

# RADIUS Attributes

---

Remote Authentication Dial-In User Server (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 appendix lists the RADIUS attributes currently supported.

## RADIUS IETF Attributes

Table 19 lists the supported RADIUS (IETF) attributes. In cases where the attribute has a security server-specific format, the format is specified.

**Table 19 Supported RADIUS (IETF) Attributes**

<b>Number</b>	<b>Attribute</b>	<b>Description</b>	<b>Cisco IOS Release 11.1</b>	<b>Cisco IOS Release 11.2</b>	<b>Cisco IOS Release 11.3</b>
1	User-Name	Indicates the name of the user being authenticated.	yes	yes	yes
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 the IETF Draft #2 (or later) specifications.	yes	yes	yes
3	CHAP-Password	Indicates the response value provided by a PPP Challenge-Handshake Authentication Protocol (CHAP) user in response to an Access-Challenge.	yes	yes	yes
4	NAS-IP Address	Specifies the IP address of the network access server that is requesting authentication.	yes	yes	yes

Table 19 Supported RADIUS (IETF) Attributes (Continued)

Number	Attribute	Description	Cisco IOS Release 11.1	Cisco IOS Release 11.2	Cisco IOS Release 11.3
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>6nsss</b>.</p>	yes	yes	yes
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:                     <ul style="list-style-type: none"> <li>Framed for known PPP or SLIP connection.</li> <li>Administrative-user for <b>enable</b> command.</li> </ul> </li> <li>In response:                     <ul style="list-style-type: none"> <li>Login—Make a connection.</li> <li>Framed—Start SLIP or PPP.</li> <li>Administrative User—Start an EXEC or <b>enable ok</b>.</li> <li>Exec User—Start an EXEC session.</li> </ul> </li> </ul>	yes	yes	yes
7	Framed-Protocol	Indicates the framing to be used for framed access.	yes	yes	yes
8	Framed-IP-Address	Indicates the address to be configured for the user.	yes	yes	yes
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.	yes	yes	yes

Table 19 Supported RADIUS (IETF) Attributes (Continued)

Number	Attribute	Description	Cisco IOS Release 11.1	Cisco IOS Release 11.2	Cisco IOS Release 11.3
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.	yes	yes	yes
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.	yes	yes	yes
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.	yes	yes	yes
14	Login-IP-Host	Indicates the host to which the user will connect when the Login-Service attribute is included.	yes	yes	yes
15	Login-Service	Indicates the service that should be used to connect the user to the login host.	yes	yes	yes
16	Login-Port	Defines the TCP port with which the user is to be connected when the Login-Service attribute is also present.	yes	yes	yes
18	Reply-Message	Indicates text that might be displayed to the user.	yes	yes	yes
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.	yes	yes	yes
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.	yes	yes	yes

**Table 19 Supported RADIUS (IETF) Attributes (Continued)**

Number	Attribute	Description	Cisco IOS Release 11.1	Cisco IOS Release 11.2	Cisco IOS Release 11.3
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 AVpair 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 "NAS Prompt" user to have immediate access to EXEC commands.</p> <p>Table 20 provides a complete list of supported TACACS+ attribute/value (AV) pairs that can be used with IETF Attribute 26.</p>	yes	yes	yes
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." This attribute is not valid for PPP sessions.</p>	yes	yes	yes

**Table 19 Supported RADIUS (IETF) Attributes (Continued)**

Number	Attribute	Description	Cisco IOS Release 11.1	Cisco IOS Release 11.2	Cisco IOS Release 11.3
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." This attribute is not valid for PPP sessions.	yes	yes	yes
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.	yes	yes	yes
35	Login-LAT-Node	Indicates the node with which the user is to be automatically connected by LAT.	no	no	no
36	Login-LAT-Group	Identifies the LAT group codes that this user is authorized to use.	no	no	no
49	Terminate-Cause	Reports details on why the connection was terminated.	no	no	no

Table 20 lists the supported TACACS+ AV pairs and their meanings for the Vendor-Specific (26) attribute. For more information about TACACS+ AV pairs, refer to the "TACACS+ AV Pairs" chapter in the Cisco IOS Release 12.0 *Security Configuration Guide*.

**Table 20 Supported TACACS+ AV Pairs**

Attribute	Description
service=x	The primary service. Specifying a service attribute indicates that this is a request for authorization or accounting of that service. Current values are <b>slip</b> , <b>ppp</b> , <b>arap</b> , <b>shell</b> , <b>tty-daemon</b> , <b>connection</b> , and <b>system</b> . This attribute must always be included.
protocol=x	A protocol that is a subset of a service. An example would be any PPP NCP. Currently known values are <b>lcp</b> , <b>ip</b> , <b>ipx</b> , <b>atalk</b> , <b>vines</b> , <b>lat</b> , <b>xremote</b> , <b>tn3270</b> , <b>telnet</b> , <b>rlogin</b> , <b>pad</b> , <b>vpdn</b> , <b>osicp</b> , <b>deccp</b> , <b>ccp</b> , <b>cdp</b> , <b>bridging</b> , <b>xns</b> , <b>nbf</b> , <b>bap</b> , <b>multilink</b> , and <b>unknown</b> .
cmd=x	A shell (EXEC) command. This indicates the command name for a shell command that is to be run. This attribute must be specified if service equals "shell." A NULL value indicates that the shell itself is being referred to.
cmd-arg=x	An argument to a shell (EXEC) command. This indicates an argument for the shell command that is to be run. Multiple cmd-arg attributes may be specified, and they are order dependent.
acl=x	ASCII number representing a connection access list. Used only when service=shell.
inacl=x	ASCII identifier for an interface input access list. Used with service=ppp and protocol=ip. Per-user access lists do not currently work with ISDN interfaces.
inacl#<n>	ASCII access list identifier for an input access list to be installed and applied to an interface for the duration of the current connection. Used with service=ppp and protocol=ip, and service=ppp and protocol=ipx. Per-user access lists do not currently work with ISDN interfaces.

**Table 20 Supported TACACS+ AV Pairs (Continued)**

Attribute	Description
outacl=x	ASCII identifier for an interface output access list. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx. Contains an IP output access list for SLIP or PPP/IP (for example, outacl=4). The access list itself must be preconfigured on the router. Per-user access lists do not currently work with ISDN interfaces.
outacl#<n>	ASCII access list identifier for an interface output access list to be installed and applied to an interface for the duration of the current condition. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx. Per-user access lists do not currently work with ISDN interfaces.
zonelist=x	A numeric zonelist value. Used with service=arap. Specifies an AppleTalk zonelist for ARA (for example, zonelist=5).
addr=x	A network address. Used with service=slip, service=ppp, and protocol=ip. Contains the IP address that the remote host should use when connecting via SLIP or PPP/IP. For example, addr=10.2.3.4.
addr-pool=x	Specifies the name of a local pool from which to get the address of the remote host. Used with service=ppp and protocol=ip.  Note that <b>addr-pool</b> works in conjunction with local pooling. It specifies the name of a local pool (which must be preconfigured on the network access server). Use the <b>ip-local pool</b> command to declare local pools. For example:  <pre>ip address-pool local ip local pool boo 10.0.0.1 10.0.0.10 ip local pool moo 10.0.0.1 10.0.0.20</pre> You can then use TACACS+ to return addr-pool=boo or addr-pool=moo to indicate the address pool from which you want to get this remote node's address.
routing=x	Specifies whether routing information is to be propagated to and accepted from this interface. Used with service=slip, service=ppp, and protocol=ip. Equivalent in function to the /routing flag in SLIP and PPP commands. Can either be true or false (for example, routing=true).
route	Specifies a route to be applied to an interface. Used with service=slip, service=ppp, and protocol=ip.  During network authorization, the route attribute can be used to specify a per-user static route, to be installed by TACACS+ as follows:  <pre>route="dst_address mask [gateway]"</pre> This indicates a temporary static route that is to be applied. The <i>dst_address</i> , <i>mask</i> , and <i>gateway</i> are expected to be in the usual dotted-decimal notation, with the same meanings as in the familiar <b>ip route</b> configuration command on a network access server.  If <i>gateway</i> is omitted, the peer's address is the gateway. The route is expunged when the connection terminates.
route#<n>	Like the route AV pair, this specifies a route to be applied to an interface, but these routes are numbered, allowing multiple routes to be applied. Used with service=ppp and protocol=ip, and service=ppp and protocol=ipx.
timeout=x	The number of minutes before an EXEC or ARA session disconnects (for example, timeout=60). A value of zero indicates no timeout. Used with service=arap.
idletime=x	Sets a value, in minutes, after which an idle session is terminated. Does not work for PPP. A value of zero indicates no timeout.
autocmd=x	Specifies an autocommand to be executed at EXEC startup (for example, autocmd=telnet muruga.com). Used only with service=shell.
noescape=x	Prevents user from using an escape character. Used with service=shell. Can be either true or false (for example, noescape=true).

**Table 20 Supported TACACS+ AV Pairs (Continued)**

Attribute	Description
nohangup=x	Used with service=shell. Specifies the nohangup option, which means that after an EXEC shell is terminated, the user is presented with another login (username) prompt. Can be either true or false (for example, nohangup=false).
priv-lvl=x	Privilege level to be assigned for the EXEC. Used with service=shell. Privilege levels range from 0 to 15, with 15 being the highest.
callback-dialstring	Sets the telephone number for a callback (for example: callback-dialstring=408-555-1212). Value is NULL, or a dial-string. A NULL value indicates that the service may choose to get the dialstring through other means. Used with service=arap, service=slip, service=ppp, service=shell. Not valid for ISDN.
callback-line	The number of a TTY line to use for callback (for example: callback-line=4). Used with service=arap, service=slip, service=ppp, service=shell. Not valid for ISDN.
callback-rotary	The number of a rotary group (between 0 and 100 inclusive) to use for callback (for example: callback-rotary=34). Used with service=arap, service=slip, service=ppp, service=shell. Not valid for ISDN.
nocallback-verify	Indicates that no callback verification is required. The only valid value for this parameter is 1 (for example, nocallback-verify=1). Used with service=arap, service=slip, service=ppp, service=shell. There is no authentication on callback. Not valid for ISDN.
tunnel-id	Specifies the username that will be used to authenticate the tunnel over which the individual user MID will be projected. This is analogous to the <i>remote name</i> in the <b>vpdn outgoing</b> command. Used with service=ppp and protocol=vpdn.
ip-addresses	Space-separated list of possible IP addresses that can be used for the end-point of a tunnel. Used with service=ppp and protocol=vpdn.
nas-password	Specifies the password for the network access server during the L2F tunnel authentication. Used with service=ppp and protocol=vpdn.
gw-password	Specifies the password for the home gateway during the L2F tunnel authentication. Used with service=ppp and protocol=vpdn.
rte-fltr-in#<n>	Specifies an input access list definition to be installed and applied to routing updates on the current interface for the duration of the current connection. Used with service=ppp and protocol=ip, and with service=ppp and protocol=ipx.
rte-fltr-out#<n>	Specifies an output access list definition to be installed and applied to routing updates on the current interface for the duration of the current connection. Used with service=ppp and protocol=ip, and with service=ppp and protocol=ipx.
sap#<n>	Specifies static Service Advertising Protocol (SAP) entries to be installed for the duration of a connection. Used with service=ppp and protocol=ipx.
sap-fltr-in#<n>	Specifies an input SAP filter access list definition to be installed and applied on the current interface for the duration of the current connection. Used with service=ppp and protocol=ipx.
sap-fltr-out#<n>	Specifies an output SAP filter access list definition to be installed and applied on the current interface for the duration of the current connection. Used with service=ppp and protocol=ipx.
pool-def#<n>	Used to define IP address pools on the network access server. Used with service=ppp and protocol=ip.
pool-timeout=	To be provided.
source-ip=x	Used as the source IP address of all VPDN packets generated as part of a VPDN tunnel. This is equivalent to the Cisco <b>vpdn outgoing</b> global configuration command.
max-links=<n>	Restricts the number of links that a user can have in a multilink bundle. Used with service=ppp and protocol=multilink. The range for <n> is from 1 to 255.

**Table 20 Supported TACACS+ AV Pairs (Continued)**

Attribute	Description
load-threshold=<n>	Sets the load threshold at which additional links are either added to or deleted from the multilink bundle. If the load goes above the specified value, additional links are added. If the load goes below the specified value, links are deleted. Used with service=ppp and protocol=multilink. The range for <n> is from 1 to 255.
dns-servers=	Identifies a DNS server (primary or secondary) that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation. To be used with service=ppp and protocol=ip. The IP address identifying each DNS server is entered in dotted decimal format.
wins-servers=	Identifies a Windows NT server that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation. To be used with service=ppp and protocol=ip. The IP address identifying each Windows NT server is entered in dotted decimal format.

For more information about RADIUS configuration tasks, refer to the “Configuring RADIUS” chapter.

## RADIUS Accounting Attributes

Table 21 lists the supported RADIUS (IETF) accounting attributes. In cases where the attribute has a security server-specific format, the format is specified.

**Table 21 Supported RADIUS (IETF) Accounting Attributes**

Number	Attribute	Description	Cisco IOS Release 11.1	Cisco IOS Release 11.2	Cisco IOS Release 11.3
25	Class	Arbitrary value that the network access server includes in all accounting packets for this user if supplied by the RADIUS server.	yes	yes	yes
30	Called-Station-Id	Allows the network access server to send the telephone number the user called as part of the Access-Request packet (using Dialed Number Identification [DNIS] or similar technology). This attribute is only supported on ISDN, and modem calls on the Cisco AS5200 if used with PRI.	yes	yes	yes
31	Calling-Station-Id	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.	yes	yes	yes

**Table 21 Supported RADIUS (IETF) Accounting Attributes (Continued)**

<b>Number</b>	<b>Attribute</b>	<b>Description</b>	<b>Cisco IOS Release 11.1</b>	<b>Cisco IOS Release 11.2</b>	<b>Cisco IOS Release 11.3</b>
40	Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (start) or the end (stop).	yes	yes	yes
41	Acct-Delay-Time	Indicates how many seconds the client has been trying to send a particular record.	yes	yes	yes
42	Acct-Input-Octets	Indicates how many octets have been received from the port over the course of this service being provided.	yes	yes	yes
43	Acct-Output-Octets	Indicates how many octets have been sent to the port in the course of delivering this service.	yes	yes	yes
44	Acct-Session-Id	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.	yes	yes	yes
45	Acct-Authentic	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.	yes	yes	yes
46	Acct-Session-Time	Indicates how long (in seconds) the user has received service.	yes	yes	yes
47	Acct-Input-Packets	Indicates how many packets have been received from the port over the course of this service being provided to a framed user.	yes	yes	yes
48	Acct-Output-Packets	Indicates how many packets have been sent to the port in the course of delivering this service to a framed user.	yes	yes	yes
50	Acct-Multi-Session-Id <sup>1</sup>	A unique accounting identifier used to link multiple related sessions in a log file.  Each linked session in a multilink session has a unique Acct-Session-Id value, but shares the same Acct-Multi-Session-Id.	no	no	yes

**Table 21 Supported RADIUS (IETF) Accounting Attributes (Continued)**

Number	Attribute	Description	Cisco IOS Release 11.1	Cisco IOS Release 11.2	Cisco IOS Release 11.3
51	Acct-Link-Count <sup>2</sup>	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.	no	no	yes
61	NAS-Port-Type	Indicates the type of physical port the network access server is using to authenticate the user.	yes	yes	yes

1. Only stop records contain multi-session IDs. This is because start records are issued before any multilink processing takes place.
2. Only stop records contain link counts. This is because start records are issued before any multilink processing takes place.

For more information about configuring RADIUS accounting, refer to the “Configuring RADIUS” chapter in the Cisco IOS Release 11.3 *Security Configuration Guide*.

## RADIUS Vendor-Proprietary Attributes

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. Table 22 lists the supported vendor-proprietary RADIUS attributes:

**Table 22 Supported Vendor-Proprietary RADIUS Attributes**

Number	Vendor-Proprietary Attribute	Description
17	Change-Password	Specifies a request to change a user’s password.
21	Password-Expiration	Specifies an expiration date for a user’s password in the user’s file entry.
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	Terminate-Cause	Reports details on why the connection was terminated.
208	PW-Lifetime	Enables you to specify on a per-user basis the number of days that a password is valid.
209	IP-Direct	Specifies in a user’s file entry the IP address to which the Cisco router redirects packets from the user. When you include this attribute in a user’s file entry, the Cisco router bypasses all internal routing and bridging tables and sends all packets received on this connection’s WAN interface to the specified IP address.
210	PPP-VJ-Slot-Comp	Instructs the Cisco router not to use slot compression when sending VJ-compressed packets over a PPP link.

**Table 22 Supported Vendor-Proprietary RADIUS Attributes (Continued)**

Number	Vendor-Proprietary Attribute	Description
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.
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.
228	Route-IP	Indicates whether IP routing is allowed for the user's file entry.
233	Link-Compression	Defines whether to turn on or turn off "stac" compression over a PPP link.
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.
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.

For more information about configuring RADIUS to recognize vendor-proprietary attributes, refer to the "Configuring RADIUS" chapter.

