RADIUS 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 appendix describes the following types of RADIUS attributes supported in Broadband Network Gateway (BNG):

RADIUS IETF Attributes

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.

Table 1: Supported RADIUS IETF Attributes

Name	Value	Type
Acct-Delay-Time	integer	41
Acct-Input-Giga-Words	integer	52
Acct-Input-Octets	integer	42
Acct-Input-Packets	integer	47

Name	Value	Type
Acct-Interim-Interval	integer	85
Acct-Link-Count	integer	51
Acct-Output-Giga-Words	integer	53
Acct-Output-Octets	integer	43
Acct-Output-Packets	integer	48
Acct-Status-Type	integer	40
Acct-Terminate-Cause	integer	49
CHAP-Challenge	binary	40
CHAP-Password	binary	3
Delegated-IPv6-Prefix	binary	123
Dynamic-Author-Error-Cause	integer	101
Event-Timestamp	integer	55
Filter-Id	string	11
Framed-Interface-Id	binary	96
Framed-IP-Address	ipv4addr	8
Framed-IPv6-Route	string	99
Framed-Pool	string	88
Framed-Protocol	integer	7
Framed-Route	string	22
Nas-Identifier	string	32
NAS-IP-Address	ipv4addr	4
NAS-IPv6-Address	string	95
NAS-Port	integer	5
Reply-Message	binary	18
Service-Type	integer	6
Session-Timeout	integer	27
Stateful-IPv6-Address-Pool	binary	123
X-Ascend-Client-Primary-DNS	ipv4addr	135
X-Ascend-Client-Secondary-DNS	ipv4addr	136

Filter-Id

Filter-ID specifies the access control list (ACL) that is applied to the subscriber interface. The format of the Filter-Id attribute is as follows:

```
Filter-Id = <ACL-Name> <in | out>
```

Where, **in** and **out** indicate the direction of the ACL feature to be applied. **ACL in** is mapped to the input direction (IPv4 Ingress), and **ACL out** is mapped to the output direction (IPv4 Egress) of the CP-UP session programming interface. You can configure only one attribute per direction.

Session-Timeout

Session-Timeout sets the maximum number of seconds of service to be provided to the user before the session terminates. Session-Timeout attribute can be sent as part of CoA request, Access-Accept, or Access-Challenge messages.

You can enable session-timeout using the user-profile on a RADIUS server. For example:

```
user1 Cleartext-Password := "cisco"
  Session-timeout = 90'
```

Once the timer expires, the subscriber is removed from the server.

For session deletion due to session-timeout, the reason of disconnect can be observed as “Session-Timeout” in accounting messages. For example,

```
(5) Sent Access-Accept Id 7 from 10.1.35.10:1812 to 10.1.32.83:16384 length 0
(5)   Session-Timeout = 90

(8)   Acct-Terminate-Cause = Session-Timeout
(8)   Ascend-Disconnect-Cause = Session-Timeout
```

Verification:

You can verify the session-timeout configuration using the **show subscriber session detail** command:

```
show subscriber session detail
    "subcfgInfo": {
        "committedAttrs": {
          "attrs": {
            "accounting-list": "automation-aaaprofile",
            "acct-interval": "2000",
            "addr-pool": "automation-poolv4",
            "ipv4-mtu": "1400",
            "ppp-ipcp-reneg-ignore": "true",
            "ppp-ipv6cp-reneg-ignore": "true",
            "ppp-lcp-reneg-ignore": "true",
            "session-acct-enabled": "true",
            "session-timeout": "90",
            "vrf": "automation-vrf"
          }
        },
```

IETF Tagged Attributes on LAC

The IETF Tagged Attributes support on L2TP Access Concentrator (LAC) provides a means of grouping tunnel attributes referring to the same tunnel in an Access-Accept packet sent from the RADIUS server to the LAC. The Access-Accept packet can contain multiple instances of same RADIUS attributes, but with different tags. The tagged attributes support ensures that all attributes pertaining to a given tunnel contain the same value in their respective tag fields, and that each set includes an appropriately-valued instance of the Tunnel-Preference attribute. This conforms to the tunnel attributes that are to be used in a multi-vendor network environment, thereby eliminating interoperability issues among Network Access Servers (NASs) manufactured by different vendors.

For details of RADIUS Attributes for Tunnel Protocol Support, refer RFC 2868.

These examples describe the format of IETF Tagged Attributes:

```
Tunnel-Type = :0:L2TP, Tunnel-Medium-Type = :0:IP, Tunnel-Server-Endpoint = :0:"1.1.1.1",
Tunnel-Assignment-Id = :0:"1", Tunnel-Preference = :0:1, Tunnel-Password = :0:"hello"
```

A tag value of 0 is used in the above example in the format of `:0:`, to group those attributes in the same packet that refer to the same tunnel. Similar examples are:

```
Tunnel-Type = :1:L2TP, Tunnel-Medium-Type = :1:IP, Tunnel-Server-Endpoint = :1:"2.2.2.2",
Tunnel-Assignment-Id = :1:"1", Tunnel-Preference = :1:1, Tunnel-Password = :1:"hello"

Tunnel-Type = :2:L2TP, Tunnel-Medium-Type = :2:IP, Tunnel-Server-Endpoint = :2:"3.3.3.3",
Tunnel-Assignment-Id = :2:"1", Tunnel-Preference = :2:2, Tunnel-Password = :2:"hello"

Tunnel-Type = :3:L2TP, Tunnel-Medium-Type = :3:IP, Tunnel-Server-Endpoint = :3:"4.4.4.4",
Tunnel-Assignment-Id = :3:"1", Tunnel-Preference = :3:2, Tunnel-Password = :3:"hello"

Tunnel-Type = :4:L2TP, Tunnel-Medium-Type = :4:IP, Tunnel-Server-Endpoint = :4:"5.5.5.5",
Tunnel-Assignment-Id = :4:"1", Tunnel-Preference = :4:3, Tunnel-Password = :4:"hello"

Tunnel-Type = :5:L2TP, Tunnel-Medium-Type = :5:IP, Tunnel-Server-Endpoint = :5:"6.6.6.6",
Tunnel-Assignment-Id = :5:"1", Tunnel-Preference = :5:3, Tunnel-Password = :5:"hello"
```

Table 2: Supported IETF Tagged Attributes

IETF Tagged Attribute Name	Value	Type
Tunnel-Type	integer	64
Tunnel-Medium-Type	integer	65
Tunnel-Client-Endpoint	string	66
Tunnel-Server-Endpoint	string	67
Tunnel-Password	string	69
Tunnel-Assignment-ID	string	82
Tunnel-Preference	integer	83
Tunnel-Client-Auth-ID	string	90
Tunnel-Server-Auth-ID	string	91

RADIUS Vendor-Specific Attributes

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.

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 this 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.

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"
```

The following example shows how to configure avpair aaa attribute to enable IPv6 router advertisements from an IPv4 subscriber interface:

```
Cisco-avpair= "ipv6:start-ra-on-ipv6-enable=1"
```

Attribute 26 contains these three elements:

- Type
- Length
- String (also known as data)
  - Vendor-ID
  - Vendor-Type
  - Vendor-Length
  - Vendor-Data

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.

Table 3: Supported Cisco Vendor-Specific RADIUS Attributes

Name	Value	Type	Present in AAA message type
accounting-list	string	1	Access-accept, CoA, Accounting-request
acct-input-gigawords-ipv4	integer	1	Accounting-request
acct-input-octets-ipv4	integer	1	Accounting-request
acct-input-packets-ipv4	integer	1	Accounting-request
acct-input-gigawords-ipv6	integer	1	Accounting-request
acct-input-octets-ipv6	integer	1	Accounting-request
acct-input-packets-ipv6	integer	1	Accounting-request
acct-output-gigawords-ipv4	integer	1	Accounting-request

Name	Value	Type	Present in AAA message type
acct-output-octets-ipv4	integer	1	Accounting-request
acct-output-packets-ipv4	integer	1	Accounting-request
acct-output-gigawords-ipv6	integer	1	Accounting-request
acct-output-octets-ipv6	integer	1	Accounting-request
acct-output-packets-ipv6	integer	1	Accounting-request
addrv6	string	1	Access-accept, Accounting-request
circuit-id-tag	string	1	Access-accept, Accounting-request
cisco-nas-port	string	2	Access-accept, Accounting-request
client-mac-address	string	1	Access-accept, Accounting-request
command	string	1	CoA
connect-progress	string	1	Accounting-request
delegated-ipv6-pool	string	1	Access-accept
dhcp-class	string	1	Access-accept
dhcp-client-id	string	1	Accounting-request
dhcp-vendor-class	string	1	Access-request, Accounting-request
disc-cause-ext	string	1	Accounting-request
disconnect-cause	string	1	Accounting-request
dual-stack-delay	integer	1	Access-accept
inacl	string	1	Access-accept
intercept-id	integer	1	Access-accept
ip-addresses	string	1	Access-request, Accounting-request
ip:route	string	1	Access-accept, CoA
ip:ipv6-route	string	1	Access-accept, CoA
ipv6_inacl	string	1	Access-accept, CoA
ipv6_outacl	string	1	Access-accept, CoA
ipv6-dns-servers-addr	string	1	Access-accept
ipv6-mtu	integer	1	Access-accept
ipv6-strict-rpf	integer	1	Access-accept

Name	Value	Type	Present in AAA message type
ipv6-unreachable	integer	1	Access-accept
l2tp-tunnel-password	string	1	Access-accept
md-dscp	integer	1	Access-accept
md-ip-addr	ipaddr	1	Access-accept
md-port	integer	1	Access-accept
outacl	string	1	Access-accept
parent-session-id	string	1	Accounting-request
pppoe_session_id	integer	1	Accounting-request
primary-dns	ipaddr	1	Access-accept
remote-id-tag	string	1	Access-request, Accounting-request
sa	string	1	Access-accept, CoA
sd	string	1	RADIUS CoA
secondary-dns	ipaddr	1	Access-accept
service-name	string	1	Accounting-request
source-ip	ipv4addr	1	Access-accept
Stateful-IPv6-Address-Pool	string	1	Access-accept
sub-pbr-policy-in	string	1	Access-accept, CoA
subscriber:sub-qos-policy-in	string	1	Access-accept, CoA
subscriber:sub-qos-policy-out	string	1	Access-accept, CoA
tunnel-tos-reflect	string	1	Access-accept
tunnel-tos-setting	string	1	Access-accept
tunnel-type	string	1	Access-accept
username	string	1	Access-request, Accounting-request
user-plane-ip-address	string	1	Access-request, Accounting-request
vpdn-group	string	1	Access-accept
vpn-vrf	string	1	Access-accept
vrf	string	1	Access-accept
vrf-id	string	1	Access-accept

Vendor-Specific Attributes for Account Operations

Table 4: Supported Vendor-Specific Attributes for Account Operations

RADIUS AVP	Value	Type	Action
subscriber:command=account-update	string	1	account update
subscriber:sa=<service-name>	string	1	service activate
subscriber:sd=<service-name>	string	1	service de-activate

RADIUS ADSL Attributes

Table 5: Supported RADIUS ADSL Attributes

Name	Value	Type
Agent-Circuit-Id	string	1
Agent-Remote-Id	string	2

RADIUS ASCEND Attributes

Table 6: Supported RADIUS Ascend Attributes

Name	Value	Type
Ascend-Client-Primary-DNS	ipv4addr	135
Ascend-Client-Secondary-DNS	ipv4addr	136
Ascend-Connection-Progress	integer	196
Ascend-Disconnect-Cause	integer	195

RADIUS Disconnect-Cause Attributes

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.

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 7: Supported Disconnect-Cause Attributes

Cause Code	Value	Description
2	Unknown	Reason unknown.
3	Call-Disconnect	The call has been disconnected.
11	Lost-Carrier	Loss of carrier.
21	Idle-Timeout	Timeout waiting for user input. **Note** Codes 21, 100, 101, 102, and 120 apply to all session types.
28	EXEC-Process-Destroyed	EXEC process destroyed.
33	Insufficient-Resources	Insufficient resources.
40	Timeout-PPP-LCP	PPP LCP negotiation timed out. **Note** Codes 40 through 49 apply to PPP sessions.
41	Failed-PPP-LCP-Negotiation	PPP LCP negotiation failed.
42	Failed-PPP-PAP-Auth-Fail	PPP PAP authentication failed.
45	PPP-Remote-Terminate	PPP received a Terminate Request from remote end.
47	NCP-Closed-PPP	PPP session closed because there were no NCPs open.
52	Invalid-IP-Address	IP address is not valid for Telnet host.
100	Session-Timeout	Session timed out.
150	RADIUS-Disconnect	Disconnected by RADIUS request.
151	Local-Admin-Disconnect	Administrative disconnect.
170	PPP-Authentication-Timeout	PPP authentication timed out.

RADIUS Attributes