

# Additional Vendor-Proprietary RADIUS Attributes

---

## Feature Summary

Remote Authentication Dial-In User Server (RADIUS) is an access server authentication, authorization, and accounting protocol originally developed by Livingston, Inc. Although an Internet Engineering Task Force (IETF) draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. In this release, Cisco IOS software introduces support for additional vendor-proprietary RADIUS attributes, which are listed in Table 1.

**Table 1 Additional Vendor-Proprietary RADIUS Attributes**

Number	Vendor-Proprietary Attribute	Description
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.
190	Pre-Input-Octets	Records the number of input octets before authentication. The Pre-Input-Octets attribute is sent in accounting-stop records.
191	Pre-Output-Octets	Records the number of output octets before authentication. The Pre-Output-Octets attribute is sent in accounting-stop records.
192	Pre-Input-Packets	Records the number of input packets before authentication. The Pre-Input-Packets attribute is sent in accounting-stop records.
193	Pre-Output-Packets	Records the number of output packets before authentication. The Pre-Output-Packets attribute is sent in accounting-stop records.
195	Disconnect-Cause	Specifies the reason a connection was taken off-line. 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. Refer to Table 2 for a list of Disconnect-Cause values and their meanings.

**Table 1 Additional Vendor-Proprietary RADIUS Attributes (Continued)**

Number	Vendor-Proprietary Attribute	Description
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.

Table 2 lists the values and their meanings for the Disconnect-Cause (195) attribute.

**Table 2 Disconnect-Cause Attribute Values**

Value	Description
Unknown (2)	Reason unknown.
CLID-Authentication-Failure (4)	Failure to authenticate calling-party number.
No-Carrier (10)	No carrier detected. This value applies to modem connections.
Lost-Carrier (11)	Loss of carrier. This value applies to modem connections.
No-Detected-Result-Codes (12)	Failure to detect modem result codes. This value applies to modem connections.
User-Ends-Session (20)	User terminates a session. This value applies to EXEC sessions.
Idle-Timeout (21)	Timeout waiting for user input. This value applies to all session types.
Exit-Telnet-Session (22)	Disconnect due to exiting Telnet session. This value applies to EXEC sessions.
No-Remote-IP-Addr (23)	Could not switch to SLIP/PPP; the remote end has no IP address. This value applies to EXEC sessions.
Exit-Raw-TCP (24)	Disconnect due to exiting raw TCP. This value applies to EXEC sessions.
Password-Fail (25)	Bad passwords. This value applies to EXEC sessions.
Raw-TCP-Disabled (26)	Raw TCP disabled. This value applies to EXEC sessions.
Control-C-Detected (27)	Control-C detected. This value applies to EXEC sessions.
EXEC-Process-Destroyed (28)	EXEC process destroyed. This value applies to EXEC sessions.
Timeout-PPP-LCP (40)	PPP LCP negotiation timed out. This value applies to PPP sessions.
Failed-PPP-LCP-Negotiation (41)	PPP LCP negotiation failed. This value applies to PPP sessions.
Failed-PPP-PAP-Auth-Fail (42)	PPP PAP authentication failed. This value applies to PPP sessions.
Failed-PPP-CHAP-Auth (43)	PPP CHAP authentication failed. This value applies to PPP sessions.
Failed-PPP-Remote-Auth (44)	PPP remote authentication failed. This value applies to PPP sessions.

**Table 2 Disconnect-Cause Attribute Values (Continued)**

Value	Description
PPP-Remote-Terminate (45)	PPP received a Terminate Request from remote end. This value applies to PPP sessions.
PPP-Closed-Event (46)	Upper layer requested that the session be closed. This value applies to PPP sessions.
Session-Timeout (100)	Session timed out. This value applies to all session types.
Session-Failed-Security (101)	Session failed for security reasons. This value applies to all session types.
Session-End-Callback (102)	Session terminated due to callback. This value applies to all session types.
Invalid-Protocol (120)	Call refused because the detected protocol is disabled. This value applies to all session types.

For a complete list of supported IETF and vendor-proprietary RADIUS attributes, refer to the “RADIUS Attributes” appendix in the Cisco IOS Release 11.3 *Security Configuration Guide*.

## Benefits

Users who have implemented security solutions using a vendor-proprietary implementation of RADIUS can now integrate Cisco access routers into their networks more easily.

## List of Terms

**Attributes**—Data items sent between a network access server and a daemon that are used to direct AAA activities.

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

**Internet Engineering Task Force (IETF)**—A task force, working under the auspices of the Internet Society (ISOC), consisting of more than 80 working groups. The IETF is responsible for developing Internet standards.

**Network access server (NAS)**—A Cisco access server or any other Cisco device that is acting as a client to the RADIUS server.

## Platforms

The following platforms support vendor-proprietary attributes for RADIUS:

- Cisco 1003, Cisco 1004, Cisco 1005
- Cisco 2500 series
- Cisco 3000/IGS
- Cisco 4000 series (Cisco 4000, 4000-M, 4500, 4500-M, 4700, 4700-M)
- Cisco AS5200 series
- Cisco 7000 series
- Cisco 7200 series
- Cisco 7500 series

## Supported MIBs and RFCs

This feature supports the following RFCs:

- RFC 2138, Remote Authentication Dial-In User Server (RADIUS), April 1997. C. Rigney.
- RFC 2139, RADIUS Accounting, April 1997. C. Rigney, A. Rubens, W. Simpson, and S. Willens.

---

**Note** RFC 2138 obsoletes RFC 2058; RFC 2139 obsoletes RFC 2059.

---

No MIBs are supported by this feature.

## Configuration Tasks

To configure your Cisco router or access server to recognize vendor-proprietary RADIUS attributes, perform the following steps:

- Step 1** Use the **aaa new-model** global configuration command to enable AAA. RADIUS is administered through AAA so AAA must be enabled if you plan to use RADIUS, whether IETF draft-compliant or vendor-proprietary. For more information about AAA or using the **aaa new-model** command, refer to the “AAA Overview” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.
- Step 2** Use the **aaa authentication** global configuration command to define method lists, selecting RADIUS as the method for authentication. For more information about using the **aaa authentication** command, refer to the “Configuring Authentication” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.
- Step 3** Use the **line** and **interface** commands to select specific lines and interfaces to which the defined method lists will be applied. For more information about applying method lists to lines and interfaces, refer to the “Configuring Authentication” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.

- Step 4** Use the **radius-server host non-standard** command to enable your Cisco router, acting as a NAS, to recognize that the RADIUS security server is using a vendor-proprietary version of RADIUS. For more information, refer to the “Configuring RADIUS” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.
- Step 5** Use the **radius-server key** command to specify the shared secret text string used between your Cisco router and the RADIUS server. For more information, refer to the “Configuring RADIUS” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.

## Configuration Example

The following sample is a general configuration using vendor-proprietary RADIUS with the AAA command set:

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins radius local
aaa authorization network radius local
aaa accounting network start-stop radius

username root password ALongPassword

radius-server configure-nas
radius-server host alcatraz non-standard
radius-server key myRaDiUSpassWoRd

interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication pap dialins

line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
```

The lines in this sample RADIUS AAA configuration are defined as follows:

- The **aaa new-model** command enables AAA network security services.
- The **aaa authentication login admins local** command defines another method list, “admins,” for login authentication.
- The **aaa authentication ppp dialins radius local** command defines the authentication method list “dialins,” which specifies that RADIUS authentication, then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.
- The **aaa authorization network radius local** command is used to assign an address and other network parameters to the RADIUS user.
- The **aaa accounting network start-stop radius** command tracks PPP usage.
- The **username** command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.
- The **radius-server configure-nas** command defines that the Cisco router or access server will query the RADIUS server for static routes and IP pool definitions when the device first starts up.
- The **radius-server host non-standard** command defines the name of the RADIUS server host and identifies that this RADIUS host uses a vendor-proprietary version of RADIUS.

- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **interface group-async** command selects and defines an asynchronous interface group.
- The **group-range** command defines the member asynchronous interfaces in the interface group.
- The **encapsulation ppp** command sets PPP as the encapsulation method used on the specified interfaces.
- The **ppp authentication pap dialins** command applies the “dialins” method list to the specified interfaces.
- The **line** command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.
- The **autoselect ppp** command configures the Cisco IOS software to allow a PPP session to start up automatically on these selected lines.
- The **autoselect during-login** command is used to display the username and password prompt without pressing the Return key. After the user logs in, the autoselect function (in this case, PPP) begins.
- The **login authentication admins** command applies the “admins” method list for login authentication.
- The **modem dialin** command configures modems attached to the selected lines to only accept incoming calls.

## Command Reference

There are no new or modified commands introduced with this feature. All commands used with this feature are documented in the Cisco IOS Release 11.3 command references.