Technical Guide

Local RADIUS Server

Feature Overview and Configuration Guide

Introduction

In some situations, like a remote branch office, it is convenient to use an AlliedWare Plus™ switch as the RADIUS server for user and device authentication, rather than to have another, separate RADIUS server.

Hence, RADIUS server capability is provided as a built-in feature of AlliedWare Plus. The built-in RADIUS server is referred to as Local RADIUS server.

This guide describes the functionality of the Local RADIUS server, and how to configure it.

Products and software version that apply to this guide

This guide applies to AlliedWare Plus products that support the local RADIUS server, running version **5.4.4** or later. To see whether your product supports the local RADIUS server, see the following documents:

- The product's Datasheet
- The product's Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

Feature support may change in later software versions. For the latest information, see the above documents.

The following features are supported since the following software versions:

- Multiple instance of a RADIUS attributes can be assigned to users - 5.5.0-1.1

Content

Configuring the Local RADIUS Server

Enable the Local RADIUS Server

The Local RADIUS Server is disabled by default. Enter the following commands to enable the Local RADIUS Server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# server enable
awplus(config-radsrv)# exit
```

This will automatically initialize the internal Certificate Authority (CA) on the device. It will also automatically create a server certificate and enroll the certificate with the Local CA by implicitly executing the following commands:

```
awplus(config)# crypto pki trustpoint local
awplus(config)# exit
awplus# crypto pki enroll local
```

The **crypto pki trustpoint local** command declares the Local CA as the CA from which to obtain certificates. The Local CA has be defined first so certificates can be obtained from it. The **crypto pki enroll local** command obtains the system certificate from the Local CA.

For more information about PKI, see the Public Key Infrastructure (PKI) Feature Overview and Configuration Guide.

The device is automatically added to the list of authenticators that may send authentication requests to the Local RADIUS Server by implicitly executing the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# nas 127.0.0.1 key awplus-local-radius-server
awplus(config-radsrv)# exit
```

Note: The key **awplus-local-radius-server** is a pre-defined component that can be used for internal exchanges between the device's RADIUS client and its RADIUS server.

Add the Local RADIUS Server as a RADIUS Server

Although the switch is automatically defined as a NAS (Network Access Server) for the Local RADIUS Server, you must manually add the Local RADIUS Server to the server list defined for the Local RADIUS Client.

Use the following command to add the Local RADIUS Server as a RADIUS Server. The Local RADIUS Client can then send authentication requests to its Local RADIUS Server:

```
awplus(config)# radius-server host 127.0.0.1 key awplus-local-radius-
server
```

Add authenticators to the NAS list

Authenticators (sometimes referred to as Network Access Servers or NASs) are devices that can send authentication requests to the RADIUS Server.

Use the following commands to add other authenticators to the list of authenticators.

```
awplus(config)# radius-server local
awplus(config-radsrv)# nas <nas-ip-address> key <nas-keystring>
awplus(config-radsrv)# exit
```

Configure the local RADIUS Server user database

Authentication can be performed in multiple contexts, such as the authentication of users logging in at a console, as well as tri-authentication of devices connecting to switch ports.

Adding users for port authentication

For entries that will be used to authenticate dot1x supplicants, but not assign them to a VLAN, the following commands will add users to the RADIUS user list:

```
awplus(config)# radius-server local
awplus(config-radsrv)# user <radius-user-name> password <user-password>
```

Note that a RADIUS user's password, in the local RADIUS database, should be no longer than 31 characters. The password of RADIUS user in remote RADIUS server (e.g. FreeRADIUS on Linux) can be up to 128 characters in length.

Adding uses for port authentication that will be assigned a VLAN

Add users to the RADIUS user list, and define a VLAN ID that will be assigned to them.

To add entries to be used to authenticate dot1x supplicants, and assign them to a VLAN, follow the two steps shown below:

Step 1: **Create groups associated with the VIDs that will be allocated**

Enter the following commands to create groups with the VIDs that will be allocated to them

```
awplus(config)# radius-server local
awplus(config-radsrv)# group VLAN10Users
awplus(config-radsrv)# vlan 10
awplus(config-radsrv)# group VLAN11Users
awplus(config-radsrv)# vlan 11
```

Step 2: **Add the users after creating groups**

Add the users and refer to the relevant group in the command that creates the user as below:

```
awplus(config-radsrv)# user VCSPCVLAN10 password VCSPCPass group
VLAN10Users
awplus(config-radsrv)# user VCSPCVLAN11 password VCSPCPass group
VLAN11Users
```

Adding users for user-login authentication

There are three groups of privilege levels:

- Users with privilege levels 1 to 6 have access to privilege 1 level commands.
- Users with privilege 7 to 14 have access to privilege level 1 commands and all show commands.
- Users with privilege level 15 have access to all commands.

When a user logs into a management session on a switch by console, telnet, or SSH and is being authenticated by RADIUS, the RADIUS server needs to be able to indicate to the switch what privilege level to assign to the user's session.

The way that the privilege level is associated with a user is to use the RADIUS attributes. The attributes are configured on RADIUS groups.

Because there are three group of security privilege levels, there will need to be up to three different groups for login users. Each group specifies a different privilege level.

The attributes that need to be configured on the three different RADIUS groups are as follows:

1. For the users with a privilege level of 1-6 use just the RADIUS **attribute Service-Type**, and assign it the value **NAS-Prompt-User**:

```
group users
attribute Service-Type NAS-Prompt-User
```

2. For users with the security privilege of 7-14 use the following two RADIUS attributes:

```
group middle-management
attribute Cisco-AVPair shell:priv-lvl=7
attribute Service-Type NAS-Prompt-User
```

3. User with the administrator security privilege use just the RADIUS **attribute Service-Type**, and assign it the value **Administrative-User**:

```
group admin
attribute Service-Type Administrative-User
```

Since there is not an explicit RADIUS attribute for the users with the security privilege level 7, use **Cisco-AVPair** to specify this user privilege. Also, it is very important that you specify the attribute **Service-Type NAS-Prompt-User** as well, otherwise the following error is generated when a user allocated to this group tries to login into the AlliedWare Plus switch:

```
19:09:14 awplus login[16974]: Invalid user name "tests" in main:698. Abort.
```

The RADIUS Server attribute **NAS-Prompt-User** is used for non-privileged level users as per the RADIUS RFC. This attribute is used for users with security privilege levels of 1 to 6.

Configuring these RADIUS Server attributes is achieved using Local RADIUS Server commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group users
awplus(config-radsrv-group)# attribute Service-Type NAS-Prompt_User
```

See the below sample configuration for an AlliedWare Plus switch acting as the RADIUS Server, with the three different security privileges for **admin**, **middle-management**, and **users** groups:

Output 1: Sample RADIUS Server configuration for three different security privileges:

```
crypto pki trustpoint local
!
crypto pki enroll local
radius-server local
 server enable
 nas 10.1.1.1 key test
 nas 127.0.0.1 key awplus-local-radius-server
 group admin
  attribute Service-Type Administrative-User
 group middle-management
  attribute Cisco-AVPair shell:priv-lvl=7
  attribute Service-Type NAS-Prompt-User
 group users
  attribute Service-Type NAS-Prompt-User
 user test encrypted password UukoSyvxY2v9iWXm8e/JMDJd9iIc3RPyY09lGOb3pA4=
group  users
 user tested encrypted password sEDhM4iJRfJrLhhs+RgjpgkDXtCwuji6AllpApi9EjA=
group admin
 user tests encrypted password il9aIh8JLOT6kHDV+Ix7/8fzyfVpAwRErJg6NPQdJy8=
group middle-management
```

Removing users from the RADIUS users list

To remove the user Tom from the user database of the Local RADIUS server, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no user Tom
```

Creating certificates for single users and all users

As well as using passwords to authenticate users, the Local RADIUS server also supports using x.509 certificates to authenticate users.

Once a user has been added to the user database of the Local RADIUS server, follow the procedure below to create an x.509 certificate for the user, and then export the certificate so that it can be imported into the client device.

Create a certificate for a single user

A certificate for user Tom can be created from the local CA by using the command:

```
awplus# crypto pki enroll local user Tom
```

Create a certificate for all users

Certificates can be created for all currently defined users by using the command:

```
awplus# crypto pki enroll local local-radius-all-users
```

Exporting certificates

User certificates can be exported in PKCS12 format.

To export a certificate for user Tom and upload it to the TFTP server at 192.168.1.1, use the command:

```
awplus# crypto pki export local pkcs12 Tom tftp://192.168.1.1/tomcert.pkcs
```

Assigning multiple instances of a RADIUS attribute

You may want to assign multiple instances of the same RADIUS attribute to a user or group of users. This is done with the **attribute repeated** command.

For example, to configuring multiple **NAS-Filter-Rules** for dynamic Access Control Lists (ACLs) with port authentication, use the following commands:

Step 1: Configure the local RADIUS server

```
awplus# configure terminal
awplus(config)# radius-server local
```

Step 2: Define a group with the required ACL rules.

These ACL rules will to reject IP traffic from 192.168.1.x to any destination except 192.168.2.x

```
awplus(config-radsrv)# group dacl-rule
awplus(config-radsrv-group)# attribute repeated NAS-Filter-Rule "ip:permit ip 192.168.1.0/24 192.168.2.0/24"
awplus(config-radsrv-group)# attribute repeated NAS-Filter-Rule "ip:deny ip 192.168.1.0/24 any"
```

Step 3: Add a user with dynamic ACL rules:

```
awplus(config-radsrv)# user xx-xx-xx-xx-xx-xx password xx-xx-xx-xx-xx-x group dacl-rule
```

Step 4: **Enable the local RADIUS server**

```
awplus(config-radsrv)# server enable
```

Removing multiple instances of the same attribute

Using the **attribute** command without the **repeated** parameter deletes all existing instances of the attribute and creates a new single instance of that attribute. For example, the two instances of **Nas-Filter-Rule** defined before will be replaced with a single instance if the following command is run:

```
awplus(config-radsrv-group)# attribute NAS-Filter-Rule "ip:deny ip any
any"
```

To delete a specific instance of an attribute specify the attribute's name and value, for example:

```
awplus(config-radsrv-group)# no attribute NAS-Filter-Rule "ip:deny ip
192.168.1.0/24 any"
```

To delete all instances of an attribute, use the **no** variant of the attribute command:

```
awplus(config-radsrv-group)# no attribute NAS-Filter-Rule
```

Promiscuous mode

Under normal operation, in a port under port authentication control, a supplicant will only be authorized if its credentials exist in the RADIUS user database, and the credentials match the data supplied by the supplicant.

In **promiscuous mode**, a supplicant will be authorized if the credentials match as above, however, the supplicant will also be authorized if the credentials do **not** appear in the RADIUS user database.

This allows the administrator to be promiscuous in accepting supplicants.

Once authorized, the administrator can reject the supplicant or modify some of the supplicant's access characteristics (e.g., VLAN) by updating the user database.

Promiscuous mode:

- is relevant for port authentication ports protected by **mac-auth** only.
- is configured by the command: **auth-mac-promiscuous**
- requires that the existing **auth radius send service-type** global configuration is configured on the authenticator(s). This allows the RADIUS server to determine if an incoming request has come from a port protected by mac-auth.

```
awplus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ar4050(config)#radius-server local
ar4050(config-radsrv)#auth-mac-promiscuous
```

If Promiscuous mode is configured on the RADIUS server:

- An Access-Request for a user unknown to the RADIUS server user database will result in an Access-Accept (user will be authorized).
- An Access-Request for a user known to the RADIUS server user database with an incorrect password will result in an Access-Reject.
- An Access-Request for a user known to the RADIUS server user database with the correct password will result in an Access-Accept.
- An Access-Request for a user known to the RADIUS server user database with the correct password but the user has been set to reject will result in an Access-Reject.

So what's the point? The idea is that the users are let in but then their status in the network can be modified by updating the RADIUS user database then bouncing the port with a CoA port-bounce message.

You can use the **show radius local-server statistics** command to show users that exist in the local RADIUS servers logging directory but do not exist as users in the local RADIUS server user database. These users exist either because the user has been authorized in Promiscuous mode (these entries will show in the output Successes statistics) or the user has failed authorization.

```
awplus# show radius local-server statistics
Server status      : Run (administrative status is enable)
Enabled methods    : MAC EAP-MD5 EAP-TLS EAP-PEAP
Available methods  : MAC EAP-MD5 EAP-TLS EAP-PEAP
EAP trustpoints    : local
Promiscuous mode   : Enabled
Successes              :7              Unknown NAS             :0
Failed Logins          :0              Invalid packet from NAS:0
Internal Error         :0              Unknown Error           :0

NAS : 127.0.0.1
Successes              :7              Shared key mismatch     :0
Failed Logins          :0              Unknown RADIUS message  :0
Unknown EAP message    :0              Unknown EAP auth type   :0
Corrupted packet       :0


Users present in the User Database:
Username                                Successes  Failures  Last Interaction
                                                             Local time (+00:00)
00-00-00-00-00-01                               0         0  -
00-00-00-00-00-02                               0         0  -
00-15-65-3f-d9-42                               0         0  -
00-90-0b-45-07-e4                               4         0  09 Jan 2024 00:32:24
graeme                                          2         0  09 Jan 2024 00:31:52
graemet                                         0         0  -
user1                                           0         0  -
user1dynvlan                                    0         0  -
user2dynvlan                                    0         0  -

Users NOT present in the User Database:
Username                                Successes  Failures  Last Interaction
                                                             Local time (+00:00)
00-90-0b-45-07-e2                               1         0  09 Jan 2024 00:31:50
```

Configuring a Secure Local RADIUS Server

AlliedWare Plus devices can be configured as a Transport Layer Security (TLS) secured RADIUS server. The RADIUS traffic between the RADIUS server and NAS will be encrypted by TLS to improve security on the network. The server includes the RADIUS and RadSec services to provide secure authentication to the NAS clients.

Creating a trustpoint for RadSec TLS certificates

In TLS encryption, the server and client hold certificates signed by a Certification Authority (CA). In AlliedWare Plus, certificates and keys are stored in containers called **trustpoints**. Within a trustpoint, the certificates form a chain that ends in a single Root CA certificate. The Root CA certificate's private key is also stored in the trustpoint.

It is possible to specify multiple trustpoints for use with a RADIUS server. The RADIUS server will use the first trustpoint's CA and server certificates when asserting its identity to the peer device on a TLS connection. It uses certificates from all the specified trustpoints to verify connections received from peers.

Typically, both the local RADIUS server and the peer devices use the same root certificate, so only one trustpoint is needed. However, it is possible for the local server's certificate to be signed by one CA and the peer device's certificate to be signed by a different CA. In this situation, you should configure the server to use two trustpoints. Configure the one containing the local server's certificate first.

For more information about trustpoints, see the Public Key Infrastructure (PKI) Feature Overview and Configuration Guide.

Step 1: **Create a trustpoint to store the certificates**

Create a trustpoint and enters the trustpoint configuration mode. The **enrollment terminal** command allows you to copy and paste the certificate key contents via the console.

```
awplus# configure terminal
awplus(config)# crypto pki trustpoint my_trustpoint
awplus(ca-trustpoint)# enrollment terminal
awplus(ca-trustpoint)# end
```

Step 2: **Import the CA public certificates**

Use the **crypto pki authenticate** command to import the CA root public certificate. If necessary, you can run this command multiple times to import additional CA certificates.

```
awplus# crypto pki authenticate my_trustpoint
```

```
Paste the certificate PEM file into the terminal.
Type "abort" to cancel.
```

Step 3: **Generate the certificate signing request (CSR)**

After importing the CA certificate, the NAS will generate the certificate signing request (CSR). Copy the content from the terminal and use this to sign the certificate from the CA.

```
awplus# crypto pki enroll my_trustpoint
```

```
Using private key "server-default"...
Cut and paste this request to the certificate authority:
-----------------------------------------------------------------
-----BEGIN CERTIFICATE REQUEST-----
MIICuzCCAaMCAQAwKzEYMBYGA1UECgwPQWxsaWVkV2FyZSBQbHVzMQ8wDQYDVQQD
DAZhd3BsdXMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDByySloBrJ
<output omitted>
mG/ur7qPNQQJI7B9sBuJgv96VkRSVqODy4L810oZ6gNqEGAK+GdcRy1E+scKCi2e
bESR5YoDc13o5glGmJY6qGHKRxZYpRG+x17v0thBAQ==
-----END CERTIFICATE REQUEST-----
-----------------------------------------------------------------
```

Note: During certificate validation the **Extended Key Usage** field in the certificate should be set and the purpose should be correct (**serverAuth** in the RADIUS server certificate and **clientAuth** in the NAS certificate). If this is not done then the connection will not be established and an error message “auth.err awplus radsecproxy: Certificate extendedKeyUsage check failed” is generated.

Step 4: **Import the NAS certificate**

Import the signed certificate from the CA in PEM format.

```
awplus# crypto pki import my_trustpoint pem
```

```
Paste the certificate PEM file into the terminal.
Type "abort" to cancel.
```

The NAS certificate is now is set and can be used to secure traffic.

Enabling the Local RADIUS Server

The RadSec Proxy application will act as a TLS translator to communicate with a remote NAS running RadSec Proxy and Local RADIUS Server.

Step 5: **Enable the local RADIUS server**

Enable the local RADIUS server.

```
awplus(config)# radius-server local
awplus(config-radsrv)# server enable
```

Enabling the local RADIUS server automatically initializes the internal Certificate Authority on the NAS. We recommend that you use an external CA for the certificates. To do this, disable the internal CA trustpoint and specify the trustpoint created in **Creating a trustpoint for RadSec TLS certificates**.

```
awplus(config-radsrv)# no server trustpoint local
awplus(config-radsrv)# server trustpoint my_trustpoint
awplus(config-radsrv)# exit
```

Step 6: Add the NAS to the local RADIUS server

Add the NAS to the list of authenticators that may send authentication requests to the local RADIUS server.

```
awplus(config)# radius-server local
awplus(config-radsrv)# nas 127.0.0.1 key awplus-local-radius-server
```

Note: The key **awplus-local-radius-server** is a pre-defined component that can be used for internal exchanges between the NAS's RADIUS client and its RADIUS server.

Configuring the RadSec Proxy server

Step 7: Enable the RadSec Proxy local server application

Enable the RadSec Proxy local server application and enter RadSec Proxy local server configuration mode.

```
awplus(config)# radius-secure-proxy local-server
awplus(config-radsecproxy-srv)#
```

Step 8: Configure NAS and trustpoint

The **client** command adds a RadSec client by either host name or IP address to the RadSec Proxy local server application.

```
awplus(config-radsecproxy-srv)# client 127.0.0.1
awplus(config-radsecproxy-srv)# client trustpoint my_trustpoint
```

Note that if a host name is used then it must be resolvable to an IPv4 address by DNS, otherwise a connection to the client will not be established.

The host name or IP address must match the name provided in the client's X.509 certificate, or the connection will fail. You can configure the client to bypass this check by adding the parameters **name-check off** to this command.

To use multiple trustpoints, you can specify more than one trustpoint in the command, or execute the command multiple times.

Step 9: Complete RADIUS configuration

You can now configure the RADIUS user database, user group, attributes, etc. Refer to related section of **Configuring the Local RADIUS Server**.

Defined RADIUS attributes list

This section contains a full list of valid attributes and pre-defined values that may be used in conjunction with the **attribute** command, to show or configure defined RADIUS attributes.

More detailed information can be found in the following RFCs, defining the attributes and values for RADIUS server:

- RFC2865: Remote Authentication Dial In User Service (RADIUS)
- RFC2866: RADIUS Accounting
- RFC2867: RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC2868: RADIUS Attributes for Tunnel Protocol Support
- RFC2869: RADIUS Extensions
- RFC3162: RADIUS and IPv6
- RFC3576: Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
- RFC3580: IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
- RFC4072: Diameter Extensible Authentication Protocol (EAP) Application
- RFC4372: Chargeable User Identity
- RFC4603: Additional Values for the NAS-Port-Type Attribute
- RFC4675: RADIUS Attributes for Virtual LAN and Priority Support
- RFC4679: DSL Forum Vendor-Specific RADIUS Attributes
- RFC4818: RADIUS Delegated-IPv6-Prefix Attribute
- RFC4849: RADIUS Filter Rule Attribute
- RFC5090: RADIUS Extension for Digest Authentication
- RFC5176: Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
- RFC5447: Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction
- RFC5580: Carrying Location Objects in RADIUS and Diameter
- RFC5607: Remote Authentication Dial-In User Service (RADIUS) Authorization for Network Access Server (NAS) Management
- RFC5904: RADIUS Attributes for IEEE 802.16 Privacy Key Management Version 1 (PKMv1) Protocol Support
- RFC6519: RADIUS Extensions for Dual-Stack Lite
- RFC6572: RADIUS Support for Proxy Mobile IPv6

- RFC6677: Channel-Binding Support for Extensible Authentication Protocol (EAP) Methods
- RFC6911: RADIUS Attributes for IPv6 Access Networks
- RFC6929: Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions
- RFC6930: RADIUS Attribute for IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)
- RFC7055: A GSS-API Mechanism for the Extensible Authentication Protocol
- RFC7155: Diameter Network Access Server Application
- RFC7268: RADIUS Attributes for IEEE 802 Networks
- RFC7499: Support of Fragmentation of RADIUS Packets
- RFC7930: Larger Packets for RADIUS over TCP

Standard attributes

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
1	User-Name	string
2	User-Password	string
3	CHAP-Password	octets (Hexadecimal string followed by 0x)
4	NAS-IP-Address	ipaddr (IPv4 address)
5	NAS-Port	Integer
6	Service-Type	Integer. Valid values are: ■ Administrative-User (6) ■ Authenticate-Only (8) ■ Authorize-Only (17) ■ Callback-Administrative (11) ■ Callback-Framed-User (4) ■ Callback-Login-User (3) ■ Callback-NAS-Prompt (9) ■ Call-Check (10) ■ Framed-Management (18) ■ Framed-User (2) ■ Login-User (1) ■ NAS-Prompt-User (7) ■ Outbound-User (5)
7	Framed-Protocol	Integer. Valid values are: ■ ARAP (3) ■ Gandalf-SLML (4) ■ PPP (1) ■ SLIP (2) ■ X.75-Synchronous (6) ■ Xylogics-IPX-SLIP (5)
8	Framed-IP-Address	ipaddr (IPv4 address)
9	Framed-IP-Netmask	ipaddr (IPv4 address)

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
10	Framed-Routing	integer. Valid values are: ■ Broadcast (1) ■ Broadcast-Listen (3) ■ Listen (2) ■ None (0)
11	Filter-Id	string
12	Framed-MTU	Integer
13	Framed-Compression	Integer. Valid values are: ■ IPX-Header-Compression (2) ■ None (0) ■ Stac-LZS (3) ■ Van-Jacobson-TCP-IP (1)
14	Login-IP-Host	IP Address
15	Login-Service	Integer. Valid values are: ■ LAT (4) ■ PortMaster (3) ■ Rlogin (1) ■ TCP-Clear (2) ■ TCP-Clear-Quiet (8) ■ Telnet (0) ■ X25-PAD (5) ■ X25-T3POS (6)
16	Login-TCP-Port	Integer. Valid values are: ■ Rlogin (513) ■ Rsh (514) ■ Telnet (23)
18	Reply-Message	string
19	Callback-Number	string
20	Callback-Id	string
22	Framed-Route	string
23	Framed-IPX-Network	IP address
24	State	octets (Hexadecimal string followed by 0x)
25	Class	octets (Hexadecimal string followed by 0x)
26	Vendor-Specific	Use the Vendor-specific Attribute Name. For valid values, see "Vendor-specific RADIUS attributes" on page 12.
27	Session-Timeout	Integer
28	Idle-Timeout	Integer
29	Termination-Action	Integer. Valid values are: ■ Default (0) ■ RADIUS-Request (1)
30	Called-Station-Id	string
31	Calling-Station-Id	string
32	NAS-Identifier	string
33	Proxy-State	octets (Hexadecimal string followed by 0x)

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
34	Login-LAT-Service	string
35	Login-LAT-Node	string
36	Login-LAT-Group	octets (Hexadecimal string followed by 0x)
37	Framed-AppleTalk-Link	Integer
38	Framed-AppleTalk-Network	Integer
39	Framed-AppleTalk-Zone	string
40	Acct-Status-Type	Integer. Valid values are: ■ Accounting-Off (8) ■ Accounting-On (7) ■ Alive (3) ■ Failed (15) ■ Interim-Update (3) ■ Start (1) ■ Stop (2) ■ Tunnel-Link-Reject (14) ■ Tunnel-Link-Start (12) ■ Tunnel-Link-Stop (13) ■ Tunnel-Reject (11) ■ Tunnel-Start (9) ■ Tunnel-Stop (10)
41	Acct-Delay-Time	Integer
42	Acct-Input-Octets	Integer
43	Acct-Output-Octets	Integer
44	Acct-Session-Id	string
45	Acct-Authentic	Integer. Valid values are: ■ Diameter (4) ■ Local (2) ■ RADIUS (1) ■ Remote (3)
46	Acct-Session-Time	Integer
47	Acct-Input-Packets	Integer
48	Acct-Output-Packets	Integer

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
49	Acct-Terminate-Cause	Integer. Valid values are: ■ Admin-Reboot (7) ■ Admin-Reset (6) ■ Callback (16) ■ Host-Request (18) ■ Idle-Timeout (4) ■ Lost-Carrier (2) ■ Lost-Service (3) ■ NAS-Error (9) ■ NAS-Reboot (11) ■ NAS-Request (10) ■ Port-Disabled (22) ■ Port-Error (8) ■ Port-Preempted (13) ■ Port-Reinit (21) ■ Port-Suspended (14) ■ Port-Unneeded (12) ■ Reauthentication-Failure (20) ■ Service-Unavailable (15) ■ Session-Timeout (5) ■ Supplicant-Restart (19) ■ User-Error (17) ■ User-Request (1)
50	Acct-Multi-Session-Id	string
51	Acct-Link-Count	Integer
52	Acct-Input-Gigawords	Integer
53	Acct-Output-Gigawords	Integer
55	Event-Timestamp	date (Not supported)
56	Egress-VLANID	Integer
57	Ingress-Filters	Integer. Valid values are: ■ Disabled (2) ■ Enabled (1)
58	Egress-VLAN-Name	string
59	User-Priority-Table	octets (Hexadecimal string followed by 0x)
60	CHAP-Challenge	octets (Hexadecimal string followed by 0x)

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
61	NAS-Port-Type	Integer. Valid values are: ■ ADSL-CAP (12) ■ ADSL-DMT (13) ■ Async (0) ■ Cable (17) ■ Ethernet (15) ■ FDDI (21) ■ G.3-Fax (10) ■ HDLC-Clear-Channel (7) ■ IDSL (14) ■ ISDN (2) ■ ISDN-V110 (4) ■ ISDN-V120 (3) ■ PIAFS (6) ■ PPPoA (30) ■ PPPoEoA (31) ■ PPPoEoE (32) ■ PPPoEoQinQ (34) ■ PPPoEoVLAN (33) ■ SDSL (11) ■ Sync (1) ■ Token-Ring (20) ■ Virtual (5) ■ Wireless-802.11 (19) ■ Wireless-Other (18) ■ X.25 (8) ■ X.75 (9) ■ xDSL (16)
62	Port-Limit	Integer
63	Login-LAT-Port	string
64	Tunnel-Type	Integer. Valid values are: ■ AH (6) ■ ATMP (4) ■ DVS (11) ■ ESP (9) ■ GRE (10) ■ IP (7) ■ IP-in-IP (12) ■ L2F (2) ■ L2TP (3) ■ MIN-IP (8) ■ PPTP (1) ■ VLAN (13) ■ VTP (5)

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
65	Tunnel-Medium-Type	Integer. Valid values are: ■ Appletalk (12) ■ Banyan-Vines (14) ■ BBN-1822 (5) ■ DecNet-IV (13) ■ E.163 (7) ■ E.164 (8) ■ E.164-NSAP (15) ■ F.69 (9) ■ HDLC (4) ■ IEEE-802 (6) ■ IP (1) ■ IPv4 (1) ■ IPv6 (2) ■ IPX (11) ■ NSAP (3) ■ X.121 (10)
66	Tunnel-Client-Endpoint	string
67	Tunnel-Server-Endpoint	string
68	Acct-Tunnel-Connection	string
69	Tunnel-Password	string
70	ARAP-Password	octets (Hexadecimal string followed by 0x)
71	ARAP-Features	octets (Hexadecimal string followed by 0x)
72	ARAP-Zone-Access	Integer. Valid values are: ■ Default-Zone (1) ■ Zone-Filter-Exclusive (4) ■ Zone-Filter-Inclusive (2)
73	ARAP-Security	Integer
74	ARAP-Security-Data	string
75	Password-Retry	integer
76	Prompt	integer. Valid values are: ■ Echo (1) ■ No-Echo (0)
77	Connect-Info	string
78	Configuration-Token	string
79	EAP-Message	octets (Hexadecimal string followed by 0x)
80	Message-Authenticator	octets (Hexadecimal string followed by 0x)
81	Tunnel-Private-Group-Id	string
82	Tunnel-Assignment-Id	string
83	Tunnel-Preference	Integer
84	ARAP-Challenge-Response	octets (Hexadecimal string followed by 0x)
85	Acct-Interim-Interval	Integer
86	Acct-Tunnel-Packets-Lost	Integer
87	NAS-Port-Id	string

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
88	Framed-Pool	string
89	Chargeable-User-Identity	string
90	Tunnel-Client-Auth-Id	string
91	Tunnel-Server-Auth-Id	string
92	NAS-Filter-Rule	string
94	Originating-Line-Info	octets[2]
95	NAS-IPv6-Address	ipv6addr (IPv6 address)
96	Framed-Interface-Id	ifid (Not supported)
97	Framed-IPv6-Prefix	ipv6prefix (Not supported)
98	Login-IPv6-Host	ipv6addr (IPv6 address)
99	Framed-IPv6-Route	string
100	Framed-IPv6-Pool	string
101	Error-Cause	Integer. Valid values are: ■ Administratively-Prohibited (501) ■ Invalid-Attribute-Value (407) ■ Invalid-EAP-Packet (202) ■ Invalid-Request (404) ■ Missing-Attribute (402) ■ Multiple-Session-Selection-Unsupported (508) ■ NAS-Identification-Mismatch (403) ■ Proxy-Processing-Error (505) ■ Proxy-Request-Not-Routable (502) ■ Request-Initiated (507) ■ Residual-Context-Removed (201) ■ Resources-Unavailable (506) ■ Session-Context-Not-Found (503) ■ Session-Context-Not-Removable (504) ■ Unsupported-Attribute (401) ■ Unsupported-Extension (406) ■ Unsupported-Service (405)
102	EAP-Key-Name	string
123	Delegated-IPv6-Prefix	ipv6prefix
124	MIP6-Feature-Vector	octets (Hexadecimal string followed by 0x)
125	MIP6-Home-Link-Prefix	ipv6prefix
126	Operator-Name	string
127	Location-Information	octets (Hexadecimal string followed by 0x)
128	Location-Data	octets (Hexadecimal string followed by 0x)
129	Basic-Location-Policy-Rules	octets (Hexadecimal string followed by 0x)
130	Extended-Location-Policy-Rules	octets (Hexadecimal string followed by 0x)
131	Location-Capable	Integer. Valid values are: ■ Civic-Location (1) ■ Geo-Location (2) ■ NAS-Location (8) ■ Users-Location (4)

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
132	Requested-Location-Info	Integer. Valid values are: ■ Civic-Location (1) ■ Future-Requests (16) ■ Geo-Location (2) ■ NAS-Location (8) ■ None (32) ■ Users-Location (4)
133	Framed-Management	Integer. Valid values are: ■ FTP (4) ■ Netconf (3) ■ RCP (7) ■ SCP (8) ■ SFTP (6) ■ SNMP (1) ■ TFTP (5)
134	Management-Transport-Protection	Integer. Valid values are: ■ Integrity-Confidentiality-Protection (3) ■ Integrity-Protection (2) ■ No-Protection (1)
135	Management-Policy-Id	string
136	Management-Privilege-Level	Integer
137	PKM-SS-Cert	octets (Hexadecimal string followed by 0x)
138	PKM-CA-Cert	octets (Hexadecimal string followed by 0x)
139	PKM-Config-Settings	octets (Hexadecimal string followed by 0x)
140	PKM-Cryptosuite-List	octets (Hexadecimal string followed by 0x)
141	PKM-SAID	short
142	PKM-SA-Descriptor	octets (Hexadecimal string followed by 0x)
143	PKM-Auth-Key	octets (Hexadecimal string followed by 0x)
144	DS-Lite-Tunnel-Name	string
145	Mobile-Node-Identifier	octets (Hexadecimal string followed by 0x)
146	Service-Selection	string
147	PMIP6-Home-LMA-IPv6-Address	ipv6addr
148	PMIP6-Visited-LMA-IPv6-Address	ipv6addr
149	PMIP6-Home-LMA-IPv4-Address	ipaddr
150	PMIP6-Visited-LMA-IPv4-Address	ipaddr
151	PMIP6-Home-HN-Prefix	ipv6prefix
152	PMIP6-Visited-HN-Prefix	ipv6prefix
153	PMIP6-Home-Interface-ID	interface identifier
154	PMIP6-Visited-Interface-ID	interface identifier
155	PMIP6-Home-IPv4-HoA	ipv4prefix

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
156	PMIP6-Visited-IPv4-HoA	ipv4prefix
157	PMIP6-Home-DHCP4-Server-Address	ipaddr
158	PMIP6-Visited-DHCP4-Server-Address	ipaddr
159	PMIP6-Home-DHCP6-Server-Address	ipv6addr
160	PMIP6-Visited-DHCP6-Server-Address	ipv6addr
161	PMIP6-Home-IPv4-Gateway	ipaddr
162	PMIP6-Visited-IPv4-Gateway	ipaddr
163	EAP-Lower-Layer	Integer. Valid values are: ■ GSS-API (8) ■ IEEE-802.16e (4) ■ IEEE-802.1X-No-Preauth (2) ■ IEEE-802.1X-Preauth (3) ■ IKEv2 (5) ■ PANA-No-Preauth (7) ■ PANA-Preauth (9) ■ PPP (6) ■ Wired-IEEE-802.1X (1)
164	GSS-Acceptor-Service-Name	string
165	GSS-Acceptor-Host-Name	string
166	GSS-Acceptor-Service-Specifics	string
167	GSS-Acceptor-Realm-Name	string
168	Framed-IPv6-Address	ipv6addr
169	DNS-Server-IPv6-Address	ipv6addr
170	Route-IPv6-Information	ipv6prefix
171	Delegated-IPv6-Prefix-Pool	string
172	Stateful-IPv6-Address-Pool	string
173	IPv6-6rd-Configuration	tlv
173.1	IPv6-6rd-IPv4MaskLen	integer
173.2	IPv6-6rd-Prefix	ipv6prefix
173.3	IPv6-6rd-BR-IPv4-Address	ipaddr
174	Allowed-Called-Station-Id	string
175	EAP-Peer-Id	octets
176	EAP-Server-Id	octets
177	Mobility-Domain-Id	integer
178	Preauth-Timeout	integer
179	Network-Id-Name	octets
180	EAPoL-Announcement	octets

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
181	WLAN-HESSID	string
182	WLAN-Venue-Info	integer
183	WLAN-Venue-Language	octets[3]
184	WLAN-Venue-Name	string
185	WLAN-Reason-Code	integer
186	WLAN-Pairwise-Cipher	integer
187	WLAN-Group-Cipher	integer
188	WLAN-AKM-Suite	integer
189	WLAN-Group-Mgmt-Cipher	integer
190	WLAN-RF-Band	integer
241	Extended-Attribute-1	extended
241.1	Frag-Status	Integer. Valid values are: ■ Fragmentation-Supported (1) ■ More-Data-Pending (2) ■ More-Data-Request (3) ■ Reserved (0)
241.2	Proxy-State-Length	integer
241.3	Response-Length	integer
241.4	Original-Packet-Code	integer
241.26	Extended-Vendor-Specific-1	evs
242	Extended-Attribute-2	extended
242.26	Extended-Vendor-Specific-2	evs
243	Extended-Attribute-3	extended
243.26	Extended-Vendor-Specific-3	evs
244	Extended-Attribute-4	extended
244.26	Extended-Vendor-Specific-4	evs
245	Extended-Attribute-5	long-extended
245.26	Extended-Vendor-Specific-5	evs
246	Extended-Attribute-6	long-extended
246.26	Extended-Vendor-Specific-6	evs

Vendor-specific RADIUS attributes

VENDOR-SPECIFIC ATTRIBUTE NAME	VALUE TYPE/PRE-DEFINED VALUE
Access-Loop-Encapsulation	octets
Actual-Data-Rate-Downstream	integer
Actual-Data-Rate-Upstream	integer
Actual-Interleaving-Delay-Downstream	integer
Actual-Interleaving-Delay-Upstream	integer

VENDOR-SPECIFIC ATTRIBUTE NAME	VALUE TYPE/PRE-DEFINED VALUE
ADSL-Agent-Circuit-Id	octets
ADSL-Agent-Remote-Id	octets
DSL-Forum-DHCP-Vendor-Specific	tlv
Attainable-Data-Rate-Downstream	integer
Attainable-Data-Rate-Upstream	integer
call-id	string
Cisco-Abort-Cause	string
Cisco-Account-Info	string
Cisco-Assign-IP-Pool	integer
Cisco-AVPair	string
Cisco-Call-Filter	integer
Cisco-Call-Type	string
Cisco-Command-Code	string
Cisco-Control-Info	string
Cisco-Data-Filter	integer
Cisco-Data-Rate	integer
Cisco-Disconnect-Cause	Integer. Valid values are: ■ No-Reason - 0 ■ No-Disconnect - 1 ■ Unknown - 2 ■ Call-Disconnect - 3 ■ CLID-Authentication-Failure - 4 ■ No-Modem-Available- 9 ■ No-Carrier - 10 ■ Lost-Carrier - 11 ■ No-Detected-Result-Codes - 2 ■ User-Ends-Session - 20 ■ Idle-Timeout - 21 ■ Exit-Telnet-Session - 22 ■ No-Remote-IP-Addr - 23 ■ Exit-Raw-TCP - 24 ■ Password-Fail - 25 ■ Raw-TCP-Disabled - 26 ■ Control-C-Detected - 27 ■ EXEC-Program-Destroyed - 28 ■ Close-Virtual-Connection - 29 ■ End-Virtual-Connection - 30

VENDOR-SPECIFIC ATTRIBUTE NAME	VALUE TYPE/PRE-DEFINED VALUE
Cisco-Disconnect-Cause (continued)	■ Exit-Rlogin - 31 ■ Invalid-Rlogin-Option - 32 ■ Insufficient-Resources - 33 ■ Timeout-PPP-LCP - 40 ■ Failed-PPP-LCP-Negotiation - 41 ■ Failed-PPP-PAP-Auth-Fail - 42 ■ Failed-PPP-CHAP-Auth - 43 ■ Failed-PPP-Remote-Auth - 44 ■ PPP-Remote-Terminate - 45 ■ PPP-Closed-Event - 46 ■ NCP-Closed-PPP - 47 ■ MP-Error-PPP - 48 ■ PPP-Maximum-Channels - 49 ■ Tables-Full - 50 ■ Resources-Full - 51 ■ Invalid-IP-Address - 52 ■ Bad-Hostname - 53 ■ Bad-Port - 54 ■ Reset-TCP - 60 ■ TCP-Connection-Refused - 61 ■ Timeout-TCP - 62 ■ Foreign-Host-Close-TCP - 63 ■ TCP-Network-Unreachable - 64 ■ TCP-Host-Unreachable - 65 ■ TCP-Network-Admin-Unreachable - 66 ■ TCP-Port-Unreachable - 67 ■ Session-Timeout - 100 ■ Session-Failed-Security - 101 ■ Session-End-Callback - 102 ■ Invalid-Protocol - 120 ■ RADIUS-Disconnect - 150 ■ Local-Admin-Disconnect - 151 ■ SNMP-Disconnect - 152 ■ V110-Retries - 160 ■ PPP-Authentication-Timeout - 170 ■ Local-Hangup - 180 ■ Remote-Hangup - 185 ■ T1-Quiesced - 190 ■ Call-Duration - 195 ■ VPN-User-Disconnect - 600 ■ VPN-Carrier-Loss - 601 ■ VPN-No-Resources - 602 ■ VPN-Bad-Control-Packet - 603 ■ VPN-Admin-Disconnect - 604 ■ VPN-Tunnel-Shut - 605 ■ VPN-Local-Disconnect - 606 ■ VPN-Session-Limit - 607 ■ VPN-Call-Redirect - 608
Cisco-Email-Server-Ack-Flag	string
Cisco-Email-Server-Address	string
Cisco-Fax-Account-Id-Origin	string
Cisco-Fax-Auth-Status	string
Cisco-Fax-Connect-Speed	string

VENDOR-SPECIFIC ATTRIBUTE NAME	VALUE TYPE/PRE-DEFINED VALUE
Cisco-Fax-Coverpage-Flag	string
Cisco-Fax-Dsn-Address	string
Cisco-Fax-Dsn-Flag	string
Cisco-Fax-Mdn-Address	string
Cisco-Fax-Mdn-Flag	string
Cisco-Fax-Modem-Time	string
Cisco-Fax-Msg-Id	string
Cisco-Fax-Pages	string
Cisco-Fax-Process-Abort-Flag	string
Cisco-Fax-Recipient-Count	string
Cisco-Gateway-Id	string
Cisco-Idle-Limit	integer
Cisco-IP-Direct	integer
Cisco-IP-Pool-Definition	string
Cisco-Link-Compression	integer
Cisco-Maximum-Channels	integer
Cisco-Maximum-Time	integer
Cisco-Multilink-ID	integer
Cisco-NAS-Port	string
Cisco-Num-In-Multilink	integer
Cisco-Policy-Down	string
Cisco-Policy-Up	string
Cisco-Port-Used	string
Cisco-PPP-Async-Map	integer
Cisco-PPP-VJ-Slot-Comp	integer
Cisco-Pre-Input-Octets	integer
Cisco-Pre-Input-Packets	integer
Cisco-Pre-Output-Octets	integer
Cisco-Pre-Output-Packets	integer
Cisco-PreSession-Time	integer
Cisco-PW-Lifetime	integer
Cisco-Route-IP	integer
Cisco-Service-Info	string
Cisco-Subscriber-Password	string
Cisco-Target-Util	integer
Cisco-Xmit-Rate	integer
dsp-id	string

VENDOR-SPECIFIC ATTRIBUTE NAME	VALUE TYPE/PRE-DEFINED VALUE
gw-final-xlated-cdn	string
gw-final-xlated-cgn	string
gw-rxd-cdn	string
gw-rxd-cgn	string
h323-billing-model	string
h323-call-origin	string
h323-call-type	string
h323-conf-id	string
h323-connect-time	string
h323-credit-amount	string
h323-credit-time	string
h323-currency	string
h323-disconnect-cause	string
h323-disconnect-time	string
h323-gw-id	string
h323-incoming-conf-id	string
h323-preferred-lang	string
h323-prompt-id	string
h323-redirect-ip-address	string
h323-redirect-number	string
h323-remote-address	string
h323-return-code	string
h323-setup-time	string
h323-time-and-day	string
h323-voice-quality	string
incoming-req-uri	string
IWF-Session	octets
Maximum-Data-Rate-Downstream	integer
Maximum-Data-Rate-Upstream	integer
Maximum-Interleaving-Delay-Downstream	integer
Maximum-Interleaving-Delay-Upstream	integer
method	string
Minimum-Data-Rate-Downstream	integer
Minimum-Data-Rate-Downstream-Low-Power	integer
Minimum-Data-Rate-Upstream	integer
Minimum-Data-Rate-Upstream-Low-Power	integer

VENDOR-SPECIFIC ATTRIBUTE NAME	VALUE TYPE/PRE-DEFINED VALUE
MS-Acct-Auth-Type	integer. Valid values are: ■ CHAP - 2 ■ EAP - 5 ■ MS-CHAP-1 - 3 ■ MS-CHAP-2 - 4 ■ PAP - 1
MS-Acct-EAP-Type	integer. Valid values are: ■ Generic-Token-Card - 6 ■ MD5 - 4 ■ OTP - 5 ■ TLS - 13
MS-AFW-Protection-Level	integer. Valid values are: ■ HECP-Response-Sign-And-Encrypt - 2 ■ HECP-Response-Sign-Only - 1
MS-AFW-Zone	integer. Valid values are: ■ MS-AFW-Zone-Boundary-Policy - 1 ■ MS-AFW-Zone-Protected-Policy - 3 ■ MS-AFW-Zone-Unprotected-Policy - 2
MS-ARAP-PW-Change-Reason	integer. Valid values are: ■ Admin-Requires-Password-Change - 3 ■ Expired-Password - 2 ■ Just-Change-Password - 1 ■ Password-Too-Short - 4
MS-BAP-Usage	integer. Valid values are: ■ Allowed - 1 ■ Not-Allowed - 0 ■ Required - 2
MS-CHAP2-CPW	octets
MS-CHAP2-Response	octets
MS-CHAP2-Success	octets
MS-CHAP-Challenge	octets
MS-CHAP-CPW-1	octets
MS-CHAP-CPW-2	octets
MS-CHAP-Domain	string
MS-CHAP-Error	string
MS-CHAP-LM-Enc-PW	octets
MS-CHAP-MPPE-Keys	octets
MS-CHAP-NT-Enc-PW	octets
MS-CHAP-Response	octets
MS-Extended-Quarantine-State	integer. Valid values are: ■ Infected - 2 ■ No-Data - 4 ■ Transition - 1 ■ Unknown - 3
MS-Filter	octets

VENDOR-SPECIFIC ATTRIBUTE NAME	VALUE TYPE/PRE-DEFINED VALUE
MS-HCAP-Location-Group-Name	string
MS-HCAP-User-Groups	string
MS-HCAP-User-Name	string
MS-Identity-Type	integer. Valid values are: ■ Ignore-User-Lookup-Failure - 2 ■ Machine-Health-Check - 1
MS-IPv4-Remediation-Servers	octets
MS-IPv6-Filter	octets
MS-IPv6-Remediation-Servers	octets
MS-Link-Drop-Time-Limit	integer
MS-Link-Utilization-Threshold	integer
MS-Machine-Name	string
MS-MPPE-Encryption-Policy	integer. Valid values are: ■ Encryption-Allowed - 1 ■ Encryption-Required - 2
MS-MPPE-Encryption-Type	octets
MS-MPPE-Encryption-Types	integer. Valid values are: ■ RC4-40bit-Allowed - 1 ■ RC4-40or128-bit-Allowed - 6 ■ RC4-128bit-Allowed- 2
MS-MPPE-Recv-Key	octets
MS-MPPE-Send-Key	octets
MS-Network-Access-Server-Type	integer. Valid values are: ■ DHCP-Server - 3 ■ HCAP-Server - 6 ■ HRA - 5 ■ Remote-Access-Server - 2 ■ Terminal-Server-Gateway - 1 ■ Unspecified - 0 ■ Wireless-Access-Point - 4
MS-New-ARAP-Password	octets
MS-Old-ARAP-Password	octets
MS-Primary-DNS-Server	ipaddr
MS-Primary-NBNS-Server	ipaddr
MS-Quarantine-Grace-Time	integer
MS-Quarantine-IPFilter	octets
MS-Quarantine-Session-Timeout	integer
MS-Quarantine-SOH	octets
MS-Quarantine-State	integer. Valid values are: ■ Full-Access - 0 ■ Probation - 2 ■ Quarantine - 1
MS-Quarantine-User-Class	string

VENDOR-SPECIFIC ATTRIBUTE NAME	VALUE TYPE/PRE-DEFINED VALUE
MS-RAS-Client-Name	string
MS-RAS-Client-Version	string
MS-RAS-Correlation	octets
MS-RAS-Vendor	integer
MS-RAS-Version	string
MS-RNAP-Not-Quarantine-Capable	integer. Valid values are: ■ SoH-Not-Sent - 1 ■ SoH-Sent - 0
MS-Secondary-DNS-Server	ipaddr
MS-Secondary-NBNS-Server	ipaddr
MS-Service-Class	string
MS-TSG-Device-Redirection	integer
MS-User-IPv4-Address	ipaddr
MS-User-IPv6-Address	ipv6addr
MS-User-Security-Identity	string
next-hop-dn	string
next-hop-ip	string
outgoing-req-uri	string
prev-hop-ip	string
prev-hop-via	string
release-source	string
remote-media-address	string
session-protocol	string
sip-conf-id	string
sip-hdr	string
subscriber	string

Allied Telesis NETWORK SMARTER

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com