



Using the BBSM Interfaces

The Cisco BBSM server is managed remotely using web-based user interfaces. These interfaces give remote administrators complete control over operation and allow the collection of detailed statistics on system use. Transaction reports and other information are presented in a web-based format to allow for remote management of the Cisco BBSM system.

Accessing the Dashboard

The BBSM Dashboard provides a central location for accessing the web-based options and features of the BBSM system.



Note

BBSM server web pages are accessed on port 9488 instead of the default web server port 80. This is done by adding “:9488” after the BBSM server IP address or host name in the http request (for example, `http://10.10.10.50:9488/www`). If you are on the inside BBSM network, you must activate a session to get access to these pages.

To access the Dashboard from a remote computer, use one of the following:

- If you are accessing BBSM from a remote location, use BBSM’s external IP address to access the BBSM server. Enter `http://<external_NIC_address>:9488/www`, where <external_NIC_address> is the external NIC address of the BBSM server you want to access; for example, type `http://999.99.999.99:9488/www`, and press **Enter**.
- If you are accessing the BBSM server within BBSM’s subnet, use the BBSM server’s internal IP address. Enter `http://<internal_IP_address>:9488/www`, where <internal_IP_address> is the internal IP address of the BBSM server you want to access; for example, type `http://888.88.888.88:9488/www`, and press **Enter**.

Dashboard Options

The following table gives a brief summary of each option located on the Dashboard and the functionality associated with that option.

Table B-1 BBSM Dashboard Options

Administration Section	
WEBconfig	Use this option to access the web pages to configure BBSM.
WEB PMS Test	Use this option to access the BBSM PMS Test option.
WEBpatch	Use this option to access WEBpatch. Use this utility to: <ul style="list-style-type: none"> • Perform remote updating of the BBSM server software • Obtain a listing containing details about all patches and BBSM service packs installed
Operations Section	
Port Control Form	Use this option to view the list of ports and edit per-port policies.
Map Rooms	Use this option to edit and map guest and meeting rooms to ports.
Subscription Port Control	Use this option to maintain ports associated with the Subscription access policy.
Access Code Management	Use this option to generate, edit and delete access codes.
Reports Section	
Reporting Pages	Use this option to view usage, transaction history, active ports, access codes, room mappings, RADIUS data, and walled garden data.

Using the BBSM Dashboard with Multiple Sites

A BBSM server configured for multiple sites displays a slightly different BBSM Dashboard screen. It is necessary to select the site before choosing a configuration option.

-
- Step 1** Launch the BBSM Dashboard.
- Step 2** Select the appropriate site from a drop-down selection menu that appears in the upper portion of the BBSM Dashboard. See [Figure B-1](#).

Figure B-1 BBSM Dashboard for Multiple Sites

- Step 3** Click the appropriate option in the lower half of the Dashboard.
-

Accessing WEBconfig

WEBconfig is the primary tool for configuring your BBSM system. This web-based GUI tool allows the administrator to make changes to the BBSM system with just a click of a button.

The interface consists of 11 web pages that are accessible from a button bar at the top of the page. Various fields and options are presented on each page with inactive buttons and options greyed-out. To close WEBconfig and return to the Dashboard, just click the Dashboard link in the upper right corner.

WEBconfig Web Page Descriptions

Table B-2 identifies the WEBconfig web pages and associated functionality.

Table B-2 WEBconfig Web Page Descriptions

Web Page	Description
Port IPs	Allows the configuration of the address ranges for the BBSM server and the network equipment.
Server	Allows the configuration of server-wide settings such as Bandwidth Manager, Transparent Proxy, SMTP forwarding IP address, and RADIUS. Allows the parameter setting for credit card servers that might be used.
Sites	Allows the adding of sites and general site information. This web page defines the preliminary billing features for the site.
Routers	Allows the setting of router interface parameters. Configures routers on the internal network. Note This feature is for routed networks and is not related to WAN activities.
Switches	Allows the selection of switch type and configuration of the stacks and switches for each site. Each site can support multiple stacks. Each stack supports one or more switches of the same type.
Page Sets	Defines the location of customized page sets designed by your web developers and the associated start page. The page set appears in the page set drop-down list on the Port Map web page.
Port Map	Allows the selection of a policy to populate the table that maps port IDs to switch stacks and rooms for a selected site.
Port Tests	Allows you to select port test parameters.
Call Type	Allows the configuration of the Call Types for each site. Call Types are Property Management System vendor provided. When users log on to the BBSM system, the Call Types information is sent to the hotel's PMS. Call Type is used by the PMS to determine the charge type for the guest folio. Most PMS systems use Call Type A to define an Internet access charge.
RADIUS Servers	Allows the definition of the IP address or DNS host name and configuration parameters for RADIUS servers.
Walled Garden	Allows the configuration of the server to allow access to web sites free of charge while denying access to the Internet as a whole. Walled Gardens provide a way for service providers to offer end user viewing on a trial basis free of charge.

WEBconfig Web Page Options

The following sections detail the options, ranges, and defaults for each WEBconfig web page.

Port IP Addresses Web Page

The Port IP Addresses web page provides a place to set the client and management IP address ranges. It is accessed using the **Port IPs** button.



Note

The Port IP Addresses configuration is a server-wide configuration. There is only one Port IP Addresses configuration for each BBSM server.

The following is a list of the settings and functions for the Port IPs web page.

- **DHCP Start**

Beginning DHCP IP address. The DHCP Start and End addresses establish the IP addresses to assign to end-user DHCP clients. This range must be on the same subnet as your internal network interface card (NIC).

- **DHCP End**

Ending DHCP IP address.

- **Foreign Start**

Beginning foreign IP address. Use the Foreign Start and Foreign End IP addresses to assign IP addresses for end-user computers without DHCP clients (static addresses). The Foreign address range allows BBSM to perform adaptive network address translation (NAT) for statically configured devices in a bridged environment.



Note All other NAT and PAT addressing is handled by the router.

- **Foreign End**

Ending foreign IP address.

- **Management Start**

Beginning Management IP address. A management range is used to assign IP addresses for switches and other network equipment. Assigning start and end IP addresses allows the BBSM server to communicate with these devices.

To remotely access equipment over the Internet, put the network equipment (such as switches, base switches, network addressable UPS systems, and cable modem headends) in the Management range.

Devices in the IP address range specified by **Management Start** and **Management End** are always given access to the Internet. These Management IP addresses can be used to support remote monitoring of BBSM network equipment.

- **Management End**

Ending management IP address.

- **Internal NIC IP**

You cannot edit this field. The IP address of internal NIC that usually connects to the base switch.

- **Internal NIC Subnet Mask**

You cannot edit this field. The subnet mask used with the internal network interface card.

- **External NIC IP**

You cannot edit this field. The IP address of external NIC that usually connects to the external router.

- **External NIC Subnet Mask**

You cannot edit this field. The subnet mask used with the external network interface card.

- **Default Gateway**

You cannot edit this field. The default gateway to the Internet.



Note

The BBSM TCP/IP Properties fields, which include Internal NIC IP, Internal NIC Subnet Mask, External NIC IP, External NIC Subnet Mask, and Default Gateway, are read-only and cannot be changed in WEBconfig. See [“Running the Address Change Wizard” section on page 2-9](#).

Server Web Page

The Server web page covers the server-wide settings for the BBSM server. These include information concerning a credit card server if credit card billing is used, and specific network configurations that impact the entire BBSM network such as the Bandwidth Manager.

The following is a list of the settings and functions for the Server web page.

- **Credit Card Server section**

- **Billing Server Address**

Address of the ICS credit card billing server. BBSM sends encrypted credit charge data to the credit card server at this address when using credit card accounting.

Default - Blank

- **Backup Billing Server Address**

(No longer used since ICS does not support a backup server.)

- **Connect Timeout Seconds**

The number of seconds the credit card server attempts to validate a credit card before rejecting the client's input. The default is 30 seconds.

- **Currency Type**

Select the type of currency used by the ICS server from drop-down menu. The default is USD.

- **Network Configuration section**

- **Enable Domain Name for SSL Page Sets**

Check this box to enable the use of SSL page sets with a certificate.

- **Domain Name**

Enter the domain name exactly as it appears in the SSL certificate.

- **Enable Maximum Active Sessions**

Click to enable maximum active sessions. Enabling this feature allows the administrator to establish the number of allowable active sessions.

Default - Disabled

– **Maximum Active Sessions**

Enter number to set maximum number of allowable active sessions. In general, this option is used to control the maximum number of simultaneous users since there is one session per user. This option is only available when Enable Maximum Active Sessions is checked.

Default - 0

– **Current Active Sessions**

Displays the current number of end users connected to the Internet through BBSM.

– **Bandwidth Manager**

Click to enable the bandwidth manager. Enabling this feature allows the user to select various bandwidth speeds when connecting. This must be checked to use a RADIUS access policy that throttles bandwidth. Bandwidth manager is not QoS.

Default - Unchecked

– **Enable Transparent Proxy**

Click to enable the transparent proxy. Enabling this features allows the BBSM server to force all clients to use a proxy even if not configured to do so. This allows collection of information on system usage which appears in the log files.

Default - Unchecked

– **SMTP Forwarding Server**

Enabling this feature allows Simple Mail Transfer Protocol (SMTP) forwarding of all e-mails. All SMTP requests received by the BBSM server are forwarded to the specified IP address or Fully-Qualified Domain Name (FQDN). If blank, the server doesn't change the SMTP destination.

SMTP is a standard TCP/IP protocol used for transferring e-mails between servers over the Internet. These transmissions are received on port 25. Blocking unregistered IP addresses from reaching an SMTP server or relay via port 25 is a standard practice by Internet Service Providers to prevent spamming. As a result, all foreign, unregistered IP addresses are blocked.

To enable the transmission of e-mail via the BBSM server, you need to contact your ISP to register the external BBSM IP address. You then enter the STMP server or relay IP address or FQDN in this field. Then, e-mails forwarded by BBSM to an STMP server will be relayed correctly to the appropriate mail server.

Default - Blank

– **NAT IP Address**

If the BBSM server is behind a NAT router, enter the public IP address that the router assigned to the BBSM server. The RADIUS access policy uses this IP address when sending authentication or accounting packets to the RADIUS server. If the field is left blank, the RADIUS access policy uses the IP address of the external NIC.

– **NAS Identifier**

Enter a unique server identifier, such as "BBSMServer1." The RADIUS access policy uses this NAS identifier when sending authentication or accounting packets to the RADIUS server. If the field is left blank, the attribute is not sent.

– **RADIUS Accounting Interim Interval**

The number of minutes between sending Interim-Update packets to a RADIUS Accounting server. If the value is 0, Interim-Update packets are not sent. The default is 0.

Sites Web Page

Use the Sites web page to configure one or more sites to be supported by the BBSM server. The Sites web page can also be used to delete a site and its related stacks, port map, and call types.

The following is a list of the settings and functions for the Sites web page:

- **General section**

- **Site Number**

Specifies the number of the site you want to add or change. The default is 1.

- **Site Description**

Use this field to record a brief description of the site.

- **Site Location**

Use this field to enter the name of location where the site is located, such as San Diego or Building One.

- **Allow multiple concurrent RADIUS sessions**

Check this box to allow a RADIUS user to have a session active on more than one computer at the same time on the internal BBSM network. Leave it unchecked (default) to prevent multiple computers from using the same RADIUS account at the same time. The default is unchecked.

- **Port Hop Delay (minutes)**

Enter a number of minutes between 1 and 60. (The default is 20.)

If BBSM port hopping is enabled and a user is disconnected from the network, BBSM searches for the user every minute until this number of minutes is reached. If the user is not found within this time frame, the BBSM session is terminated.

- **Printing section** (enabled only if KeyView Pro is installed)

- BBSM Printer

- Network/Local Printer

- Price Per Page

- Maximum Price Per Job

- Printer Account User ID

- Printer Account Password

- Confirm Password

- **Credit Card Billing section**

- **Merchant ID**

Use Merchant ID to indicate the assigned credit card charging location ID. This ID is assigned due to the relationship the service provider has with a Merchant Bank. This ID is different for every geographical location and is required by credit card companies.

If you need to enter a Merchant ID and have difficulty determining what this identity should be, contact the Cisco Technical Assistance Hotline. Use the Service and Support Information card to determine the applicable phone number for the hotline.

- **Hotel Billing section**
 - **Athdmn IP Address**
Enter the IP address of the site controller computer where the hotel PMS interface software resides. BBSM is connected to the PMS by a serial cable. Site controllers are required to interface to the PMS in the multi-site/multi-building mode. Athdmn must be started if it is used.
Leave this field blank if you are not using a site controller.
 - **PMS Billing**
Enable PMS Billing to send bills for system usage to a hotel PMS.
 - **PMS Protocol**
Select a PMS Protocol value to allow selection of the following PMS Protocols: BellHobic, Fidelio Serial, Hilton, Xiox. For information about adding other PMS interfaces, see the *Cisco BBSM SDK Developer Guide*.
 - **Print Billing**
Enable Print Billing to print bills for the BBSM system using a local printer connected directly to the server or network printer. BBSM supports USB, LAN, or a serial connection.
 - **Billing Printer**
Network address of the billing printers. If the printer is not a line printer, a printer IP address must be entered. If it is a network printer, the exact printer name must be entered.

Routers Web Page

In BBSM, all switch stacks and switches are associated with a router. This association tells the BBSM server how to build routes to reach each switch. The Routers web page data is used to record this information.



Note

Only use the WEBconfig **Router** page to configure BBSM servers that are attached to Routed Networks. If indicated for your BBSM network, the configuration information for this page will come from the network topology. Refer to [Chapter 1, “Overview”](#) for additional information.

All fields except Router Number and Password are disabled for Router Number = 0. The disabled fields will not be enabled unless Router Number is other than 0.

The following is a list of the settings and functions for the Routers web page.

- **Router Number**
Unique index number, from 1 to 999, of the router. This number can be arbitrary and need not be consecutive. The number 0 always selects the BBSM server. The default is 0, where 0 is a reserved value for the BBSM itself.
- **Router IP Address**
The address of the gateway to the Internet that the router provides to client PCs. Determine this address from your network planning diagram. On client computers, this IP address is their default gateway. In the case of computers connected to the BBSM server internal network, the gateway is the BBSM server internal NIC address. The default is 127.0.0.1. (This loopback IP address refers to the BBSM server and cannot be changed for router 0.)

- **Gateway To Router**

The address of the first hop from the BBSM server to the router. Determine this address from your network planning diagram. This address should be on the BBSM server internal network and is the external address of the router if the router is connected directly to the BBSM server internal network.

- **Client Start**

The lowest IP address for client computers on this router's network. Determine this address from your network planning diagram. The BBSM server treats traffic from the Client Start through the Client End IP address range as coming from client computers.

- **Client End**

The highest DHCP IP address for client computers on this router's network. Determine this address from your network planning diagram. The BBSM server treats traffic from the Client Start through Client End IP address range as coming from client computers.

- **Client Subnet Mask**

The subnet mask assigned to client computers on this router's network. Determine this address from your network planning diagram. This subnet mask value must be configured on the client computers and is set automatically for DHCP clients.

- **Router Supports SNMP**

For router 0, the "Router Supports SNMP" check box is checked and disabled. The SNMP password check box is enabled.

For routers other than router 0, the check box is enabled. If the administrator checks the check box, the SNMP password is enabled. Otherwise, the SNMP password is disabled.

Default - Unchecked

- **SNMP Password**

The router SNMP Community String. The BBSM server uses this string to access the ipNetToMedia Table specified in RFC-1213. The router must support this SNMP object for the BBSM system to support that router. RFC-1213 specifies the minimum information that an SNMP agent needs to provide. Generally, the password is configured by the administrator installing BBSM using procedures defined by the switch manufacturer.

- **Create DHCP Scope**

If checked, creates a DHCP scope on the BBSM server for the router subnet. This DHCP Scope is determined by the IP addresses in the Client Start and End fields. Check this box if this router uses DHCP relay to send DHCP requests from clients to the BBSM server. The default is unchecked. If you have an external DHCP server, or if the router will be acting as the DHCP server, leave this box unchecked.

Restrictions When Using the Router Supports SNMP Feature

The following list describes the restrictions and caveats that must be observed when an administrator disables the "Router Supports SNMP" feature for a router other than Router 0 (BBSM).

- The Daily Access policy has a "Welcome Back MAC" feature. Since BBSM will not know the MAC address of the client, this feature will not operate properly.
- The Access Code History report will not show the correct MAC address for the client.
- The Cruise Line Transaction History table will not contain the correct MAC address for the client.
- The Active Sessions report will not show the correct MAC address for the client.

- The RADIUS Session History report will not show the correct MAC address for the client.
- The MAC address in the core transaction history table will not be correct. Therefore any report derived from the transaction history table (usage, etc.) will not have the correct MAC address of the client.
- BBSM will not be able to use per-port policy since per-port policy depends on using the correct MAC address.
- BBSM will not be able to use any network element (switch DLL) that relies on knowing the MAC address to determine if the session is still alive. In other words, the administrator must configure the “NULL: Clients connect to router” switch on the Switches web page in WEBconfig.

Switches Web Page

Use the Switches web page to enter information about network elements and switch stacks for each site. The following is a list of the Switches web page settings and functions.

- **Site Number**
Number of the site associated with the switch. The default is 1.
- **Stack Number**
Number from 1 to 999 that identifies the stack. The default is 1.
- **Aging Period (Seconds)**
Number of seconds the BBSM user can be idle before user is signed off automatically for some switch types. The default is 300 (5 minutes).
- **Client Ports On Switch 1**
Number of ports that are usable as client (computer) ports on switch 1 of the stack. The default is 24.
- **Client Ports On Switches 2-n**
Number of ports that are usable as client (computer) ports on switches 2 through n of the stack, where n is the highest numbered switch installed on the stack. Set this to 0 if the switch is not stackable. The default is 24.
- **Stack IP Address**
A unique IP address in the management range assigned to the switch. Check with the person installing your stacks and switches if you are unsure of this IP address.
- **Router**
The IP address of the router that this site and stack are connected to. If the site and stack are directly connected to the BBSM server, use the IP address “127.0.0.1.” The Router drop-down menu shows the available router IP addresses. These addresses are established through the Routers web page. The default IP address is 127.0.0.1, which is the IP address of the BBSM server.
- **Switch Type**
Type of switches being used for this stack. Choose one of the supported switch types from the drop-down list. To use a network component not found on the list, contact the Cisco Technical Assistance Hotline. Reference the Service and Support Information card for applicable hotline phone number. The default is Cisco 2900.

- **SNMP Password**

The SNMP community string (password) to use when communicating with switches. All switches that share the same stack (that is, matrixed switches) must be installed with the same password. The default is public.

**Caution**

It is recommended that the default password on the switches and the BBSM be changed because the default password is well known and could be used to compromise the security of the network.

- **Disabled**

Indicates whether this switch stack is enabled or disabled (the default is unchecked):

- When unchecked (enabled), BBSM looks for clients on the ports for the stack. Use this setting when the switch stack is working properly.
- When checked (disabled), BBSM does not look for clients on the ports for the stack. Use the disabled setting for troubleshooting.

**Note**

The IP address for a switch remains reserved even if the switch is disabled. If you need to reuse the IP address of a disabled switch for a different switch, be sure to change the IP address of the disabled switch temporarily; otherwise, you will not be able to update the WEBconfig database.

**Tip**

Be sure to contact Cisco for guidance if you need to make drastic changes to your switch configuration.

Page Sets Web Page

The Page Sets web page defines the location of customized page sets designed by your web developers.

There is a default list of web page sets that comes with BBSM that can be used to represent the Internet service you want to offer. Your own web developers can also create customized page sets by modifying the default web pages provided by BBSM or by creating entirely new web pages.

Page sets are specified on a per-port basis. Any new page set name you establish using the Page Set web page will appear in the list of page sets on the Port Map web page.

**Caution**

Before attempting to use a non-standard custom page set, see the *Cisco BBSM SDK Developer Guide*. If necessary, consult with Cisco Systems to be sure the page can be supported. Refer to the “Preface” for more information of how to contact the appropriate group within Cisco Systems.

To define a page set, use the Page Sets web page to enter the name of the custom page set and the start page. The following are the fields:

- **Page Set**—This field displays the name of the page set you enter. As a rule, each page set specifies an access and an accounting policy.
- **Start Page**—This field displays the Start Page associated with the page set. There is a Start Page defined for each default page set that comes with BBSM. To associate a Start Page with a custom page set, enter the Start Page URL in this field. The URL must be in this format:

```
http://%iport%/ekgnkm/<page_set_name>Start.asp
```

Port Map Web Page

Use the Port Map web page to specify page sets and bandwidths you want associated with each room. This data is used to populate the table that maps port IDs with switch stacks and rooms for a selected site.

The following is a list of the settings and functions for the Port Map web page.

- **Site Number**

The site number that identifies the site you want to port map. The default is 1.

- **Clear Existing Port Map**

This check box is checked by default. Check it to create a completely new port map. Checking this box discards any existing information, including room mappings. (Recreating a new port map after deleting an existing map can be very time consuming.)

Uncheck this box to retain existing port map entries and add new entries to the existing port map data.

- **First room number**

The lowest room number you want WEBconfig to use when creating the initial port map. Pick a minimum room number that is higher than the hotel's highest guest room number.



Note The initial port ID-to-room-number mappings are placeholders only. During actual room mapping, administrators access the enterroom.asp web page from each guest room to establish the correct mappings between port IDs and real room numbers.

Administrators can use the BBSM Dashboard > Reports > Room Mappings web page to see the port IDs that use placeholder room mappings and those that are actually mapped. Any room numbers greater than or equal to the minimum room number you specified on the Port Map web page have not yet been mapped via the BBSM Dashboard > Operations > Map Rooms web page.

Default - 6000

- **Page Set**

Specifies the page set used by the site. [Table B-3](#) describes the BBSM default page sets.



Caution

Page sets whose name ends in "Clear" do not use SSL security and are designed for testing. Therefore, Cisco does not recommend using this page set in production. BBSM provides this page set for demonstration and testing situations in which installing a server certificate is not feasible.

Table B-3 BBSM Default Page Set Descriptions

Page Set	Description
AccessCode	The page set prompts the end user to enter an access code to access the Internet but does not do any accounting. It allows numerous users for each access code. The BBSM administrator or operator configures the valid authorization period for an access code.
BlockICS	The page set prompts the end user to enter credit card information to access the Internet for a block of minutes. BBSM performs credit card authentication and billing through the CyberSource ICS billing server.

Table B-3 BBSM Default Page Set Descriptions

Page Set	Description
CruiseLine	The page set prompts the end user to enter credit card information or access card information (access card information is not the same as an access code) to access the Internet per minute or for a block of minutes.
DailyHotel	The DailyHotel page set combines the Daily access policy with the Hotel accounting policy. This combination gives the user access for a 24-hour period and charges the hotel's PMS.
DailyICS	The page set prompts the end user to enter credit card information to access the Internet for a 24-hour period. BBSM performs credit card authentication and billing through the CyberSource ICS billing server by using SSL.
DailyICSClear	This page set is similar to the DailyICS page set, but it does <i>not</i> use SSL to transmit information to the BBSM server. The end user's browser transmits credit card information to BBSM from the form on DailyICSClearStart.asp in clear text. Therefore, Cisco does not recommend using this page set in production. BBSM provides this page set for demonstration and testing situations in which installing a server certificate is not feasible.
MeetingRoom	The page set prompts the end user to enter an access code to access the Internet but does not do any accounting. It allows just one user for each unique access code. The BBSM administrator or operator configures the valid authorization period for an access code.
Mega	The Mega page set allows the end user to select the access policy and the accounting policy. This page set shows you how to provide flexibility to the end user and still control access.
MinuteICS	The page set prompts the end user to enter credit card information to access the Internet per minute. BBSM performs credit card authentication and billing through the CyberSource ICS billing server.
MinuteICSClear	This page set is similar to the MinuteICS page set, but it does <i>not</i> use SSL to transmit information to the BBSM server. The end user's browser transmits credit card information to BBSM from the form on MinuteICSClearStart.asp in clear text. Therefore, as with DailyICSClear, Cisco does not recommend using this page set in a production environment. The page set is used for demonstration and testing where installing a server certificate is not feasible.
RADIUS	The page set prompts the end user to enter a RADIUS username and password to access the Internet. The information is sent by using SSL.
RADIUSClear	The RADIUSClear page set is similar to the RADIUS page set, but it does <i>not</i> use SSL to transmit information to the BBSM server. The end user's browser transmits the RADIUS username and password to BBSM from the form on RADIUSClearStart.asp in clear text. Therefore, Cisco does not recommend using this page set in production. The page set is used for demonstration and testing where installing a server certificate is not feasible.
RADIUSUBand	The page set prompts the end user to enter a RADIUS username and password to access the Internet. It also permits the end user to select their desired bandwidth at a specified price. For this page set, the disconnect web page presents the end user with an estimated summary for the time of the active session and the charges accrued at the selected bandwidth. The information is sent by using SSL.

Table B-3 BBSM Default Page Set Descriptions

Page Set	Description
RADIUSUBand Clear	The RADIUSUBandClear page set is similar to the RADIUSUBand page set, but it does <i>not</i> use SSL to transmit information to the BBSM server. The end user's browser transmits the RADIUS username and password to BBSM from the form on RADIUSUBandClearStart.asp in clear text. Therefore, Cisco does not recommend using this page set in production. The page set is used for demonstration and testing where installing a server certificate is not feasible.
Subscription	The Subscription page set allows the end user to access the Internet for a specific date range associated with the end user's port. When the end user activates a session using this page set, BBSM redirects the end user to a specified portal page.
SubscriptionHome	The page set allows the end user to access the Internet for a specific date range associated with the end user's port. When the end user activates a session using this page set, BBSM redirects the end user to the originally requested URL, which is typically the home page set in the browser.
SubscriptionHotel	The page set allows the end user to access the Internet for a specific date range associated with the end user's port. If the end user attempts to access the Internet outside the date range, the page set allows the user to self-provision the subscription, by billing the subscription to the hotel's PMS.
SubscriptionHotel MultipleDay	The page set allows the end user to access the Internet for a varied date range (which is set by the administrator) associated with the end user's port. The date range, bandwidth, and pricing is set using the MDSubPackage.asp file. If the end user attempts to access the Internet outside the date range, the page set allows the user to self-provision the subscription, billing the subscription to the hotel's PMS.
SubscriptionICS	The page set allows the end user to access the Internet for a specific date range associated with the end user's port. If the end user attempts to access the Internet outside the date range, the page set allows the user to self-provision the subscription, by billing the subscription to a credit card. BBSM performs credit card authentication and billing through the CyberSource ICS billing server.

- **Start Page**

Specifies the starting Active Server Page (asp) file associated with the value you selected for the page set. The Start Page provides the path to the first page that the client sees.

The Start Page is automatically assigned when you select a page set, but you can manually override the automatically assigned value if necessary.

Default - DailyHotelStart.asp

- **Bandwidth (Kbps)**

Specifies the bandwidth (in kbps) that the port uses if Bandwidth Manager is enabled (see [“Server Web Page” section on page B-5](#)). The value is an integer in the range 0 (maximum bandwidth) to 2000000 (2 Gbps). The default is 0 (maximum speed).

- **Enable Port Hop**

Activates the port hopping feature that allows an end user to move from one wireless access point to another without having to re-authenticate. The default is unchecked, or Disabled.

See [Appendix E, “Understanding Port Hopping.”](#)

Port Tests Web Page

To perform accurate port testing, network elements require different test parameters like number of pings to transmit, inter-packet delay and echo data size, depending on the device type. The BBSM server administrator can configure these parameters through a Port Tests web page user-interface.



Caution

You must visit the Port Tests web page after creating a new port map to enable the running of port tests during room mapping.



Note

The hardware dependent port test feature is only available to the BBSM administrator through the WEBconfig Port Tests page.

The test parameters can be configured per switch type where all ports of a switch have the same test parameters for every switch port.

The following is a list of the settings and functions for the Port Tests web page. The first four items are taken from the information entered on the Switches page. To select the proper information, use the Navigation buttons at the bottom.

- **Site Number**

The site number for which you want to test the ports. The default is 1.

- **Stack Number**

Specify the stack number of the site you are testing. The default is 1.

- **Stack IP Address**

Displays the IP address for the stack that is being tested.

Default - IP address for Site 1

- **Switch Type**

Displays the make and model of the switch associated with the site/stack selected.

Default - Switch associated with Site 1

- **Switch Mode**

Select the rate within the acceptable ranges ([Table B-4](#)) that the switch is configured for operation.

Table B-4 Switch Mode Defaults and Ranges

Switch Mode (Mbps)	Pings To Send		Inter Packet Delay		Echo Data Size	
	Default	Range	Default	Range	Default	Range
1	500	300 to 700	85	85 to 90	1024	768 to 1280
5			45	45 to 50		
10			10	10 to 15		
15			7	6 to 9		
100			3	1 to 5		

Default - 10Mbps

- **Pings to Send**
Enter the number of pings to be sent (ignore the word “bytes” after the box).
Default - 500
- **InterPacket Delay**
Enter the Inter Packet Delay in milliseconds.
Default - 10
- **Echo Data Size**
Enter the desired size for the echo data in the number of bytes.
Default - 1024

Call Types Web Page

Use this web page to configure the Call Types transmitted to the Property Management System by BBSM for a given site.

Property Management Systems expect systems that post charges to provide a single character Call Types code as part of the charging information. Use this web page to specify the one-letter code and its associated description.

The following is a list of the settings and functions for the Call Types web page.

- **Site Number**
Specify the site number of the Call Type record you want to add or change. The default is 1.
- **Description**
The default description is the word “Default.” The Default call type record is automatically created when the first site record is created on the Sites web page and is reserved for BBSM Internet sessions.



Caution Do not change the word “Default.” It is used to internally to track BBSM charges posted to the PMS. If needed for your PMS, you can change the Call Type letter associated with the Default setting.

- **Call Type**
Specify the one-letter code for the Call Type.
Enter A if you are not given another specific value for use with your hotel PMS. Enter a one-letter value other than A if directed to do so by the person who configures your hotel PMS.
Default - A

RADIUS Servers Web Page

**Note**

The RADIUS Server section can be skipped if the BBSM will not use a RADIUS Server for any authentication.

RADIUS servers are often used to maintain username and password information for Internet Server Providers (ISPs). The BBSM server can operate as a RADIUS client, allowing BBSM clients and dial-up routers to be authenticated against a RADIUS server.

The following is a list of the settings and functions for the RADIUS Servers web page.

- **Server Name**

The Server Name is the DNS name (or IP address) of the RADIUS server. The Server Name and IP address must be unique. You cannot have two entries with the same name. The maximum character length is 64.

- **Secret**

This is the RADIUS client password used to access the RADIUS server.

- **Timeout**

Timeout represents the number of seconds the RADIUS client waits to get a response from a RADIUS server before giving up and moving to the next RADIUS server. The default is 5.

- **Rank**

Defines the order in which the BBSM server will attempt to contact RADIUS servers to authenticate a user. The BBSM server contacts servers in ascending order of rank. The default is 30.

- **Enable Authentication**

Enables the BBSM system to check with a RADIUS Authentication server (Authentication Access-Request message) to verify username and password. The default is Enabled.

- **Enable Accounting**

Enables the BBSM system to contact the RADIUS Accounting server to log the Start, Interim-Update Accounting, and Stop accounting messages, as described in [Table D-2 on page D-6](#). The default is Enabled.

- **Port (for Authentication)**

This is the TCP port on the BBSM server used by the RADIUS server to communicate with the RADIUS authentication server. The default is 1645.

- **Port (for Accounting)**

This is the TCP port on the BBSM server used by the RADIUS server to communicate with the RADIUS accounting server. The default is 1646.

Walled Garden Web Page

The Walled Garden feature allows external web sites to be viewed by end users before they agree to pay for the Internet service or before they are authenticated by the system. The Walled Garden is essentially a “free zone” of Internet services that end users can always access. The Internet services are defined in BBSM by a network IP address and a network subnet mask. The Walled Garden feature operates on a BBSM per-server basis.

**Caution**

Configuring too many Walled Garden sites can impact performance.

The following is a list of the settings and functions for the Walled Garden web page.

- **Host Name**

Host Name is the name of the site where the Walled Garden web pages are located.

Example: www.cisco.com

- **Network Address**

The network address can either be an IP address of a specific host or an IP address of a specific network. In either case, it is the IP address of the website named as the Host Name.

- **Network Mask**

The subnet mask defines the filter to be applied to the Network Address. It defines the bits in the IP address that correspond to the subnet. Use the Network Mask to allow access to multiple web servers on the same IP subnet. Use 255.255.255.255 (default) as the Network Mask value when there is only one server.

Using Navigation and Special Function Buttons

Navigation and special function buttons are used on most of the BBSM web pages and forms. Use the navigation buttons to locate the appropriate information you want to see and the special function buttons to change the data. A button is disabled when there are no records or when the record is the first.

**Caution**

Be sure to use the navigation buttons to locate the correct record *before* making any changes. Be sure you are viewing the item you want to change when entering the data for the change.

Table B-5 shows the navigation buttons. Note that the buttons are disabled when no records are available for that function; for example, the First and Previous buttons are grayed out when you are viewing the first record.

Table B-5 *Navigation Button Descriptions*





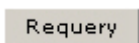

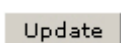
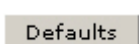
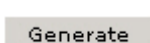
Button	Description
	Returns the user to the first record or page.
	Returns the user to the previous record or page.
	Takes the user to the next record or page.
	Takes the user to the last record or page.

Table B-6 describes the special function buttons.

Table B-6 *Special Function Button Definitions*

Button	Description
	Returns the last set of stored information to the web page from the database.
	Deletes the currently displayed record and its related data (if any). Delete is disabled if no records exist.
	Saves the setting changes. Update is disabled if no records exist.
	Displays default settings for a particular web page. Review the defaults and make changes as necessary.
	Creates a new port map.

