



Overview

As a gateway server for public access networks, Cisco Building Broadband Service Manager (BBSM) enables high-speed Internet access. It enables simple “plug-and-play” access, self-provisioning of end-user services, multiple authentication and billing options, and web-based configuration, management, and reporting.

This chapter includes these sections:

- [New in Software Release 5.3, page 1-2](#)
- [Transmission and Networking Options, page 1-3](#)
- [Understanding the BBSM Dashboard, page 1-6](#)
- [Using Navigation Buttons, page 1-12](#)
- [Connecting a Client to BBSM, page 1-12](#)

The BBSM server integrates and manages these key functions:

- **Connection**—Enables you to provide Internet access to end users regardless of the client’s network interface configurations. Network deployment options include Ethernet, long-reach Ethernet (LRE), wireless, and cable.
- **Authentication**—Supports multiple authentication methods, such as port-based authentication, RADIUS, and access codes.
- **Accounting**—Supports accounting and payment methods including credit cards, RADIUS, and the property management system (PMS). The PMS and credit card billing can also allow impulse charges for additional bandwidth or future value-added services.
- **Portal**—Includes a forced portal, walled garden free access, and Connect (start) pages that you can customize.
- **Bandwidth options**—Supports options such as bandwidth throttling and bandwidth reservation.
- **Network deployment and configuration**—Includes multiple features to support network installation, configuration, and testing.
- **SDK**—A comprehensive software developer’s kit (SDK) can help you develop custom access or accounting policies or a PMS module for a new PMS interface.

BBSM is available as a preloaded server appliance, or you can purchase the software separately and install it yourself. If you are installing the BBSM software, refer to the *Cisco BBSM 5.3 Installation Guide* for instructions on installing BBSM and for the minimum hardware and software requirements. For information on obtaining the installation guide and other documentation, refer to the “[Obtaining Documentation](#)” section in the preface to this user guide.

New in Software Release 5.3

This section briefly describes some of the new features added to the BBSM 5.3.

System Summary web page

The BBSM System Summary web page provides status details for the BBSM server and its services.

Enhanced system event monitoring and alerts

The BBSM server now issues system events such as error, warning, and informational events to the Windows system Event Log using the standard Windows 2000 process. The server can be configured to generate Simple Network Management Protocol (SNMP) traps when an event is written into the Event Log.

Dual VLAN support

A second VLAN is now supported as an Institute of Electrical and Electronics Engineers (IEEE) protocol 802.1Q trunk to network devices so BBSM supports the separation of client traffic from management traffic.

Support for duplicate IP addresses

BBSM now supports static clients that have duplicate IP addresses. This includes multiple static clients with the same static IP address or multiple static clients with an IP address that overlaps the DHCP range on BBSM. The BBSM server automatically maps clients with duplicate static IP addresses to different network address translation (NAT) IP addresses. The client browsers are automatically redirected to the appropriate Connect page and then prompted to authenticate. This feature requires that port protection is enabled on network devices to prevent duplicate IP clients from interfering with each other.

Access codes by duration

Customers can now create an access code by duration. These access codes can be used for any amount of time within a year until no time is left for the access code.

PMS or print billing configured per server

As of this release, PMS or print billing is configured for each server, not each site.

SSL page sets disabled when SSL certificate is not installed on the BBSM server

When an secure sockets layer (SSL) certificate is not installed on a BBSM server, the page sets that require SSL cannot be chosen.

Security hardening

As of BBSM 5.3, the BBSM appliances ship with security *hardening*. Hardening BBSM involves disabling unnecessary services, removing and modifying registry key entries, and applying appropriate restrictive permissions to files and services to prevent exploitation. In addition to the BBSM server being

hardened, other devices on the network should also be configured to ensure proper security. Examples include filtering on firewalls, access control lists, and intrusion detection systems. A BBSM white paper describes the procedure for hardening a BBSM server:

http://www.cisco.com/application/pdf/en/us/guest/products/ps533/c1244/cdcont_0900aecd80093fe0.pdf

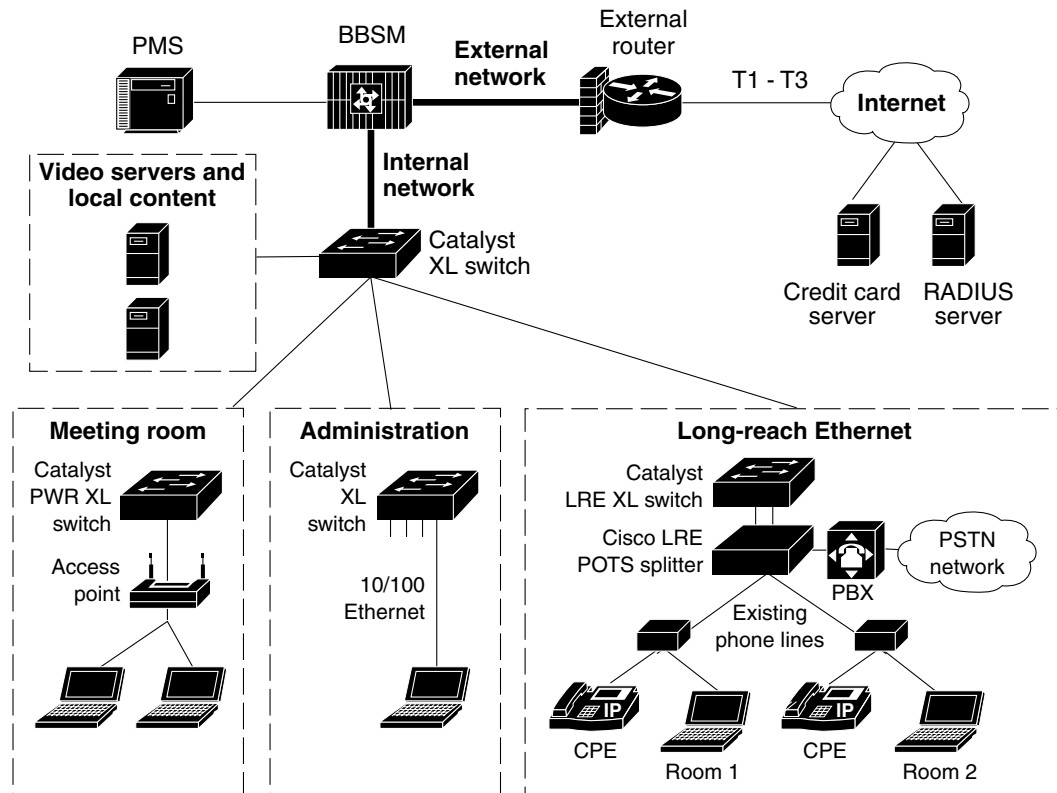
Transmission and Networking Options

BBSM manages the delivery of broadband services and the associated network devices. You can transmit BBSM data across various media and using various network types.

You can use existing phone lines, Ethernet, wireless LAN (WLAN), or cable to transmit or receive data using the BBSM server. For the Cisco Ethernet Catalyst switches, Cisco Aironet access points, and cable modem termination system (CMTS) that BBSM supports, refer to the *Cisco BBSM Products Supported Network Devices Guide*. The Cisco CMTS uses the coaxial cable that already exists in hotels, apartment buildings, and office buildings.

All traffic must pass through BBSM before it reaches the Internet. The BBSM server is assigned the predefined router number of 0 and always has an IP address of 127.0.0.1. This IP address is a loopback address that the BBSM server uses to communicate with itself. (Figure 1-1 shows a typical BBSM network.)

Figure 1-1 Typical BBSM Building Network

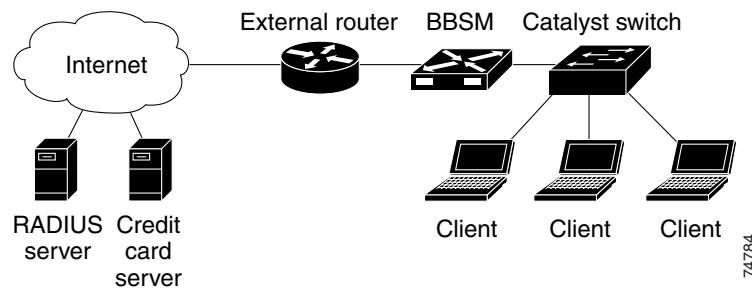


74786

The BBSM system supports the following types of networks:

- Bridged networks—A centrally located BBSM supports clients that use static IP addresses (“plug and play”) and supports DHCP clients. In a bridged network, packets do not pass through a router from the client to the BBSM server. Broadcast packets reach all network computers. All switches are on the BBSM server internal network and are associated with router number 0, which is the BBSM server. (See [Figure 1-2](#).)

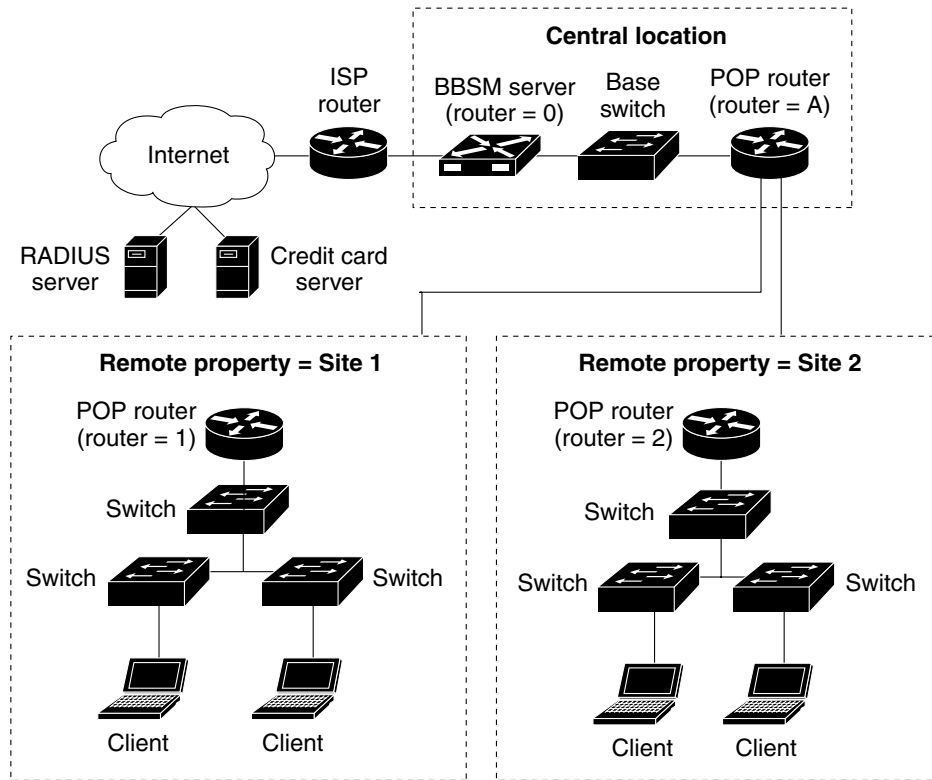
Figure 1-2 Basic Bridged BBSM Network



- Fully routed networks—Supports DHCP clients only. In a routed network, packets pass through one or more routers from the client to the BBSM server. Because BBSM does not have access to the client’s broadcast packets, plug-and-play is not supported. All switches are associated with routers numbered other than 0 (BBSM), and these routers are reachable through gateways on the BBSM internal network. (See [Figure 1-3](#).)

You must enter information in the BBSM WEBconfig about routers that act as a client’s default gateway. For example, in [Figure 1-3](#), you must specify routers 1 and 2, but router A does not need to be specified. Refer to [Chapter 12, “Configuring Network Elements.”](#) (This configuration is separate from configuring the routers themselves. To configure the router, refer to the product guide for the router.)

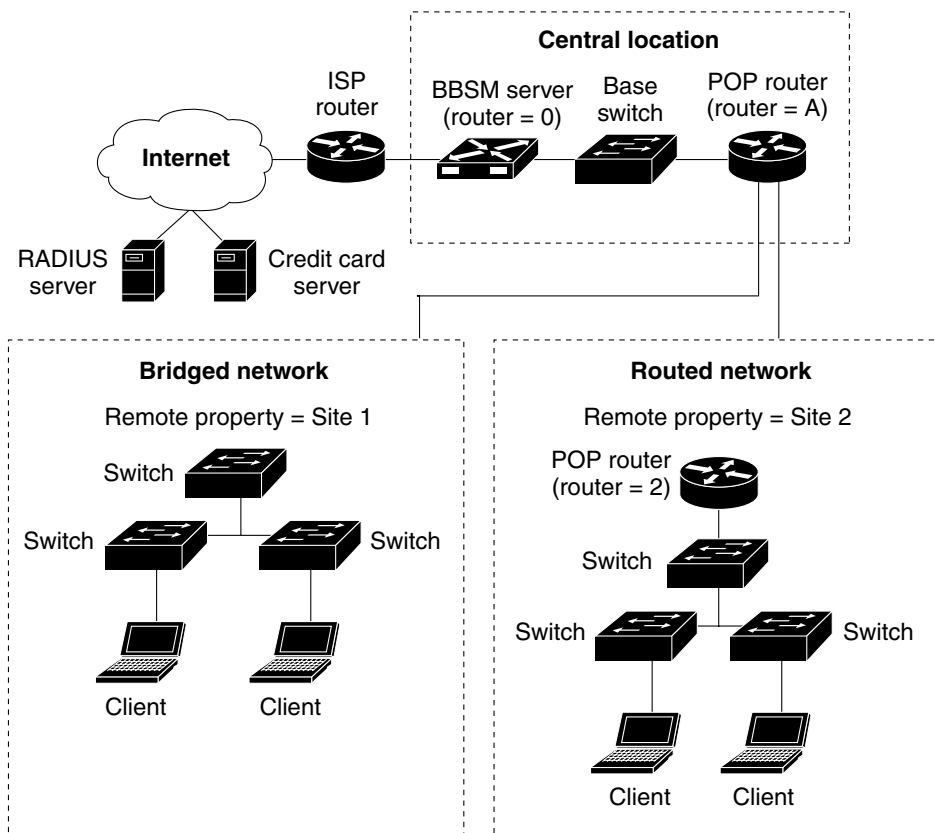
Figure 1-3 Basic Routed BBSM Network



74785

- Mixed networks—Integrated routed and bridged configurations are supported. Mixed routed and bridged networks include a bridged network and one or more routed networks. Some switches are on the BBSM server internal network, and others can be reached through gateways on the internal network. (See Figure 1-4.)

Figure 1-4 Basic Mixed and Routed BBSM Network



81627

Understanding the BBSM Dashboard

The BBSM Dashboard comprises three primary components—Administration, Operations, and Reports—that are based on user permissions. To perform system functions, select one of the sections under the components. These are the permissions of the corresponding user groups:

- Administrator—Can perform all system functions
- Operator—Can perform all Operations functions in the Dashboard Operations and Reports options.
- Reports user—Can view reports

The Dashboard and its components are described in the sections that follow.

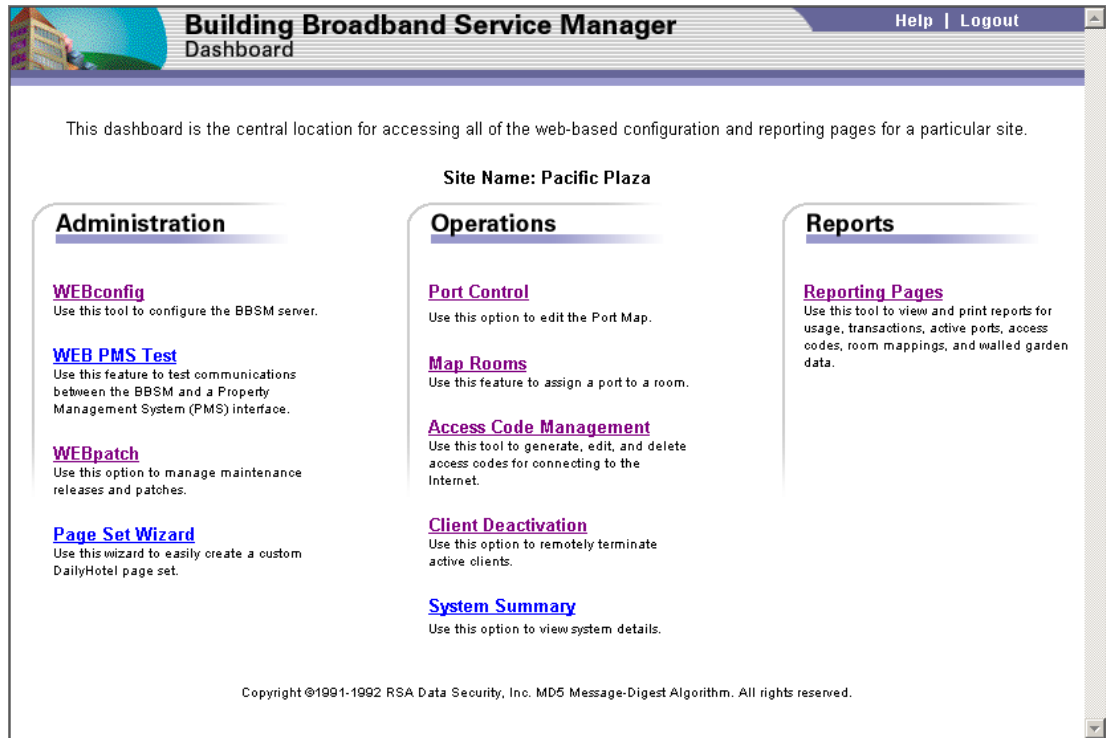
Dashboard

The Dashboard is the BBSM home page for accessing BBSM options. (See [Figure 1-5](#).) You can access the Dashboard locally or remotely:

- To access the Dashboard locally, double-click the Dashboard icon on the desktop. The Dashboard appears. (You can also choose **Start > BBSM Dashboard** to access the Dashboard.)
- To access the Dashboard remotely, launch Internet Explorer to access the BBSM server on port 9488 instead of the default web server port 80. Use one of the following:
 - To access BBSM from a remote location, enter this BBSM Dashboard URL:
http://<external_NIC_address>:9488/www, where <external_NIC_address> is the external network interface card (NIC) address of the BBSM server you want to access; for example, type **http://10.10.1.2:9488/www** and press **Enter**. The Enter Network Password dialog box appears.
 - To access the BBSM server within BBSM's internal network, enter this BBSM Dashboard URL:
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://192.168.42.1:9488/www** and press **Enter**. The Enter Network Password dialog box appears.
 - To access the BBSM Dashboard remotely via SSL, enter this URL: **https://<extNIC>/www** and press **Enter**. (You must have an SSL certificate installed on the BBSM server. Refer to the [“Installing an SSL Certificate”](#) section on page 16-2.
 - When you access the Dashboard remotely, you are prompted for a username and password. (Leave the domain name blank.) Your access level depends on the username and password that you enter:
 - Reports usernames are granted access to reports only.
 - Operator usernames are granted access to reports and operations.
 - Administrator usernames are granted access to all.

These usernames and passwords are created when a site is created. A site can be created in switch discovery or in WEBconfig during site configuration. (Refer to the [“Running the Switch Discovery Wizard”](#) section on page 5-6.)

Figure 1-5 Dashboard for Single Sites



If the BBSM system has multiple sites, the Dashboard contains a drop-down menu from which you select a site and then a Dashboard option.

Administration

The four Administration options enable you to perform all administrative tasks, including configuring the BBSM system. The Administration section requires that the user have the privileges of the Administrators user group, which is the default Windows 2000 Administrator group. Only users with full administrative rights can access these three options:

- **WEBconfig**—WEBconfig is the primary tool for configuring BBSM. Clicking WEBconfig displays the BBSM Server Settings web page and the navigation bar (NavBar) for selecting all of the web pages used to configure the system. (See Figure 1-6.) To close WEBconfig and return to the Dashboard, click the Dashboard link in the upper right-hand corner of the web page.
- **WEB PMS Test**—WEB PMS Test is used to test the physical connection and transfer of data between BBSM and the PMS.
- **WEBpatch**—WEBpatch is used to transfer and install service packs or patches for the BBSM software. With WEBpatch, you can update the BBSM server software remotely and obtain a list of details about the installed BBSM service packs, patches, and upgrades.
- **Page Set Wizard**—The Page Set Wizard enables you to create your own custom DailyHotel page set using a web-based wizard.

Figure 1-6 BBSM WEBconfig Default Web Page and Navigation Bar

The screenshot displays the BBSM WEBconfig interface. At the top, the navigation bar includes "Dashboard | Help | Logout" and the page title "Building Broadband Service Manager WEBconfig". A sidebar on the left lists "BBSM Server Settings" with sub-items: IP Addresses, Sites, Routers, Network Elements, Port Test Settings, Billing (Security/SSL), Bandwidth Reservation (Custom Page Sets, Walled Garden), Port Hopping, and WEB Printing Alerts. The main content area features the Cisco Systems logo and "BBSM Server Settings" header. It is divided into three sections: "BBSM Software Information" (Version: "5.3", Updates: "None"), "Network Configuration" (with checkboxes for "Enable Maximum Active Sessions" (checked), "Enable Transparent Proxy", and "Enable Duplicate IP Addresses", plus input fields for "Maximum Active Sessions" (23), "SMTP Forwarding Server", and "Currency Type" (USD)), and "Bandwidth Management" (with checkboxes for "Enable Bandwidth Throttle" and "Access Code Bandwidth" (None)). A "Latest Update" notice is highlighted in yellow on the right, along with instructions for "Enable Duplicate IP Addresses", "SMTP Forwarding Server", "Currency Type", and "Enable Bandwidth Throttle". At the bottom of the main area are "Defaults", "Requery", and "Save" buttons. A vertical ID "R1078" is visible on the right edge.

Table 1-1 describes the WEBconfig web page options.

Table 1-1 WEBconfig Web Page NavBar Options

Web Page	Description
BBSM Server Settings	Configures server-wide settings such as bandwidth management, transparent proxy, and the SMTP forwarding IP address.
IP Addresses	Configures the IP address ranges for the BBSM server and the network equipment.
Sites	Manages site data and locations.
Routers	Sets router interface parameters. Enables you to configure routes to the switches and to the client computers attached to these switches. (This feature is for routed networks and is not related to WAN activities.)
Network Elements	Expands to the Access Points, CMTS (cable modem termination system), and Switches web pages for each site: <ul style="list-style-type: none"> Access Points—For a particular site, sets access point parameters, such as the access point IP address and type. CMTS—For a specific site and CMTS, sets the CMTS mode, parameters, and cable modem IP address ranges and DHCP options. Switches—For a particular site, cluster, and switch number, sets the switch parameters, such as number of client ports, cluster IP address, router IP address, and Cisco switch type. Each site can support multiple clusters, and each cluster can support up to 16 cluster-capable switches.
Port Test Settings	For each site, expands to the Port Test Settings web page, which enables you to select the port test parameters, including switch mode.
Billing	Expands to the PMS/Print, RADIUS, and Credit Card web pages, which define the billing features for the site: <ul style="list-style-type: none"> PMS/Print—Expands to enable you to configure the PMS settings and call types. RADIUS—Enables you to configure the RADIUS server parameters and the multiple concurrent RADIUS sessions for each site. Credit Card—Enables you to configure the credit card server parameters and the merchant ID number for each site.
Security/SSL	Configures the domain name for SSL page sets, changes the MSDE <i>sa</i> password, and changes the BBSD and Web API accounts.
Bandwidth Reservation	Expands to the External Router, Total Bandwidth, and Classes of Service web pages: <ul style="list-style-type: none"> External Router—Configures the IP address and the Telnet <i>terminal</i> and IOS <i>enable</i> passwords. Total Bandwidth—Sets the router bandwidth parameters for total property and unreserved users. Classes of Service—For the router, sets the class of service parameters. If you are entering the external router information in WEBconfig remotely, Cisco recommends using SSL to connect to the Dashboard. This will protect the sensitive data that is entered on this page.
Custom Page Sets	Adds your new custom page sets and sets the associated Start page. The page set then appears in the Page Set drop-down menu when you are configuring port settings from your Network Elements web page.
Walled Garden	Enables you to configure walled garden web sites, which let the end user view the web sites that you specify as free of charge.

Table 1-1 WEBconfig Web Page NavBar Options (continued)

Web Page	Description
Port Hopping	Configures the port hop delay.
Alerts	Enables or disables SNMP alerts. When alerts are enabled, you can enter parameters such as what level of alerts to send and where to send them.

Operations

The following options are available under the Operations section of the Dashboard, which requires users to be in the Operators or Administrators user groups. Users in these groups can view all Operations reports and perform all Operations functions:

- **Port Control**—The Port Control web pages enable you to view a list of port control data to perform maintenance for ports and edit per-port policies.
- **Map Rooms**—The Map Rooms web pages enable you to change port assignments for a room, a meeting room, or a public space.
- **Access Code Management**—Access code management enables you to generate, edit, delete, and view access codes.
- **Client Deactivation**—This option enables you to remotely terminate active client sessions and reactivate them.
- **System Summary**—The System Summary web page enables you to monitor the BBSM system status and all BBSM services.

If you need to add Operator users, refer to your Windows 2000 documentation for instructions and then choose **Start > Programs > Administrative Tools > Computer Management > Local Users and Groups** to create the new users. After creating the users, add them to these two Windows groups:

- BBSM Operator
- BBSM Operator for site *x*, where *x* is the site number

Reports

The Reports option consists of the Reporting Pages section, which enables you to view BBSM operational data. Users can be in the Reports, Operators, or Administrator user group. The interface consists of seven web pages that are accessible from a toolbar at the top of the page. To close Reports and return to the Dashboard, click the Dashboard link in the upper right corner.

If you need to add Reports users, refer to your Windows 2000 documentation for instructions and then choose **Start > Programs > Administrative Tools > Computer Management > Local Users and Groups** to create the new users. After creating the users, add them to these two Windows groups:





- BBSM Reports
- BBSM Reports for site *x*, where *x* is the site number

Using Navigation Buttons

Use the BBSM web page navigation buttons to find the correct record before making changes. (See [Table 1-2](#).)

When no records exist for that function, the button is disabled. For example, the First and Previous buttons are disabled when you are viewing the first record.

Table 1-2 *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.

Connecting a Client to BBSM

To connect a client to BBSM, the client should meet minimum requirements to ensure successful operation. This section describes those requirements and how end users connect to the BBSM server. [Table 1-3](#) shows the operating system and browser versions that have been tested and are supported for BBSM 5.3.

Table 1-3 *Minimum End-User Client Connection Requirements*

Component	Tested and Supported for BBSM 5.3
Operating system	Windows 98, 2000 Professional, and XP Professional Red Hat Linux 7.1 Macintosh OS9.0 and OS10.0
Browser	Internet Explorer 5.0 or later Netscape Navigator 4.7x or later
Color depth	256 colors (65,000 colors recommended)
Screen Area, pixels	800 by 600 For Compaq H3635 and H3760 iPAQ pocket PCs: 240 by 320 limitation. (For additional information about configuring a pocket PC, refer to the <i>Cisco BBSM SDK Developer Guide</i> .)

The page set that the BBSM administrator selects in the Switch Discovery Wizard or from the Page Set drop-down menu in the WEBconfig Network Element Port Settings pop-up window determines which Connect page the end user uses to connect to the Internet.

The following example demonstrates a general connection sequence for an end user.

A hotel has purchased a BBSM server, set it up, and selected the DailyHotel page set. After checking into a hotel room, an end user with a laptop computer might do the following:

1. Connect the laptop to the jack using a standard 10BASE-T Ethernet cable and turn it on.
2. Launch the browser. The DailyHotel Connect page appears.
3. If applicable, enter any requested authentication information.
4. Click **Connect** (or **Submit**). The end user is then redirected to a *Connecting...* window and then to the configured portal page for the hotel.

