 209    | IP-Direct                    | yes        |
| 210    | PPP-VJ-Slot-Compression      | yes        |
| 211    | PPP-VJ-1172                  | no         |
| 212    | PPP-Async-Map                | no         |
| 213    | Third-Prompt                 | no         |
| 214    | Send-Secret                  | yes        |
| 215    | Receive-Secret               | no         |
| 216    | IPX-Peer-Mode                | no         |
| 217    | IP-Pool                      | yes        |
| 218    | Static-Addr-Pool             | yes        |
| 219    | FR-Direct                    | no         |
| 220    | FR-Direct-Profile            | no         |
| 221    | FR-Direct-DLCI               | no         |
| 222    | Handle-IPX                   | no         |

| Number | Vendor-Proprietary Attribute | IOS XE 2.1 |
|--------|------------------------------|------------|
| 223    | Netware-Timeout              | no         |
| 224    | IPX-Alias                    | no         |
| 225    | Metric                       | no         |
| 226    | PRI-Number-Type              | no         |
| 227    | Dial-Number                  | yes        |
| 228    | Route-IP                     | yes        |
| 229    | Route-IPX                    | no         |
| 230    | Bridge                       | no         |
| 231    | Send-Auth                    | yes        |
| 232    | Send-Passwd                  | no         |
| 233    | Link-Compression             | yes        |
| 234    | Target-Util                  | yes        |
| 235    | Maximum-Channels             | yes        |
| 236    | Inc-Channel-Count            | no         |
| 237    | Dec-Channel-Count            | no         |
| 238    | Seconds-of-History           | no         |
| 239    | History-Weigh-Type           | no         |
| 240    | Add-Seconds                  | no         |
| 241    | Remove-Seconds               | no         |
| 242    | Data-Filter                  | yes        |
| 243    | Call-Filter                  | no         |
| 244    | Idle-Limit                   | yes        |
| 245    | Preempt-Limit                | no         |
| 246    | Callback                     | no         |
| 247    | Data-Service                 | yes        |
| 248    | Force-56                     | yes        |
| 249    | Billing Number               | no         |
| 250    | Call-By-Call                 | no         |

| Number | Vendor-Proprietary Attribute | IOS XE 2.1 |
|--------|------------------------------|------------|
| 251    | Transit-Number               | no         |
| 252    | Host-Info                    | no         |
| 253    | PPP-Address                  | no         |
| 254    | MPP-Idle-Percent             | no         |
| 255    | Xmit-Rate                    | yes        |

## Comprehensive List of Vendor-Proprietary RADIUS Attribute Descriptions

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

**Table 5** Vendor-Proprietary RADIUS Attributes

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

| <b>Number</b> | <b>Vendor-Proprietary Attribute</b> | <b>Description</b>                   |
|---------------|-------------------------------------|--------------------------------------|
| 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. |
| 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. |

| Number | Vendor-Proprietary Attribute | Description  |
|--------|------------------------------|--|
| 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.   |
| 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.  |

| Number | Vendor-Proprietary Attribute | Description               |
|--------|------------------------------|---------------------------|
| 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. |
| 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. |



| Number | Vendor-Proprietary Attribute | Description   |
|--------|------------------------------|---|
| 182    | IPX-Node-Addr                | No description available.   |
| 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-Bytes-In                 | Records the number of input bytes before authentication. The Pre-Bytes-In attribute is sent in accounting-stop records.   |

| Number | Vendor-Proprietary Attribute | Description  |
|--------|------------------------------|--|
| 191    | Pre-Bytes-Out                | Records the number of output bytes before authentication. The Pre-Bytes-Out attribute is sent in accounting-stop records.  |
| 192    | Pre-Paks-In                  | Records the number of input packets before authentication. The Pre-Paks-In attribute is sent in accounting-stop records.   |
| 193    | Pre-Paks-Out                 | Records the number of output packets before authentication. The Pre-Paks-Out 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. See the Vendor-Specific Attributes (VSA) and RADIUS Disconnect-Cause Attribute Values for more information on 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.   |

| <b>Number</b> | <b>Vendor-Proprietary Attribute</b> | <b>Description</b>   |
|---------------|-------------------------------------|--|
| 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                    | <p>When you include this attribute in a user's file entry, a framed route is installed to the routing and bridging tables.</p> <p><b>Note</b> 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.</p> |
| 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.   |
| 229    | Route-IPX                    | Allows you to enable IPX routing.  |

| Number | Vendor-Proprietary Attribute | Description   |
|--------|------------------------------|---|
| 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             | <p>Defines whether to turn on or turn off “stac” compression over a PPP link.</p> <p>Link compression is defined as a numeric value as follows:</p> <ul style="list-style-type: none"> <li>• 0: None</li> <li>• 1: Stac</li> <li>• 2: Stac-Draft-9</li> <li>• 3: MS-Stac</li> </ul> |
| 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.  |

See the Configuring RADIUS feature module for more information on vendor-proprietary RADIUS attributes.

## 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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 6** Feature Information for RADIUS Vendor-Proprietary Attributes

| Feature Name                         | Releases                 | Feature Information   |
|--------------------------------------|--------------------------|---|
| RADIUS Vendor-Proprietary Attributes | Cisco IOS XE Release 2.1 | <p>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 XE support information for these vendor-proprietary RADIUS attributes.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.





# 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, thereby, allowing vendors to support their own extended attributes otherwise not suitable for general use.

- [Finding Feature Information, page 51](#)
- [Information About RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values, page 51](#)
- [RADIUS Disconnect-Cause Attribute Values, page 59](#)
- [Additional References, page 61](#)
- [Feature Information for RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values, page 63](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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](http://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:

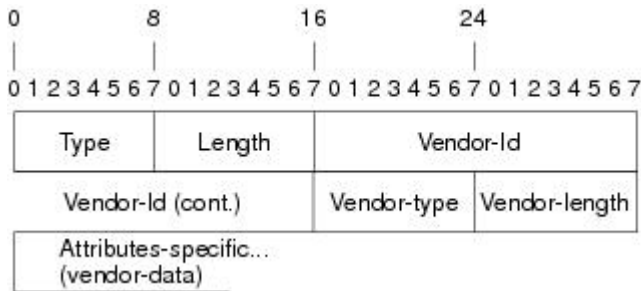
```
cisco-avpair= "shell:priv-lvl=15"
```

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 7** 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 8** Vendor-Specific RADIUS IETF Attributes

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

| Number | Vendor-Specific Company Code | Sub-Type Number | Attribute                 | Description  |
|--------|------------------------------|-----------------|---------------------------|--|
| 26     | 9                            | 1               | l2tp-busy-disconnect      | If a vpdn-group on an LNS uses a virtual-template that is configured to be pre-cloned, this attribute will control the disposition of a new L2TP session that finds no pre-cloned interface to which to connect. If the attribute is true (the default), the session will be disconnected by the LNS. Otherwise, a new interface will be cloned from the virtual-template. |
| 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.   |
| 26     | 9                            | 1               | l2tp-hidden-avp           | When enabled, sensitive AVPs in L2TP control messages are scrambled or hidden.   |

| Number                 | Vendor-Specific Company Code | Sub-Type Number | Attribute                                  | Description  |
|------------------------|------------------------------|-----------------|--|--|
| 26                     | 9                            | 1               | l2tp-nosession-timeout                     | Specifies the number of seconds that a tunnel will stay active with no sessions before timing out and shutting down.   |
| 26                     | 9                            | 1               | tunnel-tos-reflect                         | Copies the IP ToS field from the IP header of each payload packet to the IP header of the tunnel packet for packets entering the tunnel at the LNS.            |
| 26                     | 9                            | 1               | l2tp-tunnel-authen                         | If this attribute is set, it performs L2TP tunnel authentication.  |
| 26                     | 9                            | 1               | l2tp-tunnel-password                       | 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. |
| <b>H323 Attributes</b> |                              |                 |  |  |
| 26                     | 9                            | 23              | Remote-Gateway-ID<br>(h323-remote-address) | Indicates the IP address of the remote gateway.  |
| 26                     | 9                            | 24              | Connection-ID<br>(h323-conf-id)            | Identifies the conference ID.  |
| 26                     | 9                            | 25              | Setup-Time<br>(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.                    |

| Number                         | Vendor-Specific Company Code | Sub-Type Number | Attribute                                   | Description  |
|--------------------------------|------------------------------|-----------------|---|--|
| 26                             | 9                            | 26              | Call-Origin<br>(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<br>(h323-call-type)               | Indicates call leg type. Possible values are <b>telephony</b> and <b>VoIP</b> .  |
| 26                             | 9                            | 28              | Connect-Time<br>(h323-connect-time)         | Indicates the connection time for this call leg in UTC.  |
| 26                             | 9                            | 29              | Disconnect-Time<br>(h323-disconnect-time)   | Indicates the time this call leg was disconnected in UTC.  |
| 26                             | 9                            | 30              | Disconnect-Cause<br>(h323-disconnect-cause) | Specifies the reason a connection was taken offline per Q.931 specification.   |
| 26                             | 9                            | 31              | Voice-Quality<br>(h323-voice-quality)       | Specifies the impairment factor (ICPIF) affecting voice quality for a call.  |
| 26                             | 9                            | 33              | Gateway-ID<br>(h323-gw-id)                  | Indicates the name of the underlying gateway.  |
| Large Scale Dialout Attributes |                              |                 |   |  |
| 26                             | 9                            | 1               | callback-dialstring                         | Defines a dialing string to be used for callback.  |
| 26                             | 9                            | 1               | data-service                                | No description available.  |
| 26                             | 9                            | 1               | dial-number                                 | Defines the number to dial.  |
| 26                             | 9                            | 1               | force-56                                    | Determines whether the network access server uses only the 56 K portion of a channel, even when all 64 K appear to be available. |

| Number                   | Vendor-Specific Company Code | Sub-Type Number | Attribute      | Description   |
|--------------------------|------------------------------|-----------------|----------------|---|
| 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.   |
| Miscellaneous Attributes |                              |                 |                |   |
| 26                       | 9                            | 2               | Cisco-NAS-Port | <p>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.</p> <p><b>Note</b> This VSA is typically used in Accounting, but may also be used in Authentication (Access-Request) packets.</p> |
| 26                       | 9                            | 1               | min-links      | Sets the minimum number of links for MLP.   |

| Number | Vendor-Specific Company Code | Sub-Type Number | Attribute          | Description   |
|--------|------------------------------|-----------------|--------------------|---|
| 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.  |
| 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 <b>ip mobile secure host &lt;addr&gt;</b> 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. |
| 26     | 9                            | 1               | client-mac-address | Contains the MAC address of the PPPoE client.<br><br><b>Note</b> This attribute is applicable only to PPP over Ethernet (PPPoE) or to PPP over ATM (PPPoA).   |

See “Configuring Router to Use Vendor-Specific RADIUS Attributes” section of the Configuring RADIUS feature module for more information on configuring your NAS to recognize and use VSAs.



## 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, disconnect cause 4 becomes 1004.

**Table 9**      *Disconnect-Cause Attribute Values*

| Cause Code | Value                       | Description   |
|------------|-----------------------------|---|
| 2          | Unknown                     | Reason unknown.   |
| 4          | CLID-Authentication-Failure | Failure to authenticate number of the calling-party.  |
| 10         | No-Carrier                  | No carrier detected.<br><b>Note</b> 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.<br><b>Note</b> Codes 20, 22, 23, 24, 25, 26, 27, and 28 apply to EXEC sessions.                        |
| 21         | Idle-Timeout                | Timeout waiting for user input.<br>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.   |

| Cause Code | Value                      | Description  |
|------------|----------------------------|--|
| 27         | Control-C-Detected         | Control-C detected.  |
| 28         | EXEC-Process-Destroyed     | EXEC process destroyed.  |
| 40         | Timeout-PPP-LCP            | PPP LCP negotiation timed out.<br><b>Note</b> Codes 40, 41, 42, 43, 44, 45, and 46 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.  |
| 63         | PPP-Echo-Replies           | TCP connection has been closed.  |
| 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.  |
| 600        | VPN-User-Disconnect        | Call disconnected by client (through PPP).<br>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.<br>Code is sent when a client is unable to dial out using a dialer. |
| 602        | VPN-No-Resources           | No resources available to handle the call.<br>Code is sent when the client is unable to allocate memory (running low on memory).           |

| Cause Code | Value                  | Description  |
|------------|------------------------|--|
| 603        | VPN-Bad-Control-Packet | <p>Bad L2TP or L2F control packets.</p> <p>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.</p> <p><b>Note</b> VPN-Tunnel-Shut will be sent if there are active sessions in the tunnel.</p> |
| 604        | VPN-Admin-Disconnect   | <p>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.</p> <p>Code is sent when a tunnel is brought down by issuing the <b>clear vpdn tunnel</b> command.</p>  |
| 605        | VPN-Tunnel-Shut        | <p>Tunnel teardown or tunnel setup has failed.</p> <p>Code is sent when there are active sessions in a tunnel and the tunnel goes down.</p> <p><b>Note</b> This code is not sent when tunnel authentication fails.</p>   |
| 606        | VPN-Local-Disconnect   | <p>Call is disconnected by LNS PPP module.</p> <p>Code is sent when the LNS sends a PPP terminate request to the client. It indicates a normal PPP disconnection initiated by the LNS.</p>   |
| 607        | VPN-Session-Limit      | <p>VPN soft shutdown is enabled.</p> <p>Code is sent when a call has been refused due to any of the soft shutdown restrictions previously mentioned.</p>   |
| 611        | VPDN-Tunnel-In-Resync  | VPDN tunnel is in HA resync.   |

## 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        | <a href="#">Cisco IOS Master Commands List, All Releases</a>  |
| Security commands         | <i>Cisco IOS Security Command Reference</i>   |
| Security Features         | <i>Cisco IOS XE Security Configuration Guide: Securing User Services</i> , Release 2  |
| Security Server Protocols | Security Server Protocols section of the <i>Cisco IOS XE Security Configuration Guide: Securing User Services</i> , Release 2 |
| RADIUS Configuration      | Configuring RADIUS feature module.  |

### Standards

| Standard   | Title  |
|--|--|
| Internet Engineering Task Force (IETF) Internet Draft: Network Access Servers Requirements | <a href="#">Network Access Servers Requirements: Extended RADIUS Practices</a> |

### 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:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFC      | Title   |
|----------|---|
| RFC 2865 | <a href="#">Remote Authentication Dial In User Service (RADIUS)</a> |

### Technical Assistance

| Description   | Link   |
|---|--|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p> |

## 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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 10**      *Feature Information for RADIUS Vendor-Specific Attributes (VSA) and RADIUS Disconnect-Cause Attribute Values*

| Feature Name                        | Releases                 | Feature Information   |
|-------------------------------------|--------------------------|---|
| Accounting of VPDN Disconnect Cause | Cisco IOS XE Release 2.1 | This feature was introduced on Cisco ASR 1000 Series Routers. |

| Feature Name                      | Releases                 | Feature Information   |
|-----------------------------------|--------------------------|---|
| Vendor-Specific RADIUS Attributes | Cisco IOS XE Release 2.1 | <p>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.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.



## 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, page 65](#)
- [Prerequisites for Connect-Info RADIUS Attribute 77, page 66](#)
- [Information About Connect-Info RADIUS Attribute 77, page 66](#)
- [How to Verify the Connect-Info RADIUS Attribute 77, page 67](#)
- [Additional References, page 69](#)
- [Feature Information for Connect-Info RADIUS Attribute 77, page 70](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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](http://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](#), page 70.

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](#), page 66
- [Customizing Attribute 77 for ATM Connections](#), page 66

## 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, page 67](#)

### 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 | <b>enable</b>     | Enables privileged EXEC mode.  |
|        | <b>Example:</b>   |  |
|        | Router> enable    | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |

| Command or Action    | Purpose                                      |
|----------------------|--|
| Step 2               | debug radius                                 |
| Example:             | Displays information associated with RADIUS. |
| Router# debug 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'

```

## 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<br><i>Cisco IOS Dial Technologies Command Reference</i> |
| Security commands     | <i>Cisco IOS Security Command Reference</i>   |

### 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFC      | Title                             |
|----------|-----------------------------------|
| RFC 2869 | <a href="#">RADIUS Extensions</a> |

**Technical Assistance**

| Description   | Link  |
|---|---|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## 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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 11**      **Feature Information for Connect-Info RADIUS Attribute 77**

| Feature Name                     | Releases                 | Feature Information  |
|----------------------------------|--------------------------|--|
| Connect-Info RADIUS Attribute 77 | Cisco IOS XE Release 2.1 | <p>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).</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 series routers.</p> |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.





## 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, page 74](#) (similar to Cisco VSA type 1 (Cisco:AVPair (1)) except that this new VSA is tagged)
- [Encrypted String VSA, page 74](#) (similar to Cisco VSA type 1 except that this new VSA is encrypted)
- [Tagged and Encrypted String VSA, page 75](#) (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, page 73](#)
- [Prerequisites for Encrypted Vendor-Specific Attributes, page 73](#)
- [Information About Encrypted Vendor-Specific Attributes, page 74](#)
- [How to Verify Encrypted Vendor-Specific Attributes, page 75](#)
- [Configuration Examples for Encrypted Vendor-Specific Attributes, page 75](#)
- [Additional References, page 76](#)
- [Feature Information for Encrypted Vendor-Specific Attributes, page 77](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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](http://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](#), page 73 for documents that explain how to perform these tasks.

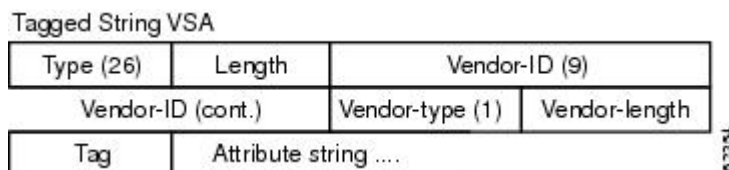
## Information About Encrypted Vendor-Specific Attributes

- [Tagged String VSA](#), page 74
- [Encrypted String VSA](#), page 74
- [Tagged and Encrypted String VSA](#), page 75

### Tagged String VSA

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

**Figure 3** Tagged String VSA Format

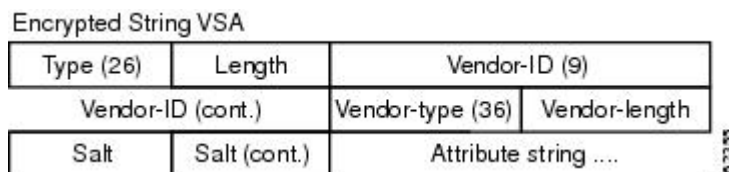


To retrieve the correct value, the Tag field must be parsed correctly. The value for this field can range only from 0x01 through 0x1F. If the value is not within the specified range, the RADIUS server ignores the value and considers the Tag field to be a part of the Attribute String field.

### Encrypted String VSA

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

**Figure 4** Encrypted String VSA Format



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# <b>debug radius</b> | 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, page 75](#)
- [RADIUS User Profile with a Tagged and Encrypted VSA Example, page 76](#)

### 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                      | <i>Cisco IOS Master Commands List, All Releases</i>                                  |
| RADIUS Attributes                       | <i>Cisco IOS XE Security Configuration Guide: Securing User Services</i> , 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:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

**RFCs**

| <b>RFC</b> | <b>Title</b>   |
|------------|--|
| RFC 2865   | <i>Remote Authentication Dial In User Service (RADIUS)</i> |
| RFC 2868   | <i>RADIUS Attributes for Tunnel Protocol Support</i>       |

**Technical Assistance**

| <b>Description</b>  | <b>Link</b>  |
|---|--|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p> |

## 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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 12**      **Feature Information for Encrypted Vendor-Specific Attributes**

| Feature Name                         | Releases                 | Feature Information  |
|--------------------------------------|--------------------------|--|
| Encrypted Vendor-Specific Attributes | Cisco IOS XE Release 2.3 | <p>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).</p> <p>In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.



## 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 addresses. Using the mapping information, service applications can begin preparing user login information to have available upon successful user authentication.

- [Finding Feature Information, page 79](#)
- [Prerequisites for RADIUS Attribute 8 Framed-IP-Address in Access Requests, page 79](#)
- [Information About RADIUS Attribute 8 Framed-IP-Address in Access Requests, page 80](#)
- [How to Configure RADIUS Attribute 8 Framed-IP-Address in Access Requests, page 80](#)
- [Configuration Examples for RADIUS Attribute 8 Framed-IP-Address in Access Requests, page 82](#)
- [Additional References, page 83](#)
- [Feature Information for RADIUS Attribute 8 Framed-IP-Address in Access Requests, page 84](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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](http://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

- [How This Feature Works, page 80](#)
- [Benefits, page 80](#)

## How This Feature Works

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.

## Benefits

The RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature makes it possible to run applications on the RADIUS server that builds mapping tables of users and IP addresses. The server can then use the mapping table information in other applications, such as preparing customized user login pages in advance of a successful user authentication with the RADIUS server.

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

- [Configuring RADIUS Attribute 8 in Access Requests, page 81](#)
- [Verifying RADIUS Attribute 8 in Access Requests, page 81](#)

## 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  |
|--|--|
| <b>Step 1</b> <b>enable</b><br><br><b>Example:</b><br>Router> enable   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| <b>Step 2</b> <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal   | Enters global configuration mode.  |
| <b>Step 3</b> <b>radius-server attribute 8 include-in-access-req</b><br><br><b>Example:</b><br>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 | <b>enable</b><br><br><b>Example:</b><br>Router> enable   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>  |
| Step 2 | <b>more system:running-config</b><br><br><b>Example:</b><br>Router# more system:running-config | Displays the contents of the current running configuration file. (Note that the <b>more system:running-config</b> command has replaced the <b>show running-config</b> command.) |
| Step 3 | <b>debug radius</b><br><br><b>Example:</b><br>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 Example, page 82](#)

### NAS Configuration That Sends the IP Address of the Dial-in Host Example

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 virtual-template1.

```

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 virtual-template1
 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 in the <i>Cisco IOS XE Security Configuration Guide: Configuring User Services</i> , Release 2. |
| Security commands                                 | <i>Cisco IOS Security Command Reference</i>  |

### 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFC      | Title   |
|----------|---|
| RFC 2138 | <a href="#">Remote Authentication Dial In User Service (RADIUS)</a> |

**Technical Assistance**

| Description   | Link  |
|---|---|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## 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](http://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<br>(Also called Sticky IP) | Cisco IOS XE Release 2.1 | <p>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.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified: <b>radius-server attribute 8 include-in-access-req.</b></p> |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.





## RADIUS Attribute 82 Tunnel Assignment ID

---

- [Finding Feature Information, page 87](#)
- [Restrictions for Radius Attribute 82 Tunnel Assignment ID, page 87](#)
- [Information about RADIUS Attribute 82 Tunnel Assignment ID, page 87](#)
- [How to Configure RADIUS Attribute 82 Tunnel Assignment ID, page 88](#)
- [Configuration Examples for RADIUS Attribute 82 Tunnel Assignment ID, page 88](#)
- [Additional References, page 90](#)
- [Feature Information for RADIUS Attribute 82 Tunnel Assignment ID, page 91](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

### 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.

- [Benefits, page 87](#)

### Benefits

The RADIUS Attribute 82: Tunnel Assignment ID feature improves LAC and L2TP network server (LNS) performance by reducing memory usage, because fewer tunnel data structures must be maintained. This

feature allows the LAC and LNS to handle a higher volume of users without negatively impacting router performance.

## How to Configure RADIUS Attribute 82 Tunnel Assignment ID

There are not any specific configuration tasks associated with support of this feature.

- [Verifying RADIUS Attribute 82, page 88](#)

### Verifying RADIUS Attribute 82

To verify that RADIUS attribute 82 is being used by the LAC during tunnel authorization, use the following privileged EXEC command:

| Command                     | Purpose  |
|-----------------------------|--|
| Router# <b>debug radius</b> | 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, page 88](#)
- [LNS Configuration Example, page 89](#)
- [RADIUS Configuration Example, page 89](#)

### 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 ispl.com
initiate-to ip 10.0.0.2
source-ip 10.0.0.1
l2tp tunnel receive-window 100
l2tp tunnel no-session-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 tunnell
!
!
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-Templatel
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 the Configuring RADIUS Attribute 82: Tunnel Assignment ID.

### Related Documents

| Related Topic                                 | Document Title   |
|---|--|
| Virtual template interfaces and dial features | <i>Cisco IOS XE Dial Technologies Configuration Guide</i> , Release 2  |
| Virtual private dialup networks (VPDNs)       | <i>Cisco IOS XE VPDN Configuration Guide</i> , Release 2   |
| RADIUS  | “Configuring RADIUS” in the <i>Cisco IOS XE Security Configuration Guide: Configuring User Services</i> , Release 2. |
| Security commands                             | <i>Cisco IOS Security Command Reference</i>  |

### 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:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

**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  |
|---|---|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## 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](http://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 | Cisco IOS XE Release 2.1 | <p>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.</p> <p>In Cisco IOS XE Release 2.1, support was added for the Cisco ASR 1000 Series Aggregation Services Routers.</p> |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.



# 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.

- [Finding Feature Information, page 93](#)
- [Prerequisites, page 93](#)
- [Restrictions, page 93](#)
- [Information About RADIUS Tunnel Attribute Extensions, page 94](#)
- [How to Configure RADIUS Tunnel Attribute Extensions, page 95](#)
- [Configuration Examples for RADIUS Tunnel Attribute Extensions, page 95](#)
- [Additional References, page 96](#)
- [Feature Information for RADIUS Tunnel Attribute Extensions, page 97](#)
- [Glossary, page 98](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

## Prerequisites

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

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

## Information About RADIUS Tunnel Attribute Extensions

- [RADIUS Tunnel Attribute Extension Benefits](#), page 94
- [RADIUS Tunnel Attribute Extension Description](#), page 94

### RADIUS Tunnel Attribute Extension Benefits

The RADIUS Tunnel Attribute Extensions feature allows you to specify a name (other than the default) of the tunnel initiator and the tunnel terminator. Thus, you can establish a higher level of security when setting up VPN tunneling.

### RADIUS Tunnel Attribute Extension Description

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 15** RADIUS Tunnel Attributes

| Number | IETF RADIUS Tunnel Attribute | Equivalent TACACS+ Attribute | Supported Protocols               | Description   |
|--------|------------------------------|------------------------------|-----------------------------------|---|
| 90     | Tunnel-Client-Auth-ID        | tunnel-id                    | Layer 2 Tunneling Protocol (L2TP) | Specifies the name used by the tunnel initiator (also known as the NAS <sup>4</sup> ) when authenticating tunnel setup with the tunnel terminator.          |
| 91     | Tunnel-Server-Auth-ID        | gw-name                      | Layer 2 Tunneling Protocol (L2TP) | Specifies the name used by the tunnel terminator (also known as the Home Gateway <sup>5</sup> ) when authenticating tunnel setup with the tunnel initiator. |

<sup>4</sup> When L2TP is used, the NAS is referred to as an L2TP access concentrator (LAC).

<sup>5</sup> 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 Configure RADIUS Tunnel Attribute Extensions

There are no configuration tasks associated with this feature.

- [Verifying RADIUS Attribute 90 and RADIUS Attribute 91, page 95](#)

## Verifying 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# <b>debug radius</b> | 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, page 95](#)
- [RADIUS User Profile with RADIUS Tunneling Attributes 90 and 91 Example, page 96](#)

### 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 l2tp-svr-auth-id password 0 l2tp-tnl-pass
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
```

```

terminate-from hostname l2tp-cli-auth-id
local name l2tp-svr-auth-id
!
interface loopback0
ip address 10.0.0.3 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface Virtual-Template1
ip unnumbered loopback0
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 for an L2TP tunnel.

```

cisco.com Password = "cisco", Service-Type = Outbound
Service-Type = Outbound,
Tunnel-Type = :1:L2TP,
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:"l2tp-cli-auth-id",
Tunnel-Server-Auth-Id = :1:"l2tp-svr-auth-id",
Tunnel-Assignment-Id = :1:"l2tp-assignment-id",
Cisco-Avpair = "vpdn:l2tp-tunnel-password=l2tp-tnl-pass",
Tunnel-Preference = :1:1

```

## Additional References

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

### Related Documents

| Related Topic                 | Document Title   |
|-------------------------------|--|
| Authentication configuration  | “Configuring Authentication” in the <i>Cisco IOS XE Security Configuration Guide: Configuring User Services</i> , Release 2                            |
| RADIUS configuration          | “Configuring RADIUS” in the <i>Cisco IOS XE Security Configuration Guide: Configuring User Services</i> , Release 2                                    |
| Overview of RADIUS attributes | “RADIUS Attributes Overview and RADIUS IETF Attributes” in the <i>Cisco IOS XE Security Configuration Guide: Configuring User Services</i> , Release 2 |
| Security commands             | <i>Cisco IOS Security Command Reference</i>  |

**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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

**RFCs**

| RFC      | Title  |
|----------|--|
| RFC 2868 | <i>RADIUS Attributes for Tunnel Protocol Support</i> |

**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.<br><br>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.<br><br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## 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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 16** Feature Information for RADIUS Tunnel Attribute Extensions

| Feature Name                       | Releases                 | Feature Information  |
|------------------------------------|--------------------------|--|
| RADIUS Tunnel Attribute Extensions | Cisco IOS XE Release 2.1 | <p>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.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> |

## Glossary

**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).



Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.





# 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, page 101](#)
- [Prerequisites for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements, page 101](#)
- [Restrictions for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements, page 102](#)
- [Information About RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements, page 102](#)
- [How to Configure RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements, page 102](#)
- [Configuration Examples for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements, page 102](#)
- [Additional References, page 103](#)
- [Feature Information for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements, page 104](#)
- [Glossary, page 105](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

## Prerequisites for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements

A Cisco IOS XE platform that supports VPDN is required. See the [Glossary, page 105](#) for more information about VPDN.

## Restrictions for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements

Your Cisco router must be running a Cisco IOS XE 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, page 102](#)

## 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 in the Cisco IOS XE software.

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

- [Setting Up the RADIUS Profile for RADIUS Attribute 66 Tunnel-Client-Endpoint Enhancements Example, page 103](#)

## 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 = tunnell
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 | <i>Cisco IOS XE Security Configuration Guide: Configuring User Services</i> , Release 2 |
| Security commands   | <i>Cisco IOS Security Command Reference</i>   |

### 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:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

**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  |
|---|---|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## 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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 17** Feature Information for RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements

| Feature Name  | Releases                 | Feature Information  |
|---|--------------------------|--|
| RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements | Cisco IOS XE Release 2.1 | <p>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.</p> <p>In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> |

## 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).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.





## RADIUS Attribute Value Screening

---

The RADIUS Attribute Value 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 Value 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, page 107](#)
- [Prerequisites for RADIUS Attribute Value Screening, page 107](#)
- [Restrictions for RADIUS Attribute Value Screening, page 108](#)
- [Information About RADIUS Attribute Value Screening, page 108](#)
- [How to Screen RADIUS Attributes, page 109](#)
- [Configuration Examples for RADIUS Attribute Value Screening, page 111](#)
- [Additional References, page 112](#)
- [Feature Information for RADIUS Attribute Value Screening, page 113](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

## Prerequisites for RADIUS Attribute Value Screening

Before configuring a RADIUS accept or reject list, you must enable AAA.

# Restrictions for RADIUS Attribute Value 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 Value Screening

The RADIUS Attribute Value 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 Value Screening, page 109](#)
- [Verifying RADIUS Attribute Value Screening, page 110](#)

## Configuring RADIUS Attribute Value 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. Router(config)# **aaa authentication ppp default**
4. Router(config)# **aaa authorization network default group** *group-name*
5. Router(config)# **aaa group server radius** *group-name*
6. Router(config-sg-radius)# **server** *ip-address*
7. Router(config-sg-radius)# **authorization** [**accept** | **reject**] *listname*
8. Router(config-sg-radius)# **exit**
9. Router(config)# **radius-server host** {*hostname* | *ip-address*} [**key string**]
10. Router(config)# **radius-server attribute list** *listname*
11. Router(config-sg-radius)# **attribute** *value1* [*value2* [*value3...*]]

### DETAILED STEPS

|        | Command or Action  | Purpose  |
|--------|--|--|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.  |

| Command or Action   | Purpose  |
|---|--|
| <p><b>Step 3</b> Router(config)# <b>aaa authentication ppp default</b></p> <p><b>Example:</b></p> <pre> group group-name </pre>   | <p>Specifies one or more AAA authentication methods for use on serial interfaces running PPP.</p>  |
| <p><b>Step 4</b> Router(config)# <b>aaa authorization network default group group-name</b></p>  | <p>Sets parameters that restrict network access to the user.</p>   |
| <p><b>Step 5</b> Router(config)# <b>aaa group server radius group-name</b></p>  | <p>Groups different RADIUS server hosts into distinct lists and distinct methods.</p>  |
| <p><b>Step 6</b> Router(config-sg-radius)# <b>server ip-address</b></p>   | <p>Configures the IP address of the RADIUS server for the group server,</p>  |
| <p><b>Step 7</b> Router(config-sg-radius)# <b>authorization [accept   reject] listname</b></p> <p><b>Example:</b></p> <p>and/or</p> <p><b>Example:</b></p> <pre> Router(config-sg-radius)# accounting [accept   reject] listname </pre> | <p>Specifies a filter for the attributes that are returned in an Access-Accept packet from the RADIUS server.</p> <p>and/or</p> <p>Specifies a filter for the attributes that are to be sent to the RADIUS server in an accounting request.</p> <p><b>Note</b> The <b>accept</b> keyword indicates that all attributes are rejected except for the attributes specified in the <i>listname</i>. The <b>reject</b> keyword indicates that all attributes are accepted except for the attributes specified in the <i>listname</i> and all standard attributes.</p> |
| <p><b>Step 8</b> Router(config-sg-radius)# <b>exit</b></p>  | <p>Exits server-group configuration mode.</p>  |
| <p><b>Step 9</b> Router(config)# <b>radius-server host {hostname   ip-address} [key string]</b></p>   | <p>Specifies a RADIUS server host.</p>   |
| <p><b>Step 10</b> Router(config)# <b>radius-server attribute list listname</b></p>  | <p>Defines the list name given to the set of attributes defined in the <b>attribute</b> command.</p> <p><b>Note</b> The <i>listname</i> must be the same as the <i>listname</i> defined in Step 5.</p>   |
| <p><b>Step 11</b> Router(config-sg-radius)# <b>attribute value1 [value2 [value3...]]</b></p>  | <p>Adds attributes to the configured accept or reject list.</p> <p><b>Note</b> This command can be used multiple times to add attributes to an accept or reject list.</p>  |

## Verifying RADIUS Attribute Value Screening

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

| Command                                 | Purpose   |
|---|---|
| Router# <b>debug aaa accounting</b>     | Displays information on accountable events as they occur.                 |
| Router# <b>debug aaa authentication</b> | Displays information on AAA authentication.                               |
| Router# <b>show radius statistics</b>   | Displays the RADIUS statistics for accounting and authentication packets. |

## Configuration Examples for RADIUS Attribute Value Screening

- [Authorization Accept Example, page 111](#)
- [Accounting Reject Example, page 111](#)
- [Authorization Reject and Accounting Accept Example, page 112](#)
- [Rejecting Required Attributes Example, page 112](#)

### 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 Value Screening feature.

### Related Documents

| Related Topic           | Document Title   |
|-------------------------|--|
| RADIUS                  | “Configuring RADIUS” feature module.   |
| Other security features | <i>Cisco IOS XE Security Configuration Guide: Securing User Services</i> , Release 2 |
| Security commands       | <i>Cisco IOS Security Command Reference</i>  |

**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   |
|-------|---|
| None. | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

**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.<br><br>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.<br><br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | <a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a> |

## Feature Information for RADIUS Attribute Value 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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 18**      **Feature Information for RADIUS Attribute Value Screening**

| Feature Name                     | Releases                 | Feature Information   |
|----------------------------------|--------------------------|---|
| RADIUS Attribute Value Screening | Cisco IOS XE Release 2.1 | <p>The RADIUS Attribute Value 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.</p> <p>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers</p> <p>The following commands were introduced or modified by this feature: <b>accounting (server-group), authorization (server-group), attribute (server-group), radius-server attribute list</b></p> |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.