



Using RADIUS Authentication, Authorization, and Accounting

Overview

Remote Authentication Dial-In User Service (RADIUS) is the industry standard for user authentication, authorization, and accounting. This client/server protocol is designed to enable a RADIUS client to communicate with a RADIUS server using secure communication methods. The customer can implement one or more RADIUS servers and a distributed network of RADIUS clients to manage security and retrieve accounting information across a variety of broadband building sites. This strategy benefits the BBSM customer by providing greater security, a more scalable architecture, implementing open standards protocol, and leveraging future enhancements driven by the Internet Engineering Task Force (IETF).

The current BBSM release has a built-in RADIUS client that supports RADIUS authentication, authorization, and accounting. The BBSM RADIUS client is compliant with RFC 2865 and RFC 2866, which are the standards for RADIUS and RADIUS Authentication, respectively. The new design for RADIUS accounting augments the existing RADIUS client by adding the ability to retrieve statistics for BBSM user sessions. Administrators can configure multiple RADIUS servers to log Start and Stop accounting messages at the beginning and end of a BBSM user session. Interim-Update accounting messages are also supported and are sent at intervals configured by the administrator. The ability to configure multiple servers provides network redundancy in case the primary RADIUS server is not responding.

BBSM officially supports the Cisco ACS (v2.6), Microsoft 2000 IAS, and Navis RADIUS servers (v4.0), but should be compatible with any RADIUS server that complies with RFC 2865 and RFC 2866 and allows configuration of the vendor-specific attribute. BBSM stores authentication and accounting information in the RADIUS_SessionHistory table of the BBSM SQL database. In addition, session information (session activation and deactivation) is stored in this table. The RADIUS_SessionHistory table provides independent auditing of end user sessions and can be viewed using the Reports option on the BBSM Dashboard.



Note

This chapter explains only the BBSM RADIUS implementation and configuration. The reader is expected to be familiar with the RADIUS protocols documented in RFC 2865 and RFC 2866 and how to configure their specific RADIUS server. Configuration of supported RADIUS servers is outside the scope of this document.

RADIUS Authentication and Authorization

BBSM performs RADIUS authentication and authorization enabling end users to access the Internet. Each time the end user attempts to connect to the Internet, BBSM prompts for a username and password. The values entered are used in the Access-Request packet to the RADIUS authentication server.

Administrators may configure multiple RADIUS authentication servers by order of rank. BBSM begins with the lowest ranked authentication server when sending Access-Request packets. BBSM attempts to authenticate end users using all configured RADIUS authentication servers in the order they are ranked until an Access-Accept packet is successfully received. If a server does not respond within the specified time, BBSM attempts to contact that server up to three times before moving to the next highest ranked server. If a server responds with an Access-Reject packet, BBSM will immediately attempt to authenticate using the next highest ranked server.

The RADIUS Session History report shows all authentication attempts regardless of whether they are successful. The report also shows session activation and deactivation entries. Session activation entries are generated when the end user authenticates via the RADIUS authentication server and gains access to the Internet. Session deactivation entries are generated when the end user's access to the Internet is terminated. The administrator can view the RADIUS_SessionHistory table either by direct SQL query or by accessing the RADIUS Session History report from the Reports option on the BBSM Dashboard.

To allow a RADIUS user to have a session active on more than one computer on the BBSM network at the same time, the Allow multiple concurrent RADIUS sessions check box on the Sites web page must be checked on the WEBconfig Sites web page. Leave it unchecked (default) to prevent multiple computers from using the same RADIUS account at the same time.

**Note**

The current release of the Navis RADIUS server does not support user accounts with blank passwords. The Microsoft IAS RADIUS server does allow for blank passwords. However, Cisco does not recommend setting up any user accounts with blank passwords because of increased security risk.

Configuration

To configure BBSM to use RADIUS authentication, the administrator needs to perform the following procedures:

- Configure RADIUS authentication servers. (See the [“Configuring RADIUS Servers”](#) section on page 3-17.)
- Install a server SSL certificate to allow secure connections between client sessions and the BBSM server. (See [Appendix C, “Installing an SSL Certificate”](#).)
- Map ports to use either the RADIUS page set or a customized page set. (See the [“BBSM Page Sets”](#) section on page 3-28.)

If you are using a customized page set, the page set must be added to BBSM. See the *Cisco BBSM SDK Developer Guide* for instructions on developing a customized page set.

Bandwidth Feature During Authentication

BBSM supports bandwidth kbps specifications sent by the RADIUS authentication server in the Access-Accept packet. When a RADIUS server sends a vendor-specific attribute that contains a bandwidth kbps value, BBSM throttles the bandwidth of the end user session to the kbps value specified.

To use this feature, administrators need to configure their RADIUS server to send the vendor-specific attribute to transmit a Vendor ID of 5263, a Vendor type of 1, and the integer value of the bandwidth kbps desired for the user account.

**Caution**

The Bandwidth Manager check box on the WEBconfig Server web page must be checked for BBSM to throttle the end user session bandwidth kbps. If the RADIUS page set allows a user-selected bandwidth, the vendor-specific attribute is ignored. (See the [“Enabling the Bandwidth Manager” section on page 3-6.](#))

**Note**

The current release of the Cisco ACS RADIUS server (v2.6) does not support the enterprise vendor specific attribute. Version 3.0 of the Cisco ACS will support this attribute.

RADIUS Accounting

RADIUS accounting provides administrators with information about end user sessions when Internet access is granted (session activation), and when access to the Internet is terminated (session deactivation). This information makes it possible to perform independent billing by mining information for an end user from RADIUS accounting servers. Administrators may choose flat rate billing or per minute billing using the information BBSM sends to the RADIUS accounting server in Start and Stop Accounting-Request packets.

BBSM also supports sending Interim-Update accounting request packets. If configured, Interim-Update packets will be sent to the RADIUS accounting server at specified intervals.

BBSM allows multiple RADIUS accounting servers to be configured. As with RADIUS authentication servers, each server is configured with a ranking. BBSM attempts to send accounting packets to accounting servers by ascending order of rank until an accounting response packet is successfully received. For each server, BBSM attempts to send accounting request packets up to three times if the server fails to respond.

The RADIUS Session History report shows all Start and Stop accounting requests and whether an accounting response was received. If BBSM is configured to send Interim-Update packets, the RADIUS Session History report displays the first Interim-Update accounting request made for each session. Subsequent Interim-Update requests will only be reported if an error occurred during the packet transmission. The administrator can view the RADIUS_SessionHistory table either by direct SQL query or by accessing the RADIUS Session History report from the Reports option on the BBSM Dashboard.

Configuration

To configure BBSM to use RADIUS authentication, the administrator needs to:

- Configure the RADIUS authentication feature. (See the [“RADIUS Authentication and Authorization” section on page D-2.](#))
- Configure the RADIUS accounting servers. (See the [“Configuring RADIUS Servers” section on page 3-17.](#))
 - Optionally configure BBSM to send Interim-Update packets by entering a value in the RADIUS Accounting Interim Interval field in the WEBconfig Servers web page. (See the [“Server Web Page” section on page B-5.](#))

**Note**

If you are using a customized page set, the page set must be added to BBSM. See the *Cisco BBSM SDK Developer Guide* for instructions on developing a customized page set and changing the tiered service offerings of the sample page sets.

User-Selected Bandwidth Page Set

User-Selected Bandwidth (UBand) page sets support user-specified bandwidth as an alternate to bandwidth specification during authentication feature described earlier. This feature allows the administrator to define the service offerings to the end user through the page sets and allows the end user to select from the tiered services offered directly from the start page, such as:

64K for \$0.15/minute
128K for \$0.25/minute
Unlimited for \$0.30/minute

When UBand is used, BBSM throttles the session bandwidth at the kbps value selected by the end user. The bandwidth kbps that the end user selects is transmitted to the RADIUS accounting servers in the Start, Stop, and Interim-Update Accounting-Request packets. BBSM ignores any bandwidth kbps value returned by RADIUS authentication servers in Access-Accept packets when UBand is in use.

When the user authenticates and gains access to the Internet, a separate pop-up window appears with a Disconnect button. When the user clicks Disconnect to end the session, the Disconnect web page appears and displays session summary information. This page displays the username, the duration of the session (in minutes), and the estimated charge for the session.

**Note**

Since BBSM does not perform the actual user billing for RADIUS session, the calculation of session charges may differ from the final bill amount. BBSM rounds all minute increments up. For example, 20 seconds is displayed as 1 minute and 62 seconds is displayed as 2 minutes.

Administrators must ensure that the RADIUS accounting servers are configured to accept the bandwidth passed by BBSM in the vendor-specific attribute. The RADIUS accounting servers must also be configured to record the attribute value in order to mine the data for billing purposes.

Configuration

**Note**

The current release of the Cisco ACS RADIUS server (v2.6) does not support the enterprise vendor specific attribute. Version 3.0 of the Cisco ACS will support this attribute.

Using a customized page set that prompts the end user to select a bandwidth kbps enables the UBand feature. The two sample page sets that implement this feature are *RADIUSUBand* and *RADIUSUBandClear*.

To configure BBSM to use the new page set, the administrator must generate new port mappings. If you are using a customized page set, the page set must be added to BBSM. See the *BBSM SDK Developer Guide* for instructions on developing a customized page set.

RADIUS Packet Attributes

The BBSM server sends the following packets to the RADIUS server:

- Authentication Access-Request
- Start Accounting-Request
- Interim-Update Accounting-Request
- Stop Accounting-Request

The sections which follow detail the RADIUS attributes that are sent to the RADIUS server for each type of packet. Specific information concerning the NAS-Port attribute is also detailed.

Authentication Access-Request Packet

The following attributes are sent in the Access-Request accounting packet to the RADIUS authentication server.

Table D-1 RADIUS Access-Request Accounting Packet

Attribute	Description
User-Name	Name entered by the end user to authenticate against the RADIUS server and access the Internet via BBSM.
User-Password	Password entered by the end user to authenticate against the RADIUS server and access the Internet via BBSM.
Acct-Session-ID	The unique Session ID assigned to each BBSM end user session. This value is used to identify all authentication and accounting messages generated for a single user session.
NAS-IP-Address	Contains either the IP address of the BBSM external NIC or the IP address entered in the WEBconfig Server web page as the NAT IP Address.
NAS-Identifier	Contains the NAS Identifier value entered in the WEBconfig Server web page. If no value is entered in this field, BBSM will not include this attribute in the RADIUS Access-Request packet.
NAS-Port	See “ NAS-Port Mapping ” below.
NAS-Port-Type	5 indicates Virtual.
Framed-Protocol	1 indicates PPP.
Framed-IP-Address	IP address of client computer (PC) connecting to the Internet via BBSM.

Accounting-Request Packets

The following attributes are sent in the Start, Stop, or Interim-Update accounting packets to the RADIUS accounting server.

Table D-2 RADIUS Accounting Packets

Attribute	Description
Acct-Status-Type	1: Indicates a Start Accounting-Request packet—Requests that a message be sent when the user gains access. 2: Indicates a Stop Accounting-Request packet—Requests that a message be sent at regular intervals, as configured. 3: Indicates an Interim-Update Accounting-Request packet—Requests that a message be sent when the end user disconnects.
User-Name	Name entered by the end user to authenticate against the RADIUS server and access the Internet via BBSM.
Acct-Session-ID	The unique Session ID assigned to each BBSM end user session. This value is used to identify all authentication and accounting messages generated for a single user session.
NAS-IP-Address	Contains either the IP address of the BBSM external NIC or the IP address entered in the WEBconfig Server web page as the NAT IP Address.
NAS-Identifier	Contains the NAS Identifier value entered in the WEBconfig Server web page. If no value is entered in this field, BBSM will not include this attribute in the RADIUS Access-Request packet.
NAS-Port	See “NAS-Port Mapping” below.
NAS-Port-Type	5: Indicates Virtual.
Framed-Protocol	1: Indicates PPP.
Framed-IP-Address	IP address of the client (PC) connecting to the Internet through BBSM.
Vendor-Specific	Attribute containing the bandwidth kbps value that the end user selects when requesting Internet access. This attribute is only sent to RADIUS accounting servers if the user-selected bandwidth feature is enabled. See the “Vendor-Specific Attribute Byte Format” section below for information on how this attribute is formatted.

Vendor-Specific Attribute Byte Format

The following is the byte format of the vendor-specific attribute BBSM sends to the RADIUS accounting servers in Start, Stop, and Interim-Update accounting requests when the UBand feature is enabled.

Table D-3 RADIUS Vendor-Specific Attribute Format

Byte	Value	Description
1	26	Vendor-specific attribute type per RFC 2865
2	(4 * sizeof (BYTE)) + (2 * sizeof (DWORD))	This is the length in bytes of the full attribute specification beginning with attribute type (byte 1), should come out to 12 if each byte size = 1.
3–6	5263	Vendor-ID value.
7	1	Vendor data type; 1 indicates bandwidth kbps value.
8	(2 * sizeof (BYTE)) + sizeof (DWORD)	This is the length in bytes of the vendor-specific portion of the attribute specification starting with vendor-specific attribute data type, should come out to 6 if each byte size = 1.
9–12	9–12	Actual bandwidth kbps value (ulong).

NAS-Port Mapping

The NAS-Port value is a numeric value. BBSM maps the NAS-Port attribute as the following:

aaabbcddd

where:

aaa = site number

bb = stack

cc = switch

ddd = port

For example, if the site number = 1, the stack number = 2, the switch number = 3, and the port number = 5, then the NAS-Port number = 10202005.



Note

Because the NAS-Port is a numeric value, the leading zeros of the site number are dropped.

