



# 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 1](#)
- [Information About RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values, page 2](#)
- [RADIUS Disconnect-Cause Attribute Values, page 9](#)
- [Additional References, page 12](#)
- [Feature Information for RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values, page 14](#)

## Finding Feature Information

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

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:

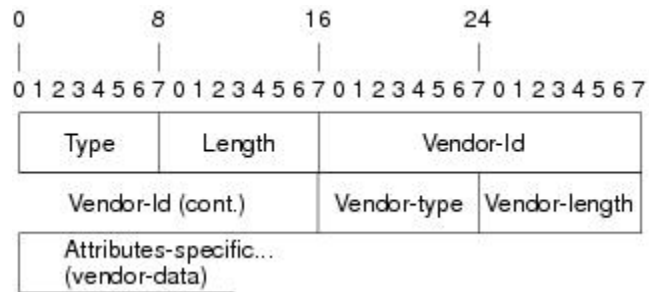
```
cisco-avpair= "shell:priv-lvl=15"
```

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 1: 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 1: Vendor-Specific Attributes Table Field Descriptions**

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

**Table 2: Vendor-Specific RADIUS IETF Attributes**

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

| Number          | Vendor-Specific Company Code | Sub-Type Number | Attribute                 | Description  |
|-----------------|------------------------------|-----------------|---------------------------|--|
| 26              | 311                          | 1               | MSCHAP-Response           | Contains the response value provided by a PPP MS-CHAP user in response to the challenge. It is only used in Access-Request packets. This attribute is identical to the PPP CHAP Identifier. (RFC 2548 )  |
| 26              | 311                          | 11              | MSCHAP-Challenge          | Contains the challenge sent by a network access server to an MS-CHAP user. It can be used in both Access-Request and Access-Challenge packets. (RFC 2548 )   |
| VPDN Attributes |                              |                 |                           |  |
| 26              | 9                            | 1               | l2tp-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.   |

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

| Number          | Vendor-Specific Company Code | Sub-Type Number | Attribute                                   | Description  |
|-----------------|------------------------------|-----------------|---|--|
| 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. |
| H323 Attributes |                              |                 |   |  |
| 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.                    |
| 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.   |

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

| Number | Vendor-Specific Company Code | Sub-Type Number | Attribute      | Description   |
|--------|------------------------------|-----------------|----------------|---|
| 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.   |
| 26     | 9                            | 1               | proxyacl#<n>   | Allows users to configure the downloadable user profiles (dynamic ACLs) by using the authentication proxy feature so that users can have the configured authorization to permit traffic going through the configured interfaces.  |



| Number | Vendor-Specific Company Code | Sub-Type Number | Attribute          | Description   |
|--------|------------------------------|-----------------|--------------------|---|
| 26     | 9                            | 1               | spi                | Carries the authentication information needed by the home agent to authenticate a mobile node during registration. The information is in the same syntax as the <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, disc-cause 4 becomes 1004.

**Table 3: 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.   |
| 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.                         |

| Cause Code | Value                      | Description  |
|------------|----------------------------|--|
| 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 4: 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> |

