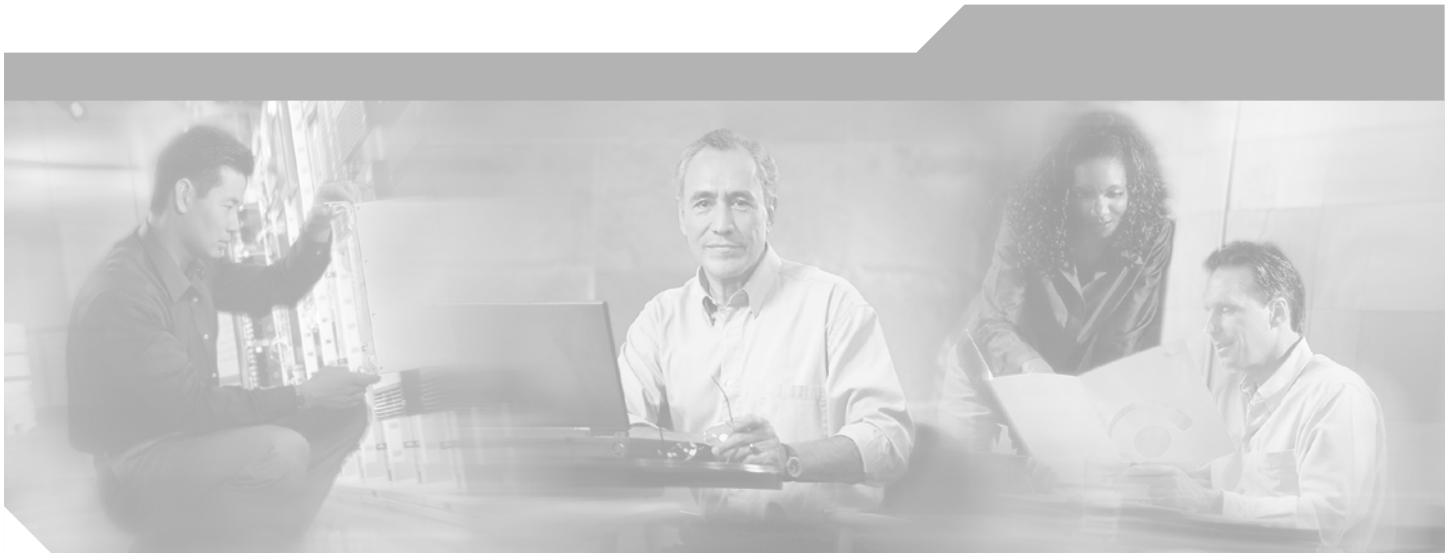


Cisco BBSM Software Configuration Guide

Software Release 5.1
August 2002

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-1566-03

CONTENTS

Preface

Audience

This guide is written for personnel responsible for configuring and maintaining the Building Broadband Service Manager (BBSM). The guide explains how to configure and define specific characteristics for BBSM networks. After BBSM has been configured, it is ready to be used at each site.

Purpose

The purpose of this guide is to help configure BBSM for operation on a site-by-site basis. During daily operation, BBSM uses the information provided during configuration to recognize the sites, ports, switches, and other related network equipment. The result allows service providers to offer Internet services on a port-by-port basis.

Note Note that the term *customer* refers to the individual or organization that purchased BBSM. The term *end user* refers to the service provider's or property owner's customer that is accessing the Internet through the BBSM system.

Organization

This guide is organized into the following chapters and appendixes.

Chapter/Appendix		
No.	**Title**	**Description**
1	Overview	Lists the software features and deployment options of this release. It provides examples of how the BBSM server is integrated into a network.
2	Preconfiguration and Setup	Provides the necessary steps to prepare the BBSM system for configuration, including setting up a Site Controller.
3	Basic BBSM Configuration (WEBconfig)	Describes how to configure the BBSM server by using the WEBconfig feature accessed under the Administration section on the BBSM Dashboard.
4	Testing the PMS Interface (WEB PMS Test)	Describes how to test the PMS interface by using the WEB PMS Test feature accessed under the Administration section on the BBSM Dashboard.
5	Installing Service Packs, Patches, and Upgrades (WEBpatch)	Describes how to install service packs, patches, and upgrades by using the WEBpatch feature accessed under the Administration section on the BBSM Dashboard.
6	BBSM Operations	Describes the four functions under the Operations section of the BBSM Dashboard: Port Control, Map Rooms, Subscription Port Control, and Access Code Management.
7	Viewing and Printing BBSM Reports	Discusses the reporting options available from the BBSM Dashboard.
8	Customizing Your BBSM System	Describes the additional features and options of your BBSM system.
9	Web Printing	Explains how to add a web printing option for end users.
A	BBSM Basics	Describes the features and options that make up the BBSM architecture.
B	Using the BBSM Interfaces	Describes the two GUI interfaces—the BBSM Dashboard and WEBconfig—that are key to the configuring and using BBSM.
C	Installing an SSL Certificate	Describes how to acquire and install an SSL certificate to provide Internet security through the BBSM server.
D	Using RADIUS Authentication, Authorization, and Accounting	Explains how to use RADIUS with the BBSM system.
E	Understanding Port Hopping	Describes port hopping as it applies to the BBSM system.
F	BBSD Feature	Describes the Building Broadband System Director (BBSD) feature.
G	Configuring a Laptop for Room Mapping	Explains how to configure your laptop so it can be used to map the room ports.

Conventions

This publication uses the following conventions to convey instructions and information:

- Commands and data you type are shown in **bold**.
- Variables or parameters for which you supply values are shown in angle brackets (< >).
- Terminal sessions and screen displays are shown in `screen` font.
- Optional elements are shown in square brackets ([ ]).

Notes and cautions use these conventions and symbols:

Note This note symbol means *take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution This caution symbol means *be careful*. This action can result in equipment damage, loss of data, or interruption of service.

Related Publications

These documents provide complete information about the BBSM:

- *Requires Immediate Attention Card for Cisco BBSM Server* (available on Cisco.com)
- *Cisco Building Broadband Service Manager and Director Installation Guide* (order number DOC-7812741=)
- *Cisco Building Broadband Service Manager Hardware Assembly Guide* (available on Cisco.com)
- *Cisco BBSM Software Configuration Guide, Software Rel. 5.1* (available on Cisco.com)
- *Cisco Building Broadband Service Director Software Configuration Guide* (available on Cisco.com)
- *Cisco BBSM SDK Developer Guide, Software Rel. 5.1* (available on Cisco.com)
- *Cisco IPORT 4.5 to Building Broadband Service Manager 5.1 Data Transfer Utility Guide* (available on Cisco.com)
- *Cisco Building Broadband Service Manager 5.0 to 5.1 Upgrade Guide* (available on Cisco.com)

To ensure you have the latest information on BBSM, before installing, configuring, or upgrading the BBSM server, refer to the release notes on Cisco.com.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

BBSM documentation is available from this Cisco.com website:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm51/index.htm

All release notes for BBSM 5.1 are located at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm51/relnotes/index.htm

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Support for Cisco Interface Specifications and APIs

Cisco has a new support program for developers who are enabling products with Cisco-supported interfaces. The Developer Support Program provides formalized support for Cisco interfaces to enable developers, customers, and partners to accelerate the delivery of compatible solutions to Cisco customers.

The Developer Support engineers are an extension of the product technology engineering teams. They have direct access to the resources necessary to provide expert support in a timely manner.

The Developer Support Program offers the following benefits:

- Minimal support fees
- Flexible support model—Purchase support as needed, or for a period of time
- Consistent level of support—Defined problem priority and escalation guidelines
- Deliver products to market faster—Dedicated program with interface experts to assist you

To find out more about this program and obtain the Developer Support Agreement, go to the Developer Support Program web site at the following URL:

http://www.cisco.com/go/developersupport

After receiving your signed agreement, we will send you your contract ID number and instructions for opening support cases with Cisco Developer Support engineers.

We look forward to working with you. Please do not hesitate to contact us at the following e-mail address if you have further questions about this program:

developer-support@cisco.com

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Overview

Cisco Building Broadband Service Manager (BBSM) is a software-based service creation platform that enables service providers or property owners to create, market, and operate broadband access services, such as high-speed Internet access. BBSM provides plug-and-play end-user connections, tiered service levels, and custom user session management. With BBSM, customers can provide their own services, which reduces support requirements and increases usage.

BBSM supports multiple authentication and billing options, including credit card, property management system (PMS), and access codes. The comprehensive software developer's kit (SDK) enables customers to customize interfaces. BBSM is available as a preloaded server appliance.

Deployment Options

BBSM manages both the delivery of broadband services and the attached network elements used to deliver these services. A centrally located BBSM server on a switched network provides Dynamic Host Configuration Protocol (DHCP) and static (plug-and-play) support. If the network is routed, only DHCP is supported because BBSM never sees the client MAC address.

The BBSM platform enables property owners and service providers to create tiered service levels in order to deliver targeted customer offerings. For instance, a hotel can set up daily network access for a series of meetings, which provides a variety of bandwidth/pricing options to capture meeting room revenue opportunities. Table 1-1 shows different ways to deploy BBSM.

Table 1-1 BBSM Deployment Options

Deployment	Description
Long-Reach Ethernet	The Cisco long-reach Ethernet (LRE) networking solution is the industry's first end-to-end product line for delivering 5- to 15-Mbps performance over existing Category 1/2/3 wiring. Cisco LRE is an ideal technology for multi-unit building (MxU) and enterprise campus environments. MxU buildings include hotels, residential multidwelling units (MDUs), and commercial multitenant units (MTUs). Enterprise campuses include manufacturing, educational campuses, and hospitals.
Wireless LAN	The Cisco Aironet 350 series of wireless LAN (WLAN) products leads the industry in performance, security, and reliability with cost-effective solutions for multi-unit buildings and public spaces.
10/100/1000 Ethernet	Cisco's full-range of 10/100/1000 Ethernet switches spans multiple product lines that address building requirements and future application needs. The product families include the following: • Cisco Catalyst 3550-12T Switch • Cisco Catalyst 3500 Series XL • Cisco Catalyst 2950 Series • Cisco Catalyst 4000 family • Cisco Catalyst 6500 Series
Cable	Cisco uBR7xxx cable modem termination system enables cost-effective, high-speed Internet access in the hotels, apartments, and office buildings by using the existing coaxial cable already in a building.

Linking Network Elements to BBSM

The BBSM system supports the following types of networks:

- Bridged networks
- Fully routed networks
- Mixed (bridged and routed) networks

The BBSM server, which is the “router” that all traffic must pass through before reaching the Internet, is assigned router number 0. This number is predefined and always has an IP address of 127.0.0.1. It is a loopback address that the BBSM server uses to communicate with itself.

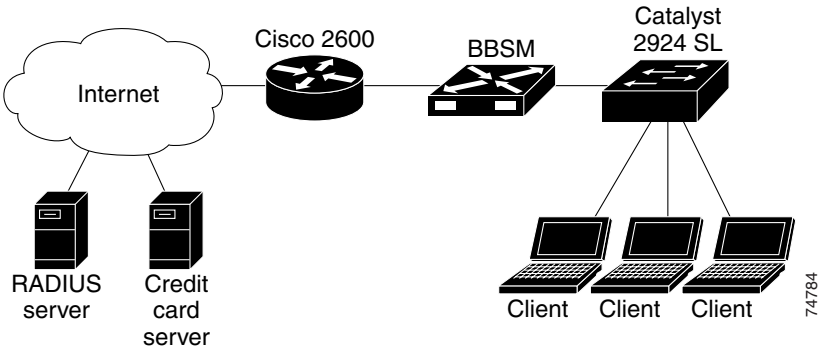
Bridged Networks

In a bridged network a packet does not pass through a router from the client to the BBSM server. BBSM is the “router” that connects the bridged network to the Internet. Broadcast packets reach all computers on the bridged network. (See Figure 1-1.)

Bridged networks are supported by associating all switches with router number 0, which is the BBSM server. All switches are on the BBSM server internal network.

Caution For some plug-and-play features to work, BBSM must use a bridged network.

Figure 1-1 Basic Bridged BBSM Network



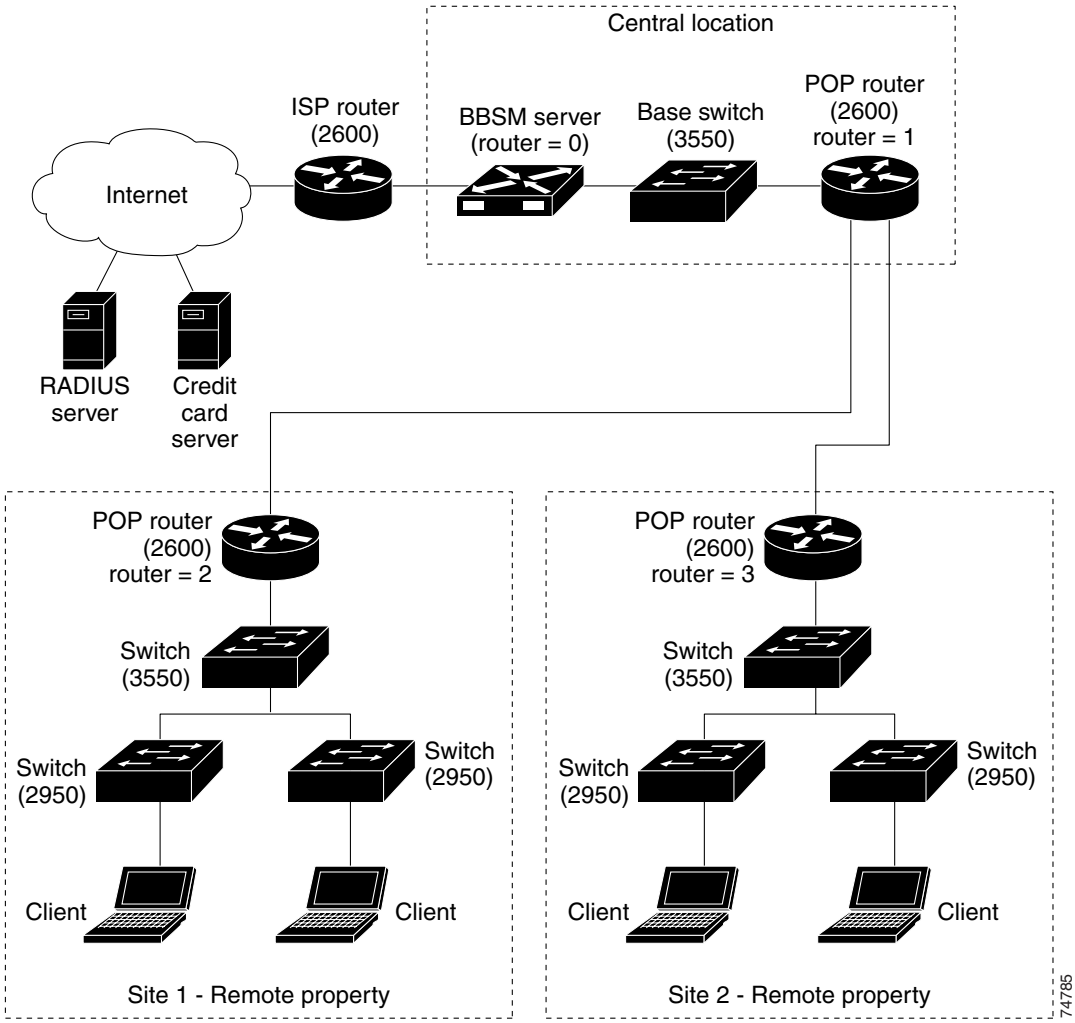
Routed Network

In a routed network a packet passes through one or more routers from the client to the BBSM server. BBSM does not have access to broadcast packets and does not support plug-and-play for these networks. (See Figure 1-2.)

Fully routed networks are supported by associating all switches with routers other than router number 0. All switches are on networks attached to routers that are reachable through gateways on the BBSM server internal network.

For routed networks, you must enter information about the routers within the BBSM internal network. Use the Routers web page to configure routes to the switches and routes to the client computers (end users) attached to the switches.

Figure 1-2 Basic Routed BBSM Network



Combined Routed and Bridged Network

Mixed 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.

User Groups and Permissions

In addition to the default Windows 2000 user group called Administrators, the BBSM server comes with two user groups already created: Operators and Reports. These three user groups provide security and control access of users to run web applications or open, edit, and view the reports. When the BBSM Web Printing feature is enabled, a fourth user group called Printers is created.

These three user groups are reflected on the BBSM Dashboard (Dashboard) by the following sections:

- Administration
- Operations
- Reports

(See Figure 1-3 on page 1-7.)

If additional Operator users need to be added, they must be added to these two groups:

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

If additional Report users need to be added, they must be added to these two groups:

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

Note To create additional Operator or Reports users, refer to your Windows documentation for detailed instructions.

Administrators

The Administrators user group has full system permission and rights. Administrators can alter any BBSM configuration setting and have access to all Dashboard options.

For example, this group has access to the web applications and can view all reports, add and delete access codes, and edit room mapping.

Operators

The Operators user group can view all reports and web applications and all the options located in the Dashboard under the Operations heading:

- Port Control
- Map Rooms
- Subscription Port Control
- Access Code Management

Reports

The Reports user group has access only to the Reporting Pages option on the Dashboard. This group can open a Room Mapping Report and verify room and port, but cannot edit room mapping. This group cannot add, update, or delete access codes.

Printers

When BBSM Web Printing is enabled, a group called Printers is created for each site that is part of the Administrators group. This group is only used for installing printers.

BBSM Configuration Interfaces

Most of the BBSM configuration and operation is handled through two graphical user interfaces (GUIs):

- Dashboard
- WEBconfig

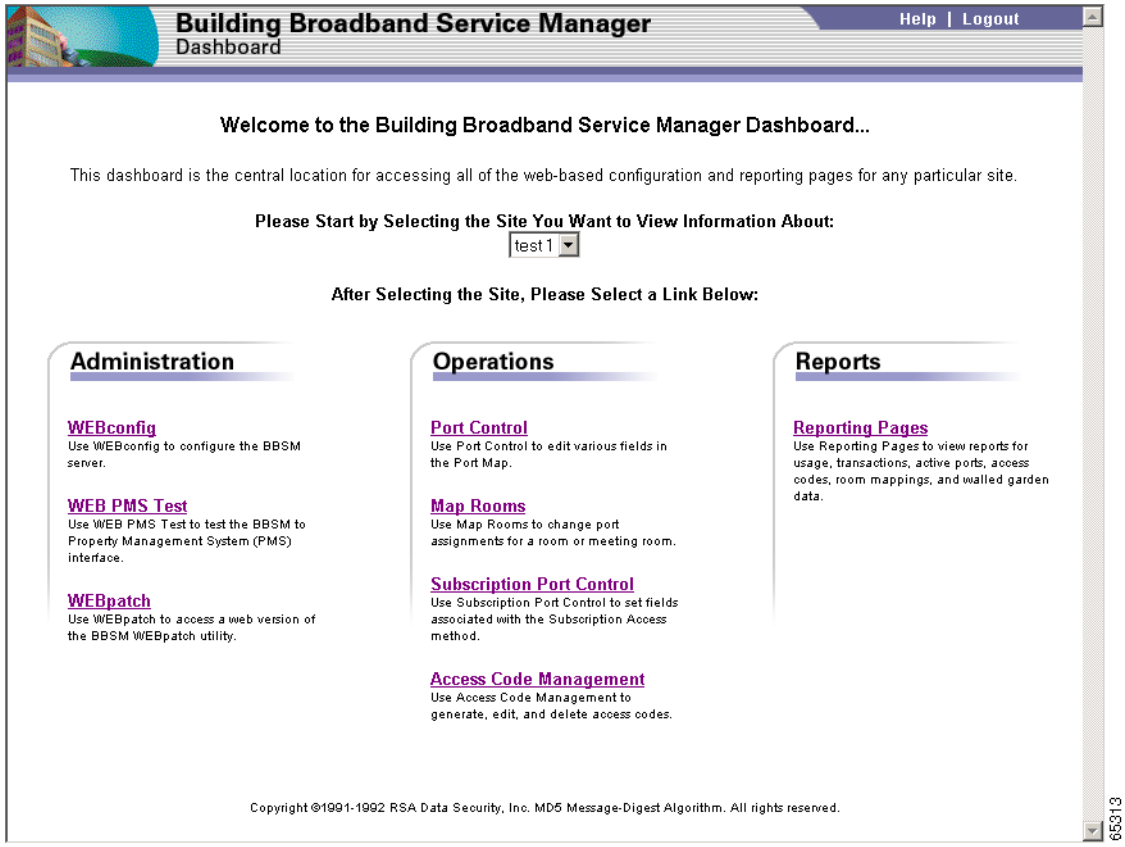
Dashboard

BBSM can be accessed locally at the BBSM console and remotely over the Internet using Internet Explorer. The BBSM home page and starting point is the Dashboard. (See Figure 1-3.) For convenience, an icon is located on the BBSM desktop. For more detail on the Dashboard, see Appendix B, "Using the BBSM Interfaces."

Note You can access BBSM server web pages on port 9488 instead of the default web server port 80. Add ":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, such as in a room connected to a BBSM port, you must activate a session and connect to the Internet to access to these pages.

Figure 1-3 BBSM Dashboard

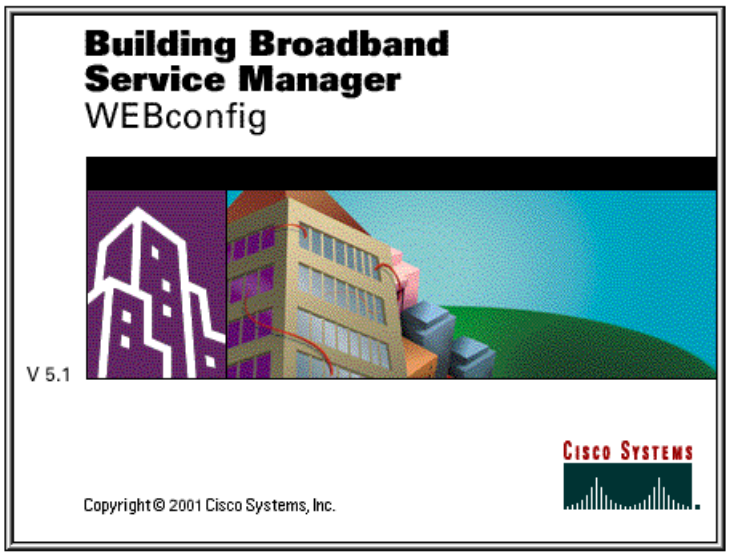


WEBconfig

WEBconfig is a web-based GUI used to configure the BBSM software to reflect your actual operating environment. It is the primary component used in the configuration of BBSM and provides access from its button bar to the various web pages used in that configuration.

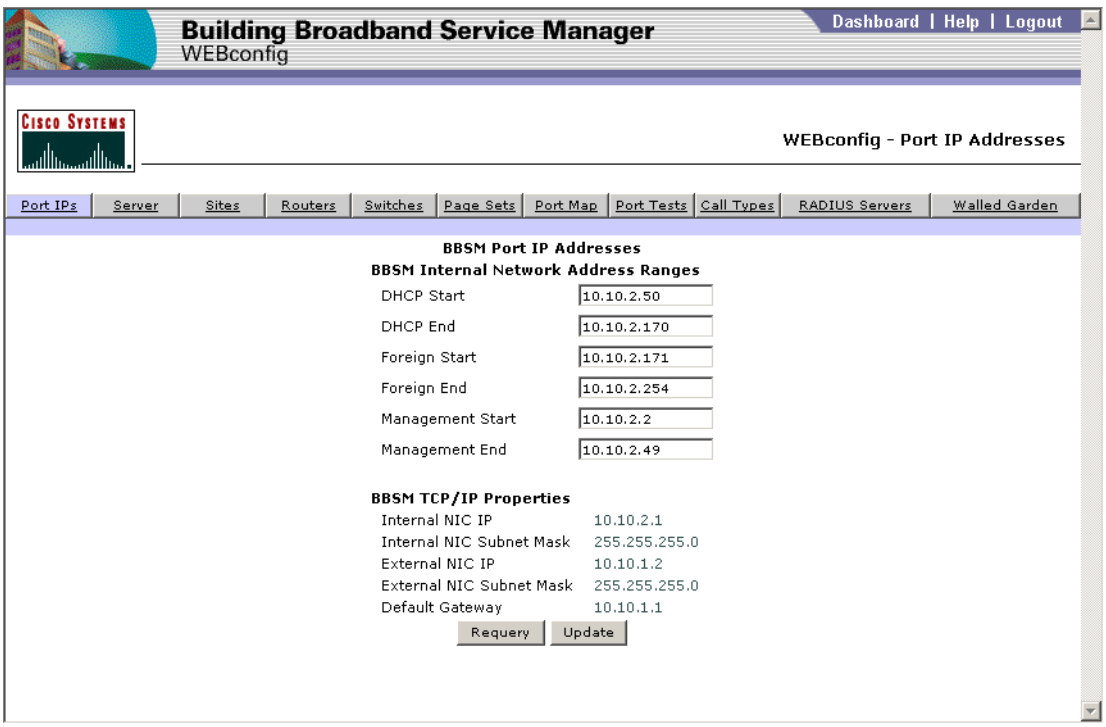
When WEBconfig is first launched, a splash screen appears. (See Figure 1-4.)

Figure 1-4 WEBconfig Splash Screen



The WEBconfig interface automatically appears after a few seconds or when you click the splash screen. The initial web page displayed is always the Port IP Addresses web page. (See Figure 1-5.)

Figure 1-5 Port IP Address Web Page



Pricing and Page Sets

A page set is a set of active server page (ASP) files that defines the access and accounting policies used for a end-user session. Defining the policy in a server-side web page is a more powerful way to customize the session and allows other technologies to be integrated into the Internet service.

Page Set Design

Page sets are written in Microsoft JScript, JavaScript, VBScript, and HTML. They are executed on the BBSM server when the end user requests them from the web browser. With page sets, you can define the end-user experience from first impression through disconnect. A typical group of ASP files can contain the following:

- A connect page
- A connected page
- An authorization fail page
- A welcome back page

Through the page set, you associate an access policy with a specific port. The page set may also include an accounting policy to determine billing parameters. Different policies contain different sets of pages depending on the BBSM features for each port. When configuring ports, you can use one of the default page sets that comes with BBSM, use one of the sample page sets from the BBSM Software Developer's Kit (SDK), or have your web developer create a custom set of pages.

Your web developer can use the default policies as templates to create a policy to meet your specific needs. The default web pages use a standard naming convention that uses the access or accounting policy name for the page set name.

When customizing a page set, use the Page Sets web page to assign the new page set to the system.

As part of the configuration process, use Windows Notepad to customize BBSM pricing, bandwidth, or session information. This information is located in ASP files in the c:\atcom\ekgnkm folder.

Note For greater detail on page set construction and design, see the *Cisco BBSM SDK Developer Guide.*

Access Policies

An access policy defines the connection process that the end user experiences when connecting to the Internet through BBSM. Every port is associated with a particular access policy.

BBSM includes default, built-in access policies as shown in the list that follows. Your web developer can add new access policies to the system using the BBSM SDK.

The administrator can assign any of the following access policies to any port:

- Access Code
- Block
- Daily
- Minute
- RADIUS

- Subscription

Accounting Policies

Through an accounting policy or method, you can determine how end users are to be billed for BBSM Internet services. An accounting policy is included in most, but not all, page sets, along with the page set's access policy. Accounting policies are usually available in one of two forms:

- Standard form that uses SSL security to transmit data
- Clear form that transmits the data in the clear

When using the standard secure form, you must buy and install a SSL certificate. See Appendix C, "Installing an SSL Certificate" for complete details on installing the certificate.

The following default accounting policies come with BBSM:

- ICS Credit Card
- Cruise Line
- Hotel Billing
- RADIUS Accounting

You can edit these policies or create new accounting policies to the system using the BBSM SDK.

Using the SDK

The BBSM SDK is available for download from Cisco Connection Online. The *Cisco BBSM SDK Developer Guide* is also downloadable and details all the steps needed to produce page sets for BBSM.

Preconfiguration and Setup

Before you can begin configuring a BBSM server for your network, you must take several preliminary steps, and all network elements must be set up and configured. This chapter covers these critical steps. In addition, be sure to read the cautions below before proceeding.

Caution Do not change the Windows 2000 computer name of your factory-installed BBSM appliance, because the BBSM MSDE database has the name embedded in the application. Changing the name will break the BBSM MSDE function, and you will begin to see SQL server errors being reported on your BBSM server. The only solution to this problem is to reinstall the server from scratch so that the MSDE database function is reinstalled. This problem is a Microsoft issue and not one that the Cisco software team can resolve. If you want a different computer name for your BBSM or BBSD server, you must purchase the CD version of the BBSM software and install the software on a clean Windows 2000 server that already has the desired computer name configured.

Caution The BBSM password must match the SNMP Read/Write Community String password that is configured in the switch hardware. If the BBSM password does not match the switch community string (password), BBSM cannot communicate with the switch, and BBSM cannot locate the end users connected to the switch. Note that the switch password can only be changed by following the switch manufacturer's procedures. Refer to these configuration instructions to change this password.

Caution If you use Netscape for your web browser, because of known compatibility issues with Netscape 4.7x and earlier, you must use Netscape 4.8 or higher for BBSM to work properly.

Caution When BBSM is installed, the user is prompted for a BBSD username and password. BBSM creates a Windows user account and a SQL server login using this username and password. Both logins are required for BBSD to function. BBSD stores a username and password for each BBSM server. For BBSD to connect to each BBSM server, the stored username and password must match both the Windows BBSD login and the SQL server login on the BBSM server. See the *Requires Immediate Attention Card for Cisco Building Broadband Service Manager Server* for detailed steps.

Caution When using WEBconfig web pages, all active services are stopped when you click Update. This action commits configuration changes to the BBSM server. After the settings are updated, services automatically restart. To prevent disrupting end-user sessions, make changes only when there are no active sessions. The current number of active sessions is found on the server web page.

Confirming Web Access

Before configuring your BBSM server, be sure a live Internet access point is available at the server. Confirm the configuration of any switches or routers used to access the Internet.

Caution For security purposes, before attaching the BBSM to the Internet connection, be sure you have changed the default passwords. Refer to the *Requires Immediate Attention Card for Cisco Building Broadband Service Manager Server.*

If you use a Cisco Building Broadband Service Director (BBSD) server to manage BBSM servers, you must change the BBSD account passwords located on each BBSM server. The BBSD Windows client password must match the BBSD MSDE client password. Be sure you use the same password for both BBSD accounts.

Also, install all recommended service packs, patches, and security fixes before attaching the BBSM server to the Internet connection.

Installing a Site Controller

Sites that need a network connection to a Property Management System (PMS) or have a printer attached to the site must use a BBSM site controller to manage those connections.

These are the minimum hardware requirements for the site controller PC:

- 133 Mhz Pentium
- 64 MB RAM
- 1 GB hard drive with at least 650 MB free
- VGA card
- Network card
- Two serial ports
- One parallel port

Note Before creating and configuring any additional sites in WEBconfig, make sure any BBSM network cabling, hardware, routers, switches, or stacks are attached to the new site.

Connecting All Necessary Hardware

The site controller computer hardware must be capable of running Windows 2000 Professional and have the following equipment:

- An Ethernet card to connect to the internal BBSM network behind the site router
- A serial or parallel port to connect to a printer (if using a printer)
- A serial port to connect to a PMS (if using the PMS interface)

Before configuring the site controller you must do the following:

- Connect the site controller to the site router or switch using an IEEE 802.3 Ethernet cable with a RJ-45 connector
- Connect printer (if using a printer)
- Connect PMS to serial port (if using the PMS interface)
- Install Windows 2000 Professional and Message Queuing on the site controller using Microsoft instructions

Configuring the IP Address on the Site Controller

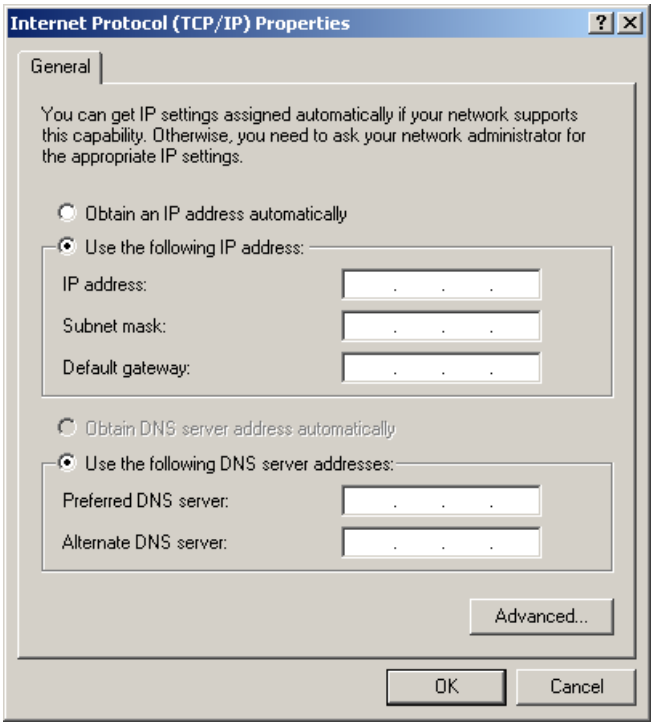
Configure the site controller with a static IP address in the management range that is specified on the Port IPs web page.

Step 1 Right-click **My Network Places** and select **Properties**.

Step 2 Right-click **Local Area Connection** (NIC) and select **Properties**.

Step 3 Double-click the **Internet Protocol** component. The Internet Protocol (TCP/IP) Properties window opens. (See Figure 2-1.)

Figure 2-1 Internet Protocol (TCP/IP) Properties Window



Step 4 Click **Use the following IP address**.

Step 5 Enter the IP address for your site controller.

Step 6 Enter the Subnet mask used by the internal adapter of your BBSM server.

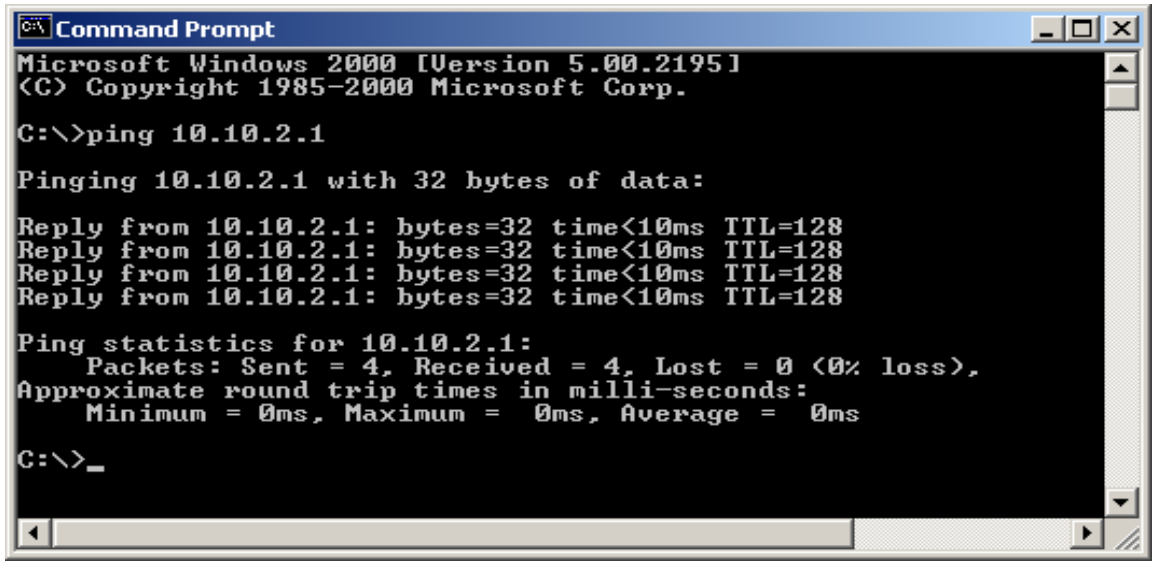
Step 7 Enter the internal adapter IP address of the BBSM server as the Default gateway.

Step 8 Click **OK**.

Step 9 Choose **Start > Programs > Command Prompt**.

Step 10 At the command prompt, type **ping xxx.xxx.xxx.xxx** (where xxx.xxx.xxx.xxx is the internal adapter IP address for the BBSM server you entered as the gateway in Step 5).

Figure 2-2 DOS Screen



Step 11 Press **Enter**.

Step 12 Type **exit** and press **Enter** to close the window.

Installing Site Controller Software

Use this procedure to install the site controller software.

Step 1 Insert the BBSM Installation CD into the BBSM CD-ROM drive. The BBSM Installation Wizard appears.

Step 2 Click **Exit** to close the BBSM Installation Wizard.

Step 3 From the CD-ROM drive, double-click the **Athdmn** folder.

Step 4 Double-click **Setup.exe** to open the site controller Installation Wizard.

Step 5 From the Welcome window, click **Next**. Wait while files are copied to the server.

Step 6 Select **Yes, I want to Restart the Computer**.

Step 7 When the Setup Complete dialog box appears, click **Finish**.

Step 8 Choose **Start > Settings > Control Panel > Add/Remove Programs > Add/Remove Windows Components** to install Message Queuing Services. Follow the Microsoft software program addition instructions.

The site controller is now ready for use with the BBSM system.

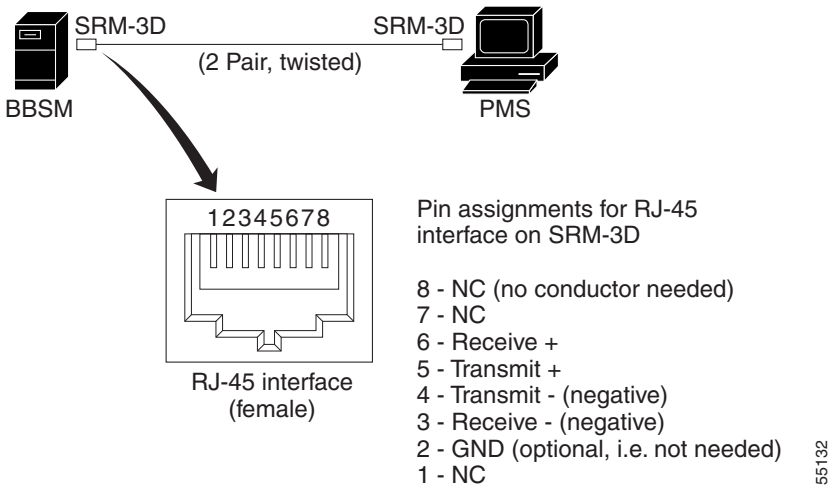
Connecting to a PMS

To connect a BBSM server or site controller to a serial port on the PMS, you need a null modem cable (modem cable that swaps transmit and receive lines) rather than a straight-through cable. Check with the hotel property PMS vendor to determine specific cabling requirements.

- For a single property site, connect a serial cable from the BBSM server to the PMS.
- For multiple property sites, for each property using a PMS, connect a serial cable from the site controller to the PMS.

Use a short-haul modem if the distance between the BBSM server and the PMS is greater than 50 feet. As an example, the RAD SRM-3D short-haul modem has been used successfully with previous BBSM installations. (See Figure 2-3.)

Figure 2-3 Modem Connection using RAD SRM-3D Connection



The short-haul modem connects from the BBSM server to the PMS using a crossover cable. To have a good connection, make sure that Transmit+ on one modem connects to Receive + on the other modem, and Transmit - from the first modem connects to Receive - on the other modem.

Verifying Prerequisites

Before you configure BBSM, make sure that the following tasks have been completed:

- Verify that network configuration information from the Site Survey, network diagrams, and configuration maps for your particular network topology are available.
- Confirm the configuration information specific to the routers, stacks, and/or switches that will be used with the BBSM server.
- Connect all hardware components, including the keyboard, mouse, and VGA-compatible monitor.
- If you are using secured (https) pages, obtain and install a Certificate Authority (third party SSL). (See Appendix C, “Installing an SSL Certificate.”)

Preparing the BBSM Server

This section explains how to prepare the BBSM server by doing the following:

- Changing the passwords
- Installing service packs and/or patches
- Running the Address Change Wizard and the Switch Discovery Wizard
- Installing KeyView Pro 6.5 for web printing
- Configuring DNS Forwarding

Changing the Passwords

This section describes how to change the default passwords for the BBSM server. (See Table 2-1 for the default passwords.)

Table 2-1 Default Passwords

Account	User Name	Password
Administrators	Administrator	changeme
MSDE System Admin	sa	changeme2
BBSD Windows Client	bbsd-client	changeme2
BBSD MSDE Client	bbsd-client	changeme2

Resetting the Administrators Password

The Windows 2000 Administrator has full system permissions and rights, can alter any BBSM configuration setting, and has access to any option on the Dashboard. To keep your BBSM server secure, use the following procedure to change the default password “changeme” after you log on for the first time.

Note For customer-installed BBSM software, skip this procedure. The administrator password was created during installation.

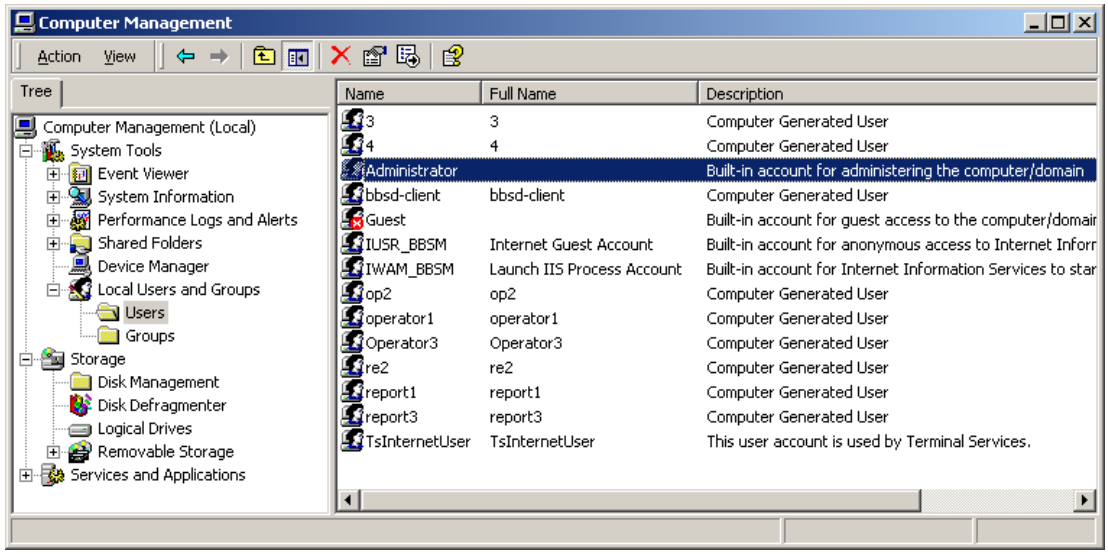
Step 1 Choose **Start > Programs > Administrative Tools > Computer Management**. (See Figure 2-4.)

Step 2 Double-click **Local Users and Groups**.

Step 3 Double-click **Users**.

Step 4 Right-click **Administrator**.

Figure 2-4 BBSM Computer Management Window



Step 5 Select **Set Password**.

Step 6 Enter the new administrator password. The screen will show only asterisks.

Step 7 Enter the new password again in the Confirm password entry field and click **OK**.

Step 8 When The password has been changed window appears, click **OK**.

Step 9 Close the Computer Management window.

Resetting the MDSE Passwords

To change the MSDE passwords, type this command line at the command prompt:

```
osql -E -Q "exec sp_password '<old_pwd>','<new_pwd>',<user>"
```

Caution The BBSD Windows client password *must* match the BBSD MSDE client password. Be sure you use the same password for both BBSD accounts.

Installing Service Packs or Patches

Before beginning the basic configuration of your BBSM server, be sure to determine if any service packs or patches need to be installed. We recommend that you install all available service packs and patches to maximize the functionality of your BBSM server. For instructions on performing these installations, see Chapter 5, “Installing Service Packs, Patches, and Upgrades (WEBpatch).”

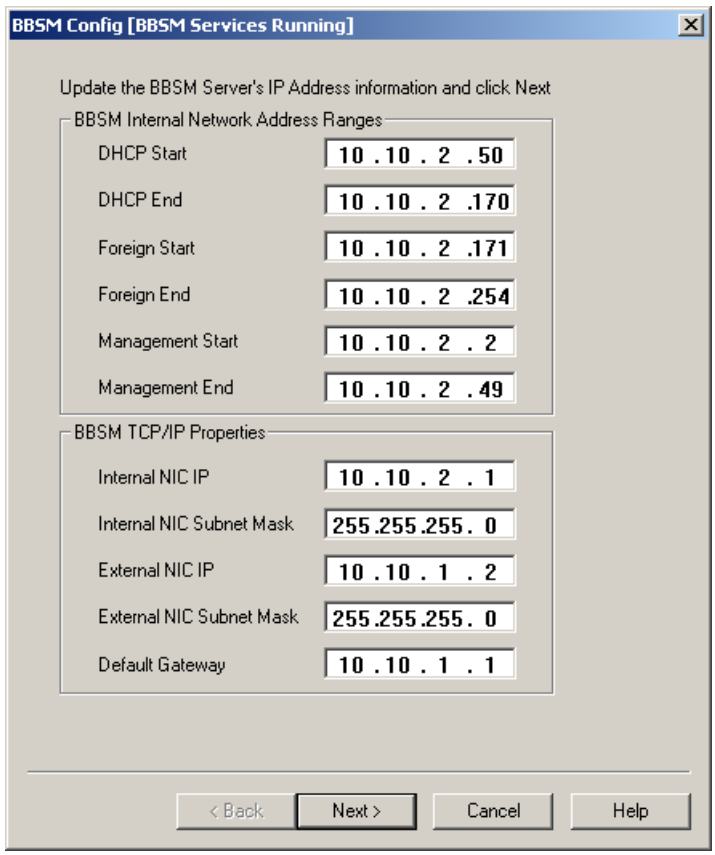
Running the Address Change Wizard

To ensure that BBSM functions properly, the correct TCP/IP settings must be in place. Because TCP/IP settings cannot be changed or updated from the BBSM web pages, use the Address Change Wizard to correct the IP addresses.

Caution If the TCP/IP properties are not correctly set, BBSM will not function properly. The external TCP/IP properties cannot be changed or updated in the Port IP Addresses web page.

Step 1 Choose **Start > BBSM Configuration Wizards > Address Change Wizard**. The BBSM Config window appears. (See Figure 2-5.)

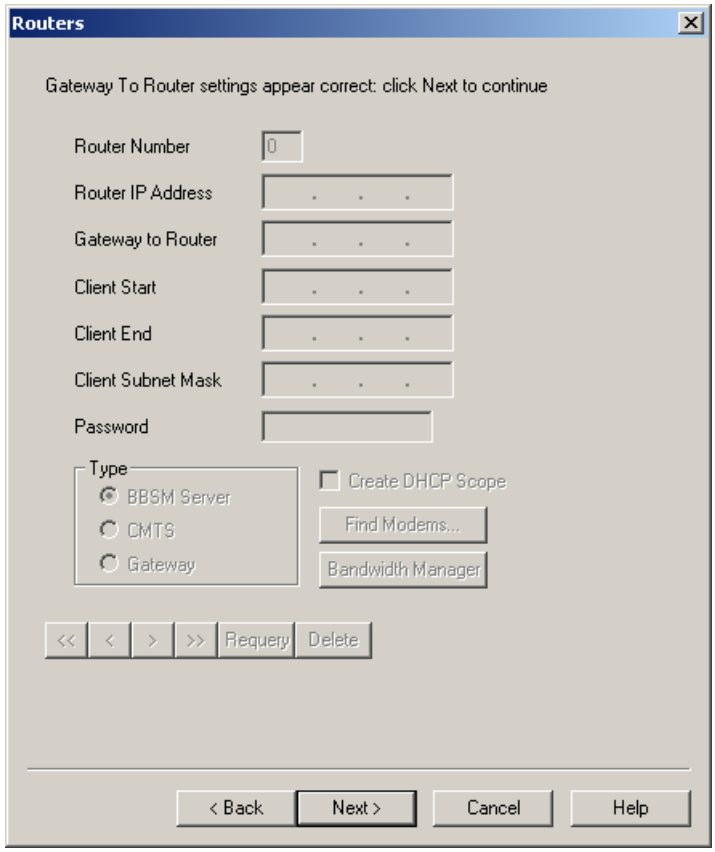
Figure 2-5 BBSM Config Window



Step 2 If the BBSM server's IP address information is incorrect, enter the correct information.

Step 3 Click **Next**. The Routers window appears. (See Figure 2-6.)

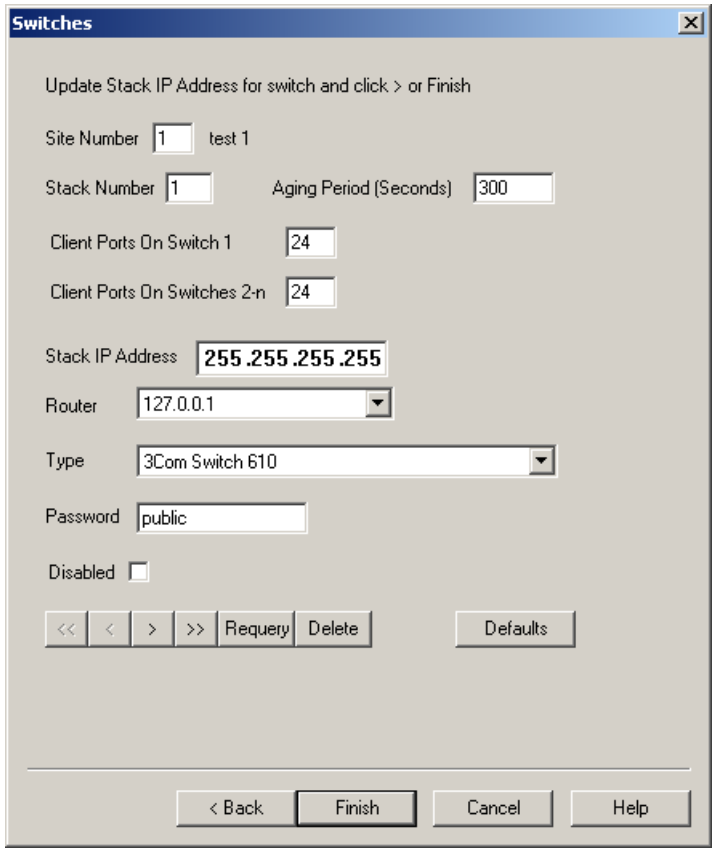
Figure 2-6 Routers Window



Step 4 If the **Gateway To Router** settings are incorrect, enter the correct settings.

Step 5 Click **Next**. The Switches window appears. (See Figure 2-7.)

Figure 2-7 Switches Window



Step 6 If the **Stack IP Address** is incorrect, enter the IP address. If necessary, click **Defaults** to access the default settings.

Step 7 Click **Finish**.

Note The server may prompt you to reboot after you click Finish. If it does, click the appropriate button to proceed. While the server is rebooting, you cannot access the BBSM server.

Running the Switch Discovery Wizard

Switch Discovery is a utility that locates switches connected to a bridged BBSM network, determines their type, and creates records for them in the BBSM database. This program only finds switches that are already connected to the network and have been properly configured with an IP address and the same SNMP read/write community string.

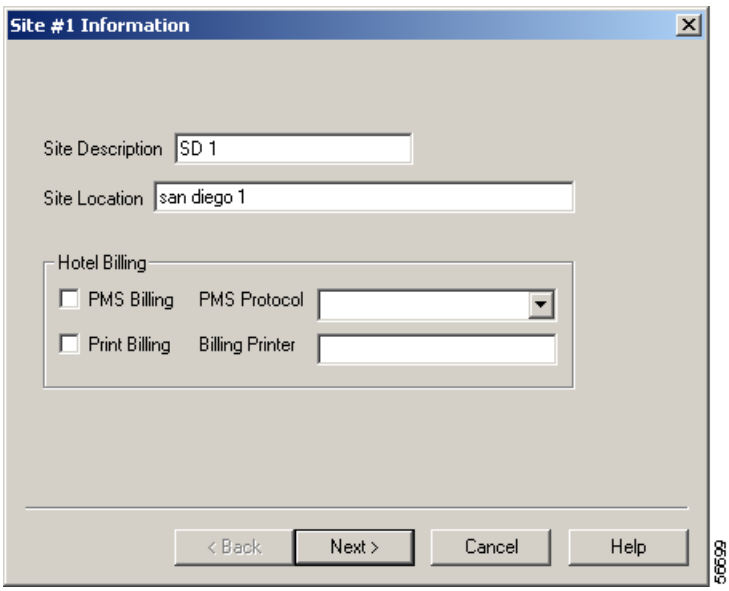
Caution Run the Switch Discovery Wizard only once at the beginning on an installation. Do not rerun it to find newly added switches, because running it again clears the existing data. Add any new switches manually and then remap the ports without clearing the existing port map.

Note Switch Discovery is designed for a single-site, bridged configuration of a BBSM server. The Switch Discovery Wizard does not work with routed or mixed networks.

Follow this procedure to run the Switch Discovery Wizard.

Step 1 Choose **Start > BBSM Configuration Wizards > Switch Discovery Wizard**. The Site Information dialog box appears. (See Figure 2-8.)

Figure 2-8 Site Information Dialog Box

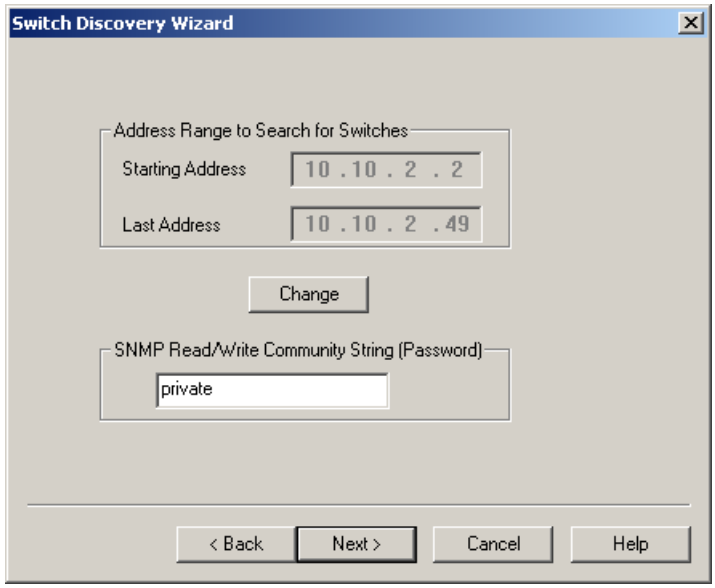


Step 2 Enter the site description and location.

Caution Do not check the PMS Billing check box. If you do, a charge of $9.95 will be applied to each room that is mapped.

Step 3 Click **Next**. The Switch Discovery Wizard dialog box appears. (See Figure 2-9.)

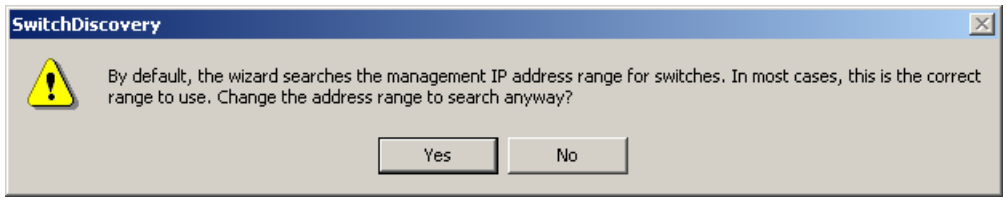
Figure 2-9 Switch Discovery Wizard Dialog Box



Step 4 In the SNMP Read/Write Community String (Password) field, verify that the password is the same as the one used for the switch hardware. The password must be the same for all the switches.

Step 5 Click **Change**. A confirmation dialog box appears. (See Figure 2-10.)

Figure 2-10 Change Address Range Confirmation Dialog Box



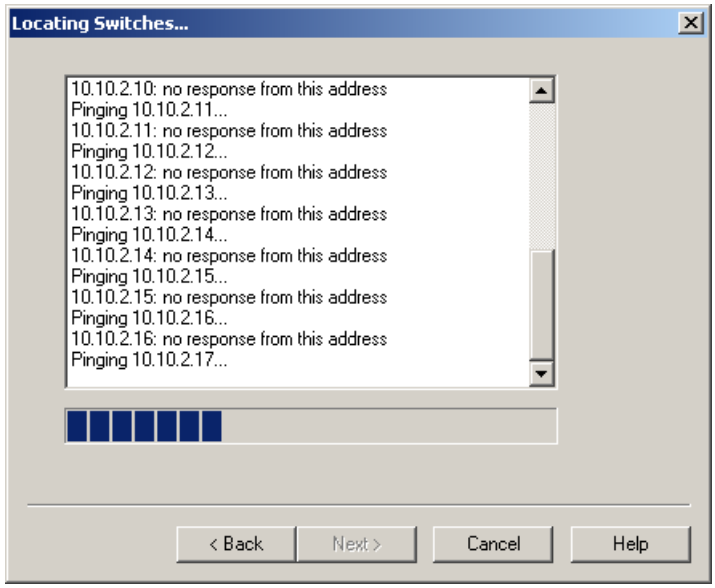
Step 6 Click **Yes** to clear the message.

Step 7 Enter the correct address range. To speed the discovery process, enter the address of the last switch in the Last Address field.

Step 8 Click **Next**. The Locating Switches dialog box appears. (See Figure 2-11.)

Note The Switch Discovery Wizard determines which ports are connected to uplink ports. This information is stored in the BBSM database.

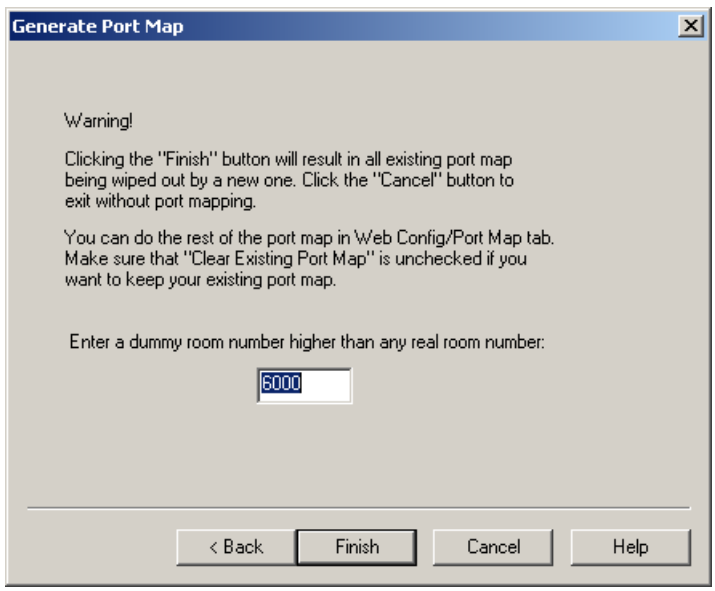
Figure 2-11 Locating Switches Dialog Box



Note If you are using switches that use the same identifier name for different models, a dialog box opens. Select the model that you are using and click **OK**.

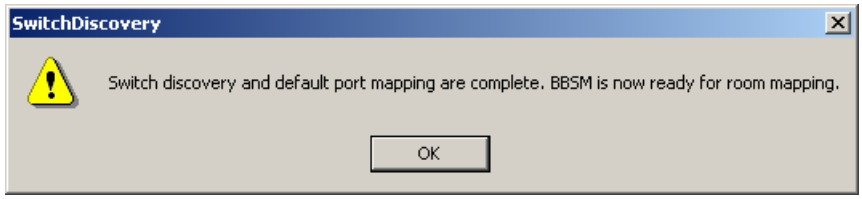
Step 9 After all the switches are located, the utility enables the Next button. Click **Next**. The Generate Port Map screen appears. (See Figure 2-12.)

Figure 2-12 Generate Port Map Dialog Box



Step 10 Accept the default dummy room number (or enter a different number, such as a number larger than the highest room number). Click **Finish**. A completion dialog box appears. (See Figure 2-13.)

Figure 2-13 Completion Dialog Box



Step 11 Click **OK**. Windows Notepad opens, displaying a log of Switch Discovery activities.

Step 12 After reviewing the log, close the window.

Installing KeyView Pro 6.5 for Web Printing

KeyView Pro 6.5 software must be purchased and installed to enable web printing on the BBSM server. The software is available separately from most software vendors. Follow these steps to install KeyView Pro.

Note If you are not planning on using the Web Printing feature of BBSM, you can skip this procedure.

Step 1 Insert the KeyView Pro Installation CD into the CD ROM drive. If Autostart does not launch the program, choose **Start > Run** to execute setup.exe.

Step 2 At the Install options window, click **Install KeyView Pro**.

Step 3 To bypass the Welcome screen, click **Next**.

Step 4 At the Software License Agreement window, read the license agreement and click **Yes** to accept and continue.

Step 5 At the Registration window, enter the KeyView Pro serial number, and click **Next**.

Note The serial number is on the stick-on labels which came with the KeyView software.

Step 6 At the Destination Path window, click **Next** to accept the default destination directory.

Step 7 From the Integration window, click **Next**.

Step 8 To ignore the Information message and continue the installation, click **OK**.

Step 9 Close the readme.txt file.

Step 10 Remove the KeyView Pro Installation CD from the CD-ROM drive.

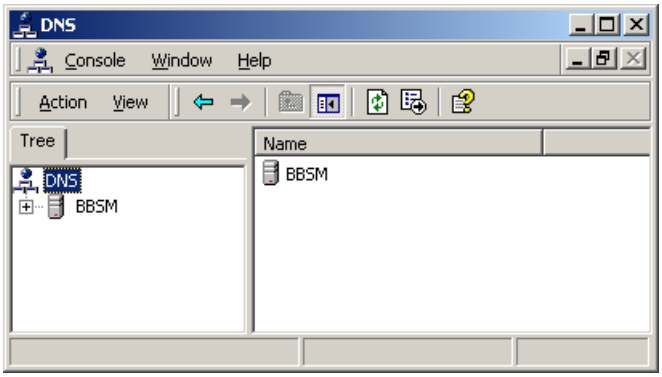
Configuring DNS Forwarding

The Domain Name System (DNS) forwarding feature allows you to relay DNS requests to a remote DNS server on another network. Follow these steps to configure DNS forwarding.

Note You must obtain the IP address for your DNS servers from your ISP before you can perform the following procedure.

Step 1 Choose **Start > Programs > Administrative Tools > DNS**.

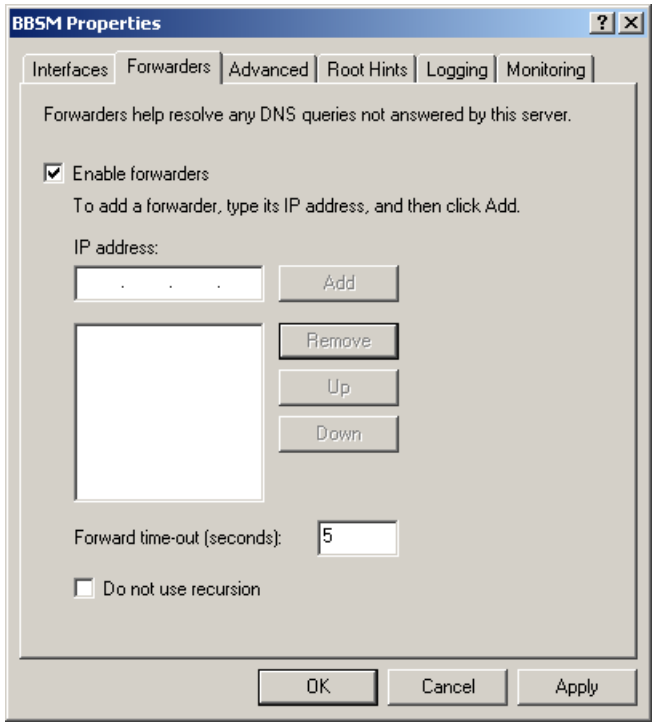
Figure 2-14 DNS Window



Step 2 In either pane, right-click your BBSM server name.

Step 3 Click **Properties**. The BBSM Properties window appears.

Figure 2-15 BBSM Server Properties



Step 4 Click the **Forwarders** tab.

Step 5 Check the **Enable forwarders** check box.

Step 6 In the IP address field, enter your Internet service provider's IP address in the IP address field, and click **Add**. Repeat this step for each DNS server IP address.

Step 7 Click **OK**.

Step 8 Close the DNS window.

Step 9 Restart your computer and log on as administrator with the proper password.

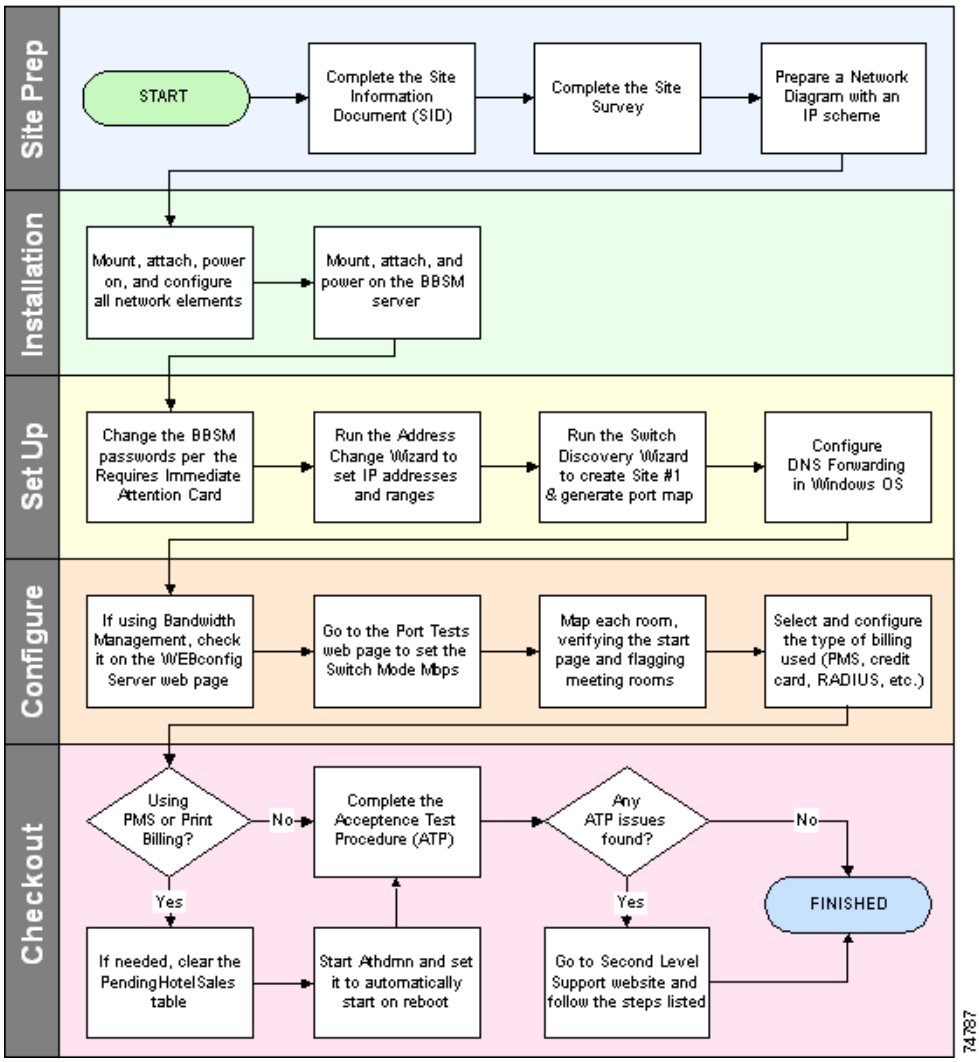
Basic BBSM Configuration (WEBconfig)

Cisco recommends that you install the basic elements and features of the BBSM system before configuring the advanced options. This chapter covers the basic steps to ensure a successful configuration.

Caution The configuration of your BBSM server is an intricate process that must be followed exactly to assure success. Before proceeding, be sure you have verified all the configuration considerations and completed all activities in Chapter 2, "Preconfiguration and Setup." Failure to do so could result in a loss of data and delays and will most likely result in your server not working properly.

The following flowchart gives a sample diagram of the basic steps needed to configure a BBSM server for use.

Figure 3-1 BBSM Software Configuration Flowchart



Planning Your BBSM Software Configuration

The following simplified outline shows the basic procedures for configuring your BBSM system. You perform these procedures in WEBconfig, which is accessed from the dashboard (called Dashboard) on your BBSM server. The specific WEBconfig web page where the changes are made is shown in parentheses at the end of the procedure.

Note For details on installing a customer-installed BBSM server or reinstalling the BBSM software, see the *Cisco Building Broadband Service Manager and Director Installation Guide*.

1. Establish the initial settings for Site 1.
   a. Enter the internal client IP addresses (BBSM Port IP Addresses).
   b. Enable Bandwidth Manager (BBSM Server).
   c. Configure the basic site information (BBSM Sites).
   d. If using a routed solution, enter the router information (BBSM Routers).
   e. Set up the switches for the site (BBSM Switches).
   f. If you have created a custom page set, input your page set name. (BBSM Page Sets). For additional information about modifying or creating custom page sets, refer to the *Cisco BBSM SDK Developer Guide*.
   g. Generate a port map (BBSM Port Map)
   h. Modify the port test settings (BBSM Port Tests).
   i. Configure any other items that apply to your configuration, such as the following:
      - Configuring a credit card server (BBSM Server).
      - Adding walled gardens (BBSM Walled Garden).
      - Configuring RADIUS servers (RADIUS)—WLAN only.
      - Configuring BBSM for port hopping (BBSM Port Map)—WLAN only.
   j. Map the rooms and test the ports.
2. Add and configure any additional sites.
   a. Establish the initial settings for the new site.
   b. Generate a port map for the new site (BBSM Port Map).
   c. Map the new site's rooms and test the ports.
3. Complete the BBSM configuration by addressing any special needs, such as the following:
   a. Configure a PMS connection for billing (BBSM Sites).
   b. If desired, enable local bill printing (BBSM Sites).
   c. Configure the call type (BBSM Call Types).
   d. Change the policies for special-use ports such as meeting rooms (BBSM Port Map).

Configuring the Initial Settings for Site 1

The first step in configuring a BBSM server is creating and setting up the primary site, called Site 1. You will use the WEBconfig interface to configure most of the settings.

Accessing the Dashboard and WEBconfig

The BBSM server is configured by using WEBconfig, which is located on the Dashboard. (The Dashboard can be accessed locally at the server or remotely.)

Note BBSM web pages are accessed on port 9488 instead of the default web server port 80. This port is accessed 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 internal BBSM network, you must activate a session to get access to these pages.

Accessing BBSM through Remote Access

This procedure describes how to access BBSM remotely. It can be run from the Internet or from inside the BBSM network.

Note If you are accessing WEBconfig from within the local subnet, you can use a private IP address. If you are accessing it remotely through the Internet, BBSM's external NIC must have a one-to-one NAT to publicly routable IP addresses.

Step 1 Open Internet Explorer. If necessary, activate a session.

Step 2 In the IE browser Address field, enter **http://<IP_address>:9488/www**, where IP_address is 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**.

Step 3 Enter the username and password. The Dashboard appears.

Step 4 Click **WEBconfig**. The WEBconfig screen appears, defaulted to the BBSM Port IP Addresses web page.

Accessing BBSM through Local Access

Use the following procedure for local access of the Dashboard from the BBSM console.

Step 1 On the desktop, double-click the **BBSM Dashboard** icon. The Dashboard appears. (You can also choose **Start > BBSM Dashboard** to access the dashboard.)

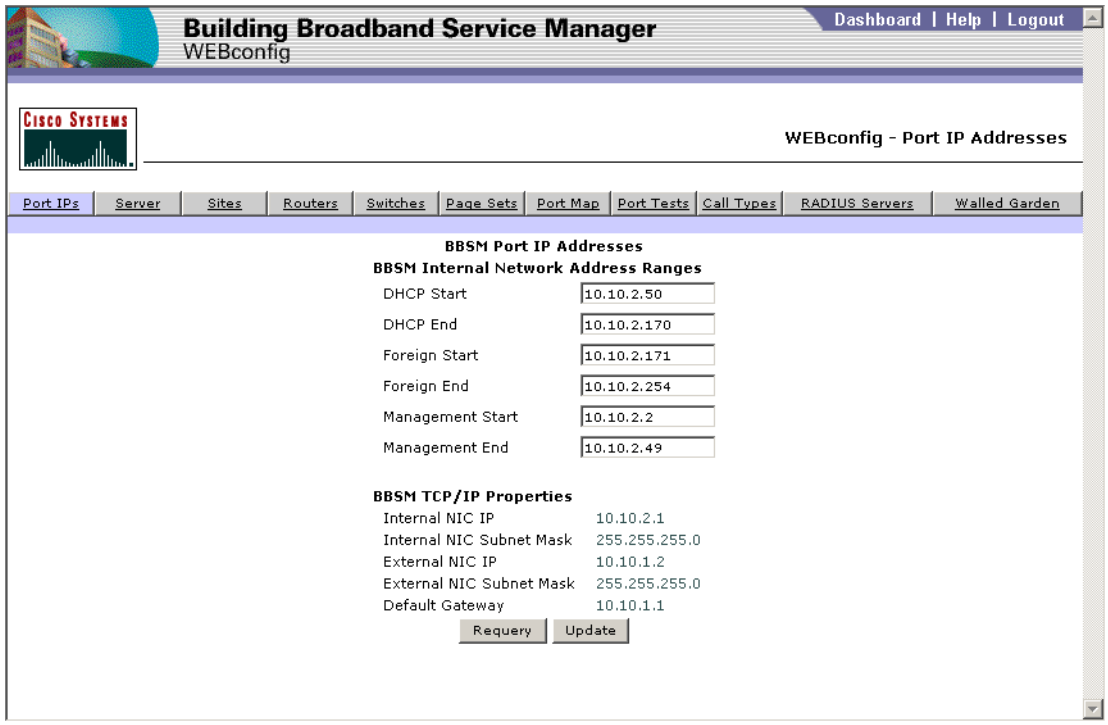
Step 2 Click **WEBconfig**. The WEBconfig screen appears, defaulted to the BBSM Port IP Addresses web page.

Entering Client IP Address Ranges

When you click WEBconfig on the Dashboard, the web page that appears is the BBSM Port IP Addresses web page. This is the starting point for configuring the BBSM server. (See Figure 3-2.) The BBSM Port IP Addresses web page can also be accessed by clicking the Port IPs button in WEBconfig. The IP addresses that BBSM accesses—end-user clients (DHCP and Foreign addresses) and network equipment (Management addresses)—are configured by using this web page.

Note For complete details and field descriptions, see Appendix B, "Using the BBSM Interfaces."

Figure 3-2 BBSM Port IP Addresses Web Page



Note The Port IP configuration is a server-wide configuration. Only one Port IP configuration exists for each BBSM server. The BBSM external TCP/IP Properties fields are read only and cannot be changed. If these fields are incorrect, see Running the Address Change Wizard, page 2-9 to change them.

Use the following procedure to configure the BBSM Port IP addresses.

Caution Note that the external TCP/IP properties cannot be changed or updated in the Port IP Addresses web page. If the TCP/IP properties are not correctly set, BBSM will not function properly.

Step 1 From the Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

Step 2 Enter the DHCP IP range, Foreign IP range, and Management IP range settings.

Step 3 Confirm that the BBSM TCP/IP Properties information is correct.

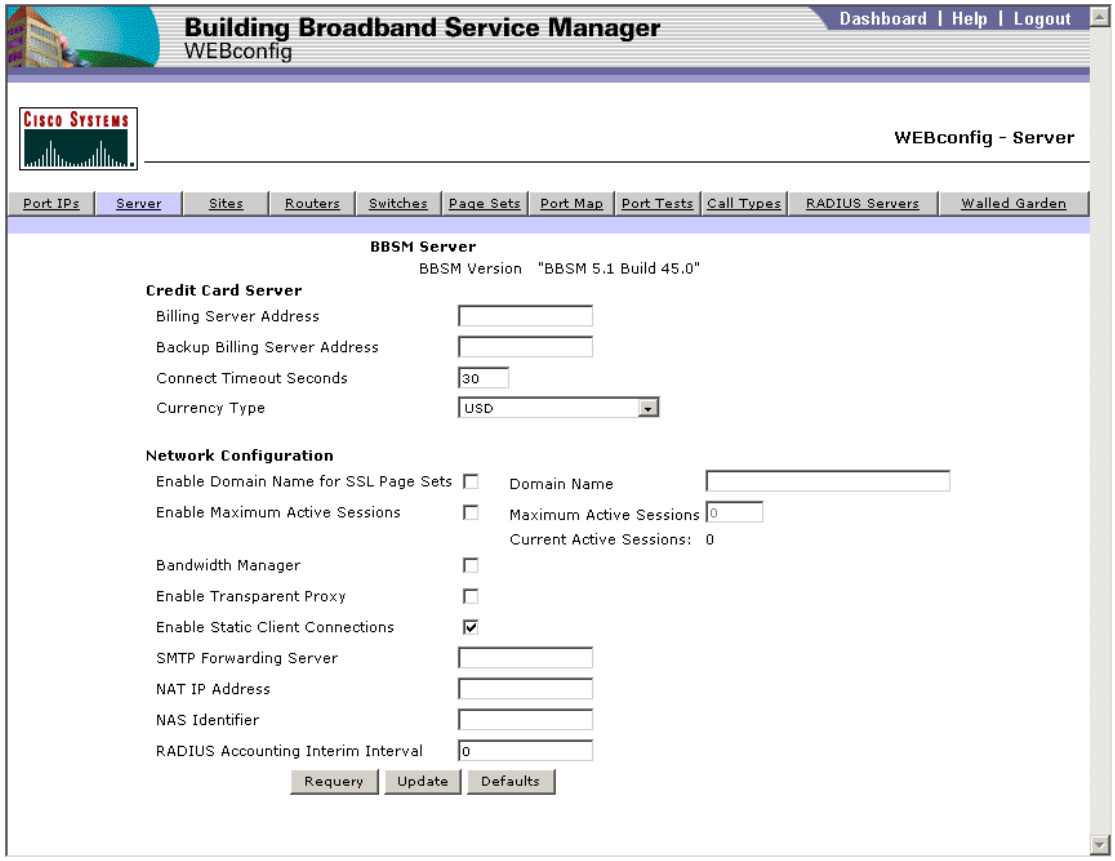
Step 4 Click **Update**.

Enabling the Bandwidth Manager

With BBSM, property managers and service providers can adjust policies to manage bandwidth on a per-port or per-site basis. To enable the bandwidth management by the BBSM server, you must enable the Bandwidth Manager feature. This option is located on the BBSM Server web page in WEBconfig. (See Figure 3-3.)

Note For complete details and field descriptions, see Appendix B, "Using the BBSM Interfaces."

Figure 3-3 BBSM Server Web Page



Use the following procedure to configure the BBSM Server web page.

Step 1 From the Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

Step 2 Click the **Server** button. The BBSM Server web page appears.

Step 3 Under Network Configuration, check the **Bandwidth Manager** check box.

Step 4 Change default settings or add data to complete all applicable fields.

Step 5 Click **Update**.

Configuring BBSM Sites

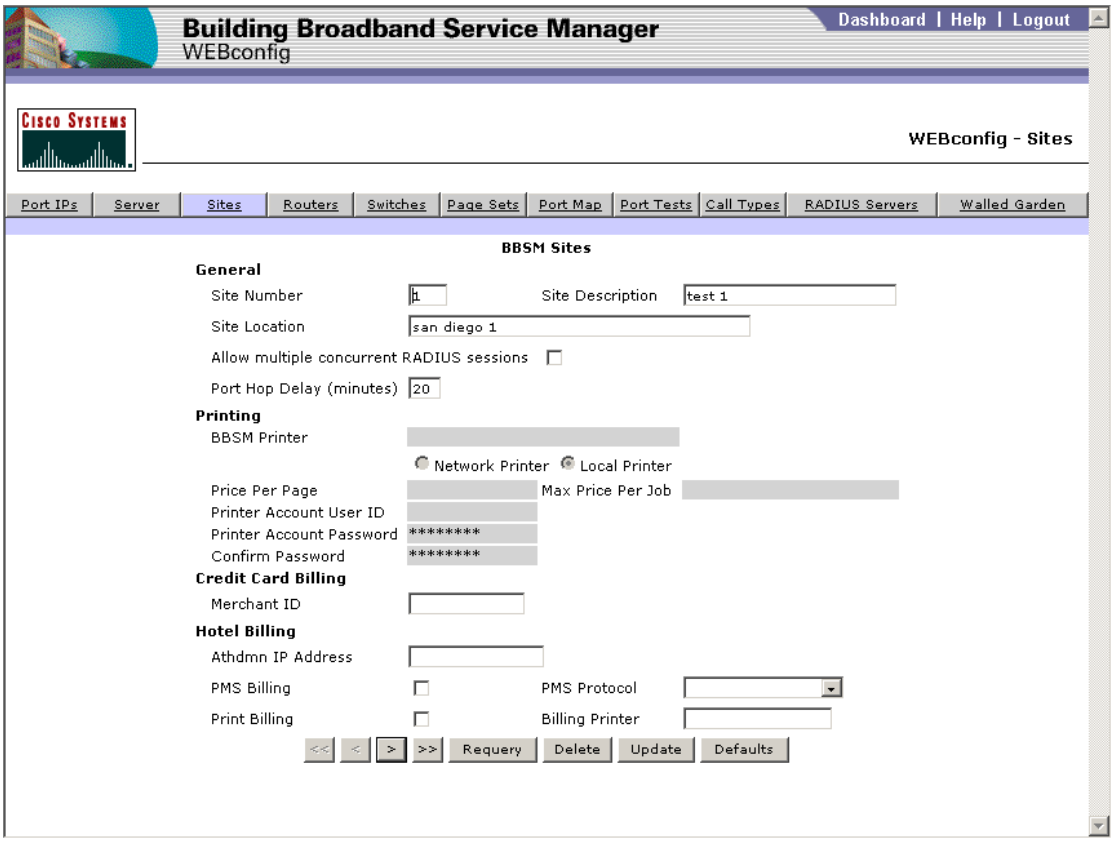
You configure one or more BBSM sites by using the BBSM Sites web page in WEBconfig. (See Figure 3-4.) You can also delete a site and its related stacks, port map, and call types by using this web page.

Caution Be careful when modifying data on the BBSM Sites page. If you are creating a new site, be sure to change the site number. Otherwise, data for Site 1 can inadvertently be changed when you attempt to create Site 2.

Deleting site records on the Sites web page also deletes the related stacks, port maps, and call types. Creating port map information is very time consuming, because rooms must be manually mapped again.

Note For complete details and field descriptions, see Appendix B, "Using the BBSM Interfaces."

Figure 3-4 BBSM Sites Web Page



Note If you need to edit the Operator Account or Report Account usernames or passwords, refer to your Windows documentation.

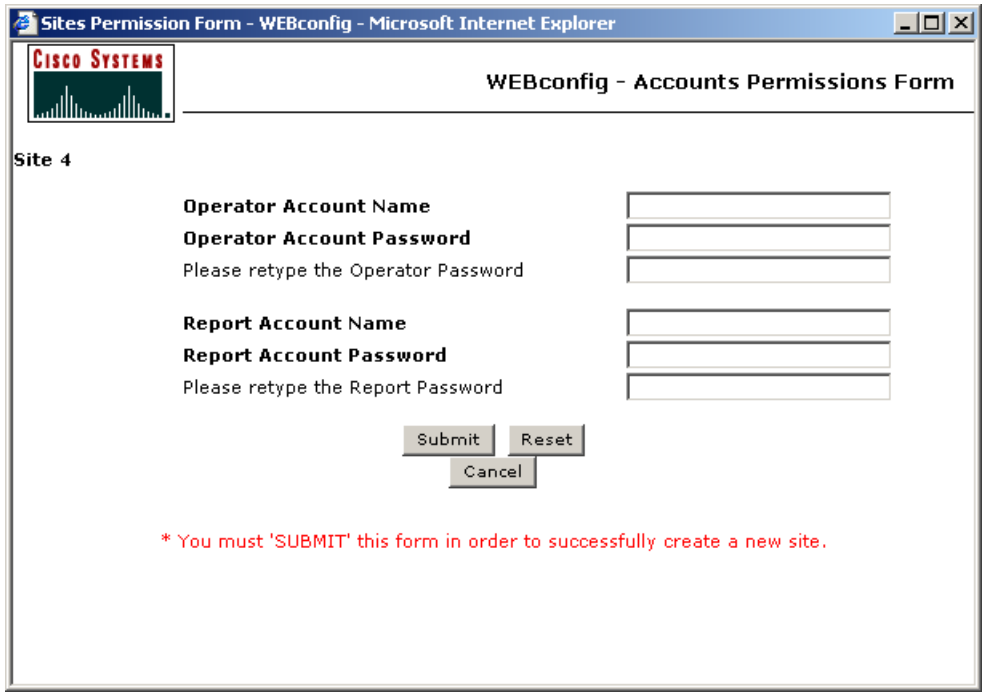
Be sure that the Athdmn service has been started if you are using a site controller to access PMS.

Use the following procedure to configure the BBSM Sites web page for the first site (Site 1).

Step 1 From the Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

Step 2 Click the **Sites** button. Enter the new site number, then click on another field (or click tab). The Accounts Permissions Form appears. (See Figure 3-5.)

Figure 3-5 Accounts Permission Form



Step 3 Create the site Operator and Reports user groups and add the group users. (For additional information about user privileges, see the "User Groups and Permissions" section on page 1-4.)

a. Enter the site's **Operator** Account group name and password. Retype the password.

b. Enter the site's **Report** Account group name and password. Retype the password.

c. Click **Submit**.

Step 4 Confirm that the Site Number is **1**.

Step 5 Enter the correct Site 1 information based on the network topology being used:

a. In the General section, enter the site identification information.

b. If you are using web printing, in the Printing section, enter the printer information for Site 1.

Note If the Printing fields are grayed out, KeyView Pro 6.5 has not been installed, and web printing will not work.

c. If you are using credit card billing, in the Credit Card section, type in the Merchant ID number.

d. In the Hotel Billing section, enter the appropriate hotel billing information.

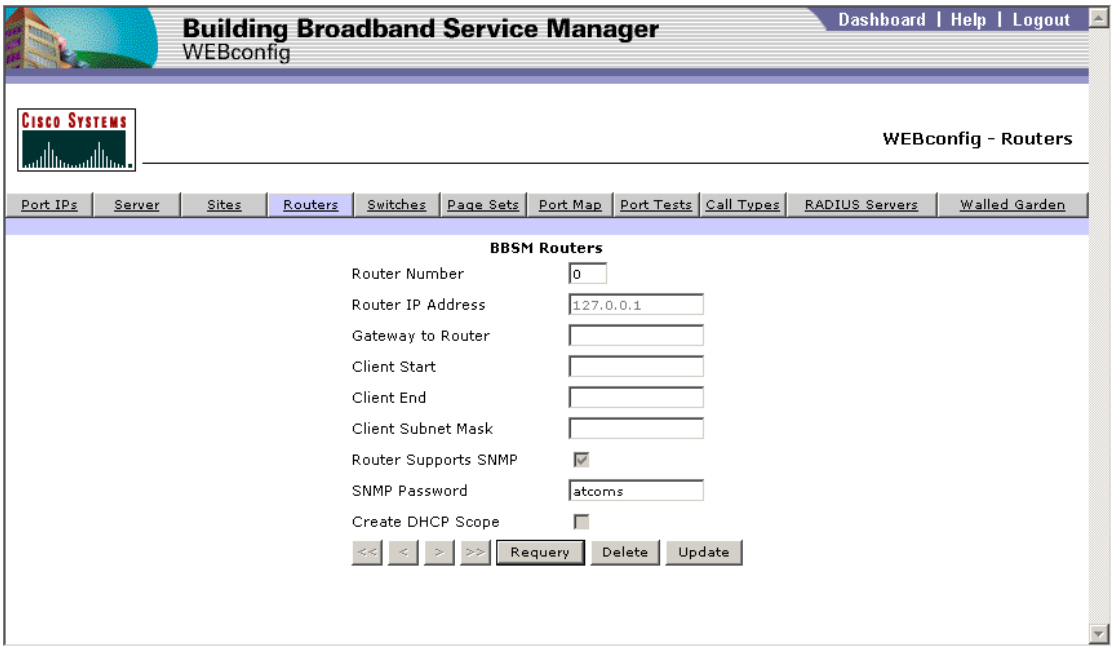
Step 6 Click **Update**.

Configuring Routers

BBSM servers that are attached to routed networks can be configured by using the BBSM Routers web page in WEBconfig. (See Figure 3-6.) Refer to your network configuration information for your particular network topology to complete the fields on this web page.

Note For additional information about routed networks, see the "Routed Network" section on page 1-3. For complete details and field descriptions, see Appendix B, "Using the BBSM Interfaces."

Figure 3-6 BBSM Routers Web Page



Use the following procedure to configure a BBSM router. To add additional routers to this site, make sure that they are physically installed before attempting to configure them.

Step 1 From the Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

Step 2 Click the **Routers** button. The BBSM Routers web page appears.

Step 3 In the BBSM Routers fields, enter the desired settings:

a. In the Router Number field, enter the router number. Note that the BBSM server is always number zero (0). For this reason, to add router numbers for additional routers and for the fields on this web page to be configurable, a router number other than zero must be entered in this field; that is, not a BBSM server.

a. Enter the IP addresses and the subnet mask.

b. If you are using a router that supports SNMP, check the Router Supports SNMP check box.

c. In the SNMP Password field, enter the password. Make sure the SNMP password matches the router SNMP community string. Note that certain restrictions apply when using Router Supports SNMP. See the "Restrictions When Using the Router Supports SNMP Feature" section on page B-9.

d. If BBSM is your DHCP server, check the Create DHCP Scope check box. If you are using another DHCP server or a router for DHCP, leave this check box unchecked.

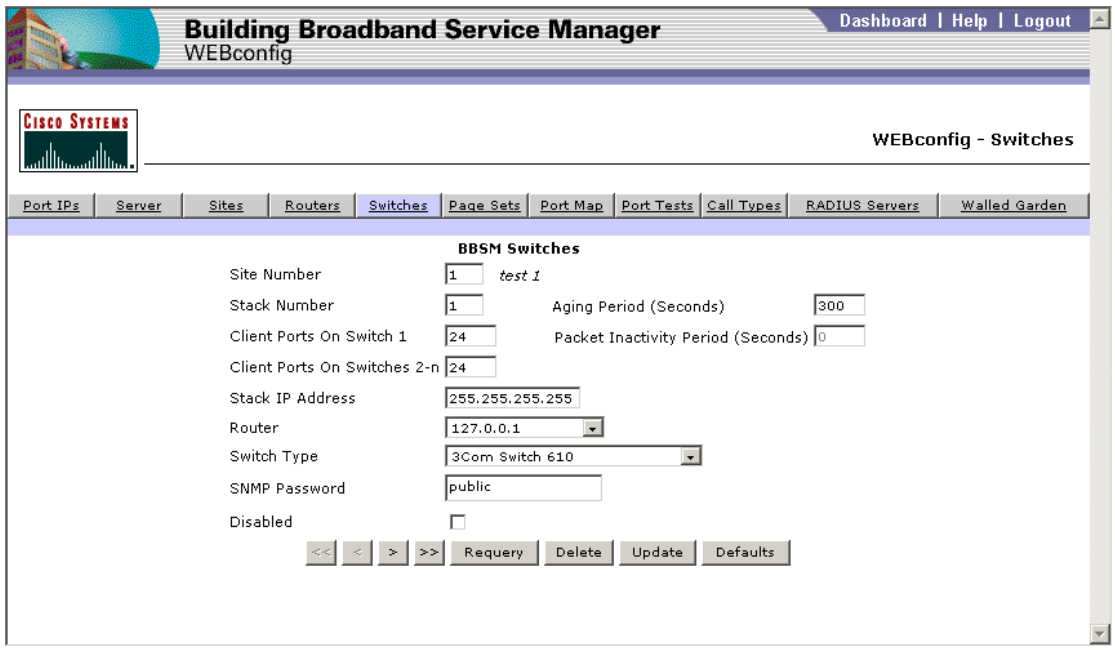
Step 4 Click **Update**.

Configuring BBSM Switches and Switch Stacks

Network elements and any switch stacks for each site are configured by using the BBSM Switches web page in WEBconfig. (See Figure 3-7.) Note that network elements can consist of hardware other than switches, because BBSM also supports wireless access points, DSL, and cable modems. (Note that a *switch stack* is a set of switches managed by the same IP address, and *stackable switches* are the switches that support the switch stack. Most switches are not stackable.)

Note For complete details and field descriptions, see Appendix B, "Using the BBSM Interfaces."

Figure 3-7 BBSM Switches Web Page



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.

Most installations have two types of switches: a base switch with client switches connected to it and client switches for connections to client computers. Unused ports on the base switch can be used as client ports if the base switch is added to the BBSM Switches web page and the number of clients on the switch equals the number of client ports.

Use the following procedure to configure the BBSM switches and switch stacks. (If you need to make substantial changes to your switch configuration, contact the Cisco TAC. See the "Obtaining Technical Assistance" section in the Preface to this user guide.)

Note For your future reference, we recommend that you print out all of the web page screens (if possible) or write down the information as you enter the network elements and/or switch stacks.

The procedure assumes that the switches are physically connected to the server and that the site number indicates the site number being configured.

Use the following procedure to configure each BBSM switch.

Step 1 From the Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

Step 2 Click the **Switches** button. The BBSM Switches web page appears.

Step 3 For each site, configure the switches and switch stacks.

Step 4 For each site, enter a unique stack number for each switch stack.

Step 5 In the SNMP Password field, note that SNMP community string (password) matches the SNMP Read/Write Community String password for the switch. All switches that share the same stack; that is, matrixed switches, must be installed with the same password.

Caution We strongly recommend that you change the default passwords for the switches and for the BBSM server immediately. The default SNMP Read/Write Community String password that is configured in the switch hardware is well known and could be used to compromise network security.

Step 6 For all other applicable fields, change the default settings or add data.

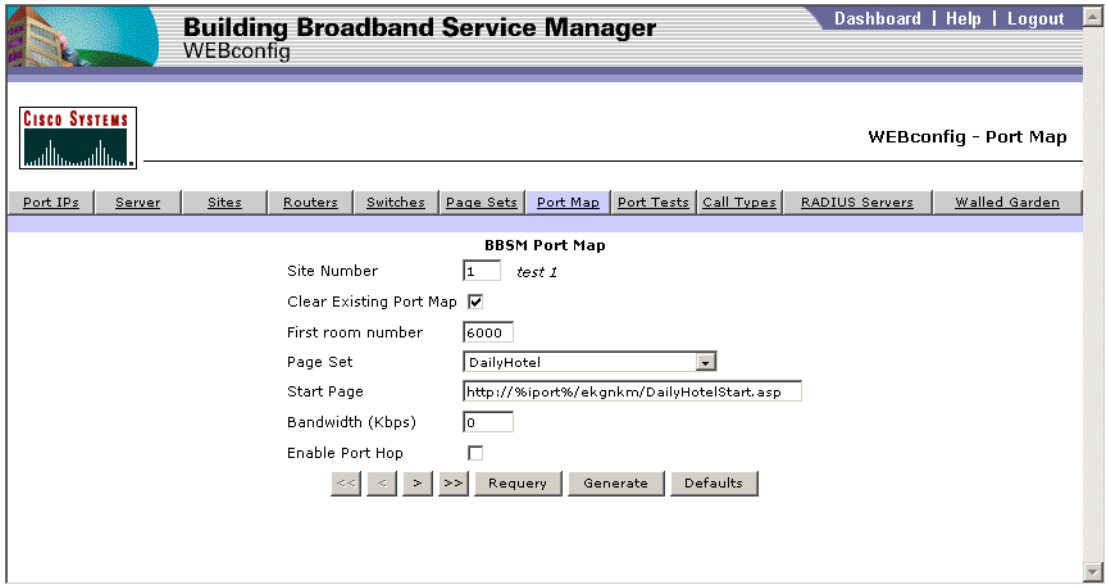
Step 7 Click **Update**.

Generating a Port Map

The page sets and bandwidths that you want to associate with each room number or location can be specified by using the BBSM Port Map web page in WEBconfig. (See Figure 3-8.) This data is used to populate the table that maps port IDs with the switch stacks and room numbers for a selected site.

Note For complete details and field descriptions, see Appendix B, “Using the BBSM Interfaces.”

Figure 3-8 BBSM Port Map Web Page



Use the following procedure to specify the desired page sets and bandwidths.

Step 1 From the Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

Step 2 Click the **Port Map** button. The BBSM Port Map web page appears.

Step 3 If this is the first site, in the Site Number field, verify that the site number is 1.

Caution Selecting the **Clear Existing Port Map** check box permanently removes all port data. Only select **Clear Existing Port Map** if you are creating a new site port map or completely replacing an existing one.

Step 4 If necessary, check the **Clear Existing Port Map** check box.

Step 5 In the First room number field, enter a placeholder room number.

Step 6 From the Page Set drop-down menu, select the desired page set. The initial BBSM page sets are provided as templates from which your web developer can create custom page sets. The default page set is DailyHotel.

Step 7 For wireless installations, check the **Enable Port Hop** check box.

Step 8 Click **Generate**. This generates a port map with port hopping enabled for all ports (in this case, the first site). (During the initial configuration, WEBconfig creates a port map with dummy room numbers to establish each port's initial settings.)

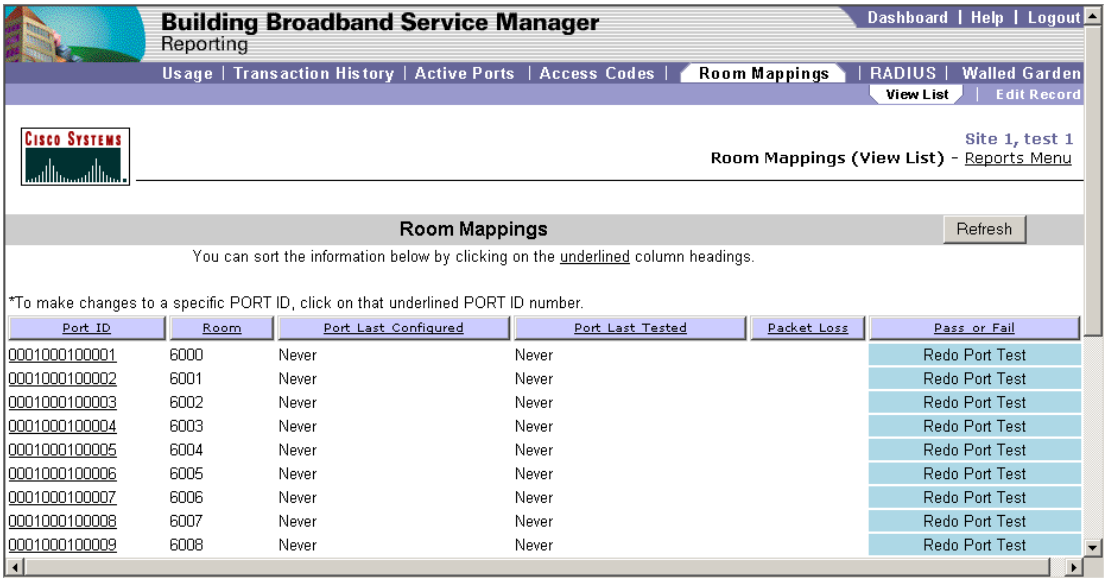
Step 9 To verify the port map entries, perform the following steps:

a. In the upper right-hand corner of the web page, click **Dashboard.**

b. Click **Reporting Pages**.

c. Click **Room Mappings**. The mapped ports with dummy room numbers appear. (See Figure 3-9.)

Figure 3-9 Room Mappings (View List)



Step 10 To return to the Dashboard and continue configuring your system, in the upper right-hand corner of the web page, click **Dashboard.** The Dashboard appears.

Configuring the Port Test Parameters

Caution Even if no changes are necessary, the WEBconfig Port Tests button *must* be clicked to populate the database and activate the port testing feature for room mapping.

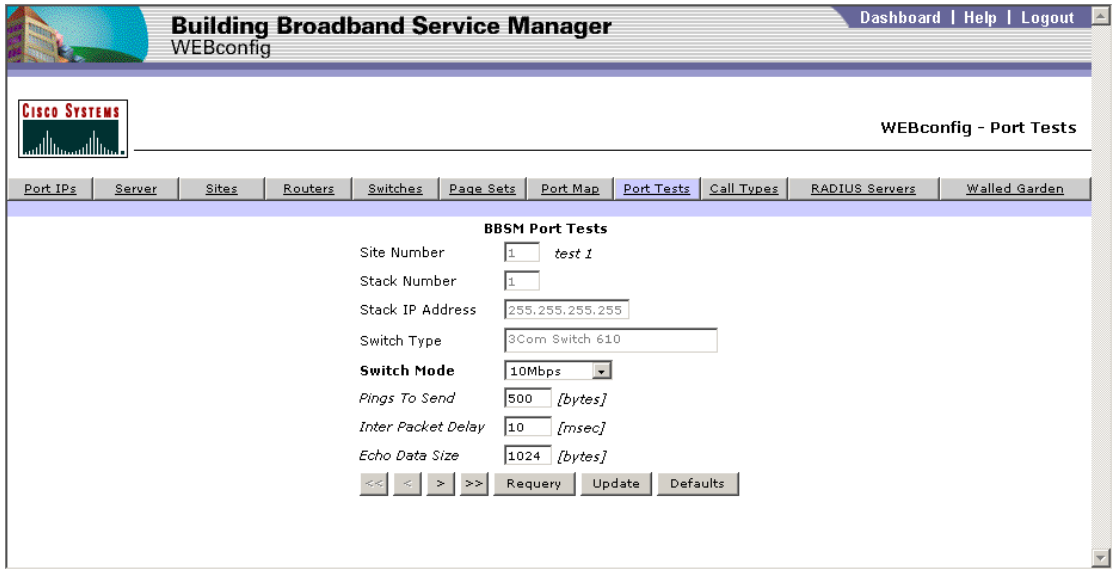
To perform accurate port testing, network elements require different test parameters like the number of pings to transmit, interpacket delay, and echo data size, depending on the device type. These parameters are configured by using the BBSM Port Tests web page in WEBconfig. (See Figure 3-10.) Because this test feature is hardware dependent, only the BBSM administrator has permission to perform these tests.

The test parameters can be configured per switch type in which all switch ports have the same test parameters.

Note For complete details and field descriptions, see Appendix B, "Using the BBSM Interfaces."

The first four items shown on the web page were derived from the information entered on the BBSM Switches web page. To change any of these items, see "Configuring BBSM Switches and Switch Stacks" section on page 3-11.

Figure 3-10 BBSM Port Tests Web Page



Use the following procedure to configure the port test parameters.

Step 1 From the Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

Step 2 Click the **Port Tests** button.

Step 3 Use the navigation buttons to locate the switch you want to change.

Step 4 From the **Switch Mode** drop-down menu, select **10Mbps** or higher.

Step 5 Click **Update**.

Configuring Optional System Settings

Depending on the type of deployment, certain other options and features might need configuring. Table 3-1 shows the optional features that can be configured.

Table 3-1 Optional Deployment Features

Deployment	Feature
Hospitality	Walled gardens
Wireless hot spots	RADIUS Credit card server

Configuring a Credit Card Server

When using credit card billing, a credit card authorization server must be selected and entered by using the BBSM Server web page in WEBconfig. (See Figure 3-3 on page 3-7.)

Note For complete details and field descriptions, see Appendix B, "Using the BBSM Interfaces."

Use the following procedure to configure credit card billing.

Step 1 From the Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

Step 2 Click the **Server** button. The BBSM Server web page appears.

Step 3 In the Billing Server Address field, enter the IP address for the credit card server.

Step 4 For the Backup Billing Server Address, leave this field blank, because this information is no longer needed in this release.

Step 5 In the Connect Timeout Seconds field, enter the desired number of seconds before the connection times out.

Step 6 From the Currency Type drop-down menu, select the local currency type. Note that the currency type that you select on the BBSM Server web page will be the designated currency type for the entire BBSM server.

Step 7 Click **Update**.

Step 8 Click the **Sites** button. The BBSM Sites web page appears.

Step 9 Under Credit Card Billing, in the Merchant ID field, enter the Merchant ID.

Step 10 Click **Update**.

Configuring Walled Gardens

The Walled Garden feature allows end users to view external websites before they agree to pay for the Internet service or before the system has authenticated them. The Walled Garden is essentially a "free zone" of Internet services that end users can always access. A network IP address and a network subnet mask define these Internet services in BBSM. The Walled Garden feature operates on a BBSM per-server basis.

A web page developer creates web pages with embedded links to free sites. These web pages represent the pages displayed to end users when the Walled Garden feature is in use before the end user clicks to be authorized for a pay service.

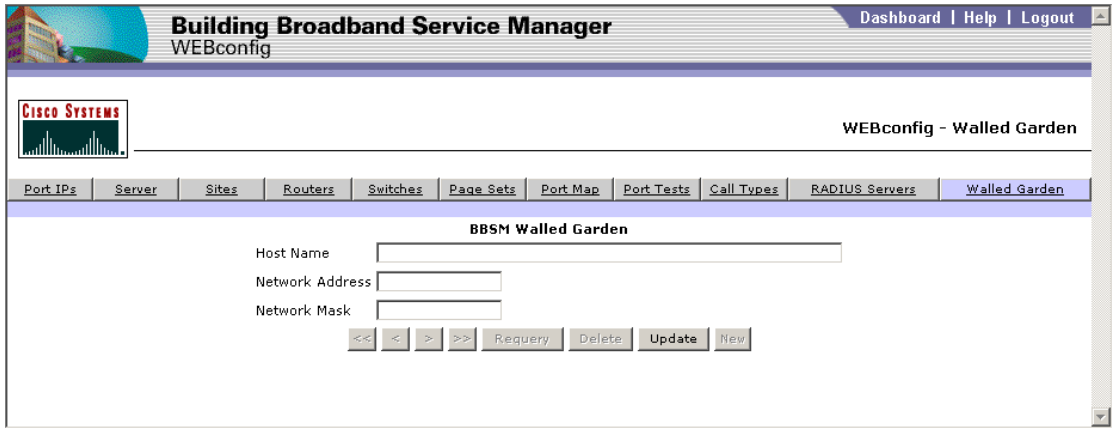
The pages can be grouped for all sites that BBSM services, or they can be designed to contain site-specific data. When the pages are site specific, you create a web page for each site where you have Walled Garden data.

Caution Configuring too many Walled Garden sites can impact performance.

Note For complete details and field descriptions, see Appendix B, "Using the BBSM Interfaces."

The path for each free site where walled garden pages are located and where end users are granted access is established by using BBSM Walled Garden web page in WEBconfig. (See Figure 3-11.)

Figure 3-11 BBSM Walled Garden Web Page



Use the following procedure to configure the walled gardens.

Step 1 From the Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

Step 2 Select the **Walled Gardens** button.

Step 3 In the Host Name field, enter the host name.

Step 4 In the Network Address field, enter the network address.

Step 5 In the Network Mask field, enter the network mask.

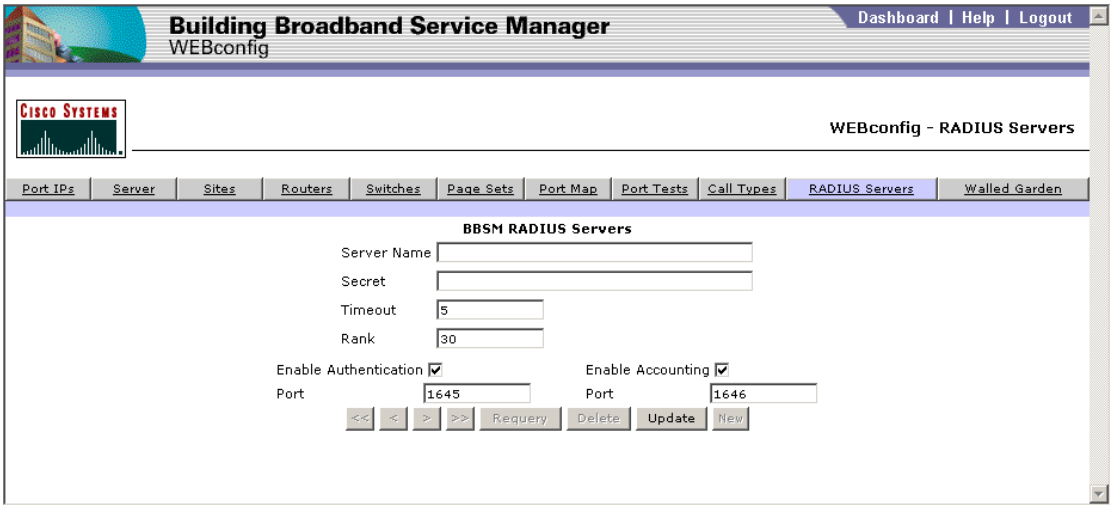
Step 6 Click **Update**.

Configuring RADIUS Servers

The BBSM server can operate as a RADIUS client, which allows BBSM clients and dial-up routers to be authenticated against a RADIUS server. RADIUS servers are often used to maintain username and password information for Internet service providers (ISPs). The RADIUS server options are configured by using the BBSM Servers web page in WEBconfig. (See Figure 3-12.)

Note For complete details and field descriptions, see Appendix B, "Using the BBSM Interfaces." For additional information using RADIUS, see Appendix D, "Using RADIUS Authentication, Authorization, and Accounting."

Figure 3-12 RADIUS Servers Web Page



Use the following procedure to configure RADIUS.

Step 1 From the Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

Step 2 Select the **RADIUS Servers** button.

Step 3 In the Server Name field, enter the RADIUS Server IP address or DNS name.

Step 4 In the Secret field, enter the password for the RADIUS server.

Step 5 In the Timeout field, enter the number of seconds that the BBSM server waits before attempting to access the RADIUS server a second or third time or before going to the next RADIUS server that is not responding. Note that BBSM will attempt to contact each RADIUS server three times before attempting to contact the next RADIUS server. The default for this setting is 5 seconds.

Caution The IIS default ASP Script timeout period is 90 seconds. This timeout period is the number of seconds that the browser will attempt to access the Internet before timing out. This time period is important to note, because if you increase the RADIUS Servers Timeout period (in Step 5 above) and more than one RADIUS server is unavailable, the total time period during which BBSM attempts to contact the RADIUS servers may be greater than the timeout period for the browser itself. Then the browser will time out.

For example, if the timeout period set in Step 5 is 20 seconds and two RADIUS servers are not responding, BBSM attempts to contact the first RADIUS server three times within 60 seconds. If BBSM cannot contact the first RADIUS server, it tries to contact the second server three times, again within 60 seconds. However, because the timeout period for IIS is 90 seconds, the browser will time out before BBSM finishes searching for the second RADIUS server.

Step 6 In the Rank field, enter the order in which the BBSM server attempts to contact RADIUS servers to authenticate a user. The BBSM server contacts servers in ascending order of rank. The default is 30.

Step 7 Verify the other items as appropriate for your network configuration.

Step 8 Click **Update**.

Configuring BBSM for Port Hopping

Port hopping is enabled, configured, and enabled/disabled on a port basis, by using the WEBconfig web pages.

Note For additional information about port hopping, see Appendix E, "Understanding Port Hopping."

If you are using BBSM page sets for the Subscription access service, enable or disable the Port Hop feature through the Subscription Port Control option on the Dashboard.

Use the following procedure to enable or disable port hopping for specific ports and configure the port hop delay.

Step 1 To enable or disable port hopping for specific ports, follow the steps below:

a. On the Dashboard, click **Port Control**. The Port Control List web page appears.

b. In the # column, click the desired port number. The Port Control Form web page appears.

c. In the Enable Port Hop field, click the True or False radio button, as desired:

- True: Enables port hopping for a specific port
- False: Disables port hopping for the specific port

d. Click **Update** to save the change.

Step 2 To configure the Port Hop Delay parameter, follow the steps below:

a. From the Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

b. Click the **Sites** button. The BBSM Sites button appears.

c. In the Port Hop Delay (minutes) field, enter the number of desired minutes between 1 and 60 that BBSM will search for the end user after the user (active session) has been disconnected from the original port. If the user is not found within this time frame, the BBSM session is terminated. Note that the port hopping feature must be enabled. The default number of minutes is 20.

d. Click **Update** to save the change.

Adding BBSM Sites

BBSM sites can be added by using the BBSM Sites web page in WEBconfig. After the site is created, the other WEBconfig web pages can be used to configure the site.

Note When adding new sites on the BBSM Sites web page, type the new information over the old text in the fields and click **Update**.

Use the following procedure to add a new BBSM site.

Step 1 From the Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

Step 2 Click the **Sites** button. The BBSM Sites web page appears.

Step 3 In the Site Number field, enter the new site number.

Step 4 Press **Tab**. The WEBconfig - Accounts Permissions Form appears. (See Figure 3-5 on page 3-9.)

Step 5 In the Operator Account Name field, enter the Operator account group name for this site.

Step 6 In the Operator Account Password field, enter the password for this site, then retype the password.

Step 7 In the Report Account Name field, enter the Report account group name for the site.

Step 8 In the Report Account Password field, enter the password for the site, then retype the password.

Step 9 Click **Submit**. The BBSM Sites web page reappears.

Step 10 Complete the appropriate data fields for the new site.

Step 11 Click **Update**.

Step 12 Using the appropriate WEBconfig web pages, configure the rest of the site parameters.

Mapping Rooms and Port Testing

During the initial configuration, WEBconfig creates a port map with dummy room numbers to establish initial settings for each port. Completing the procedures in this section allows you to replace the dummy room numbers in the port map with the actual room numbers and verify the connectivity to each room.

Verify that you have completed the following steps:

- Completed all BBSM server installation steps
- Installed all routers, RADIUS support, stacks, and switches
- Completed all BBSM wiring in the guest rooms
- Generated a port map for each site by using the BBSM Port Map web page of WEBconfig

Caution Before you can map the rooms, the switch mode must be set. See the "Configuring the Port Test Parameters" section on page 3-14.

Use the following procedure to map each room. Repeat the procedure until all of the ports have been mapped and tested.

Step 1 Connect a laptop to the in-room jack.

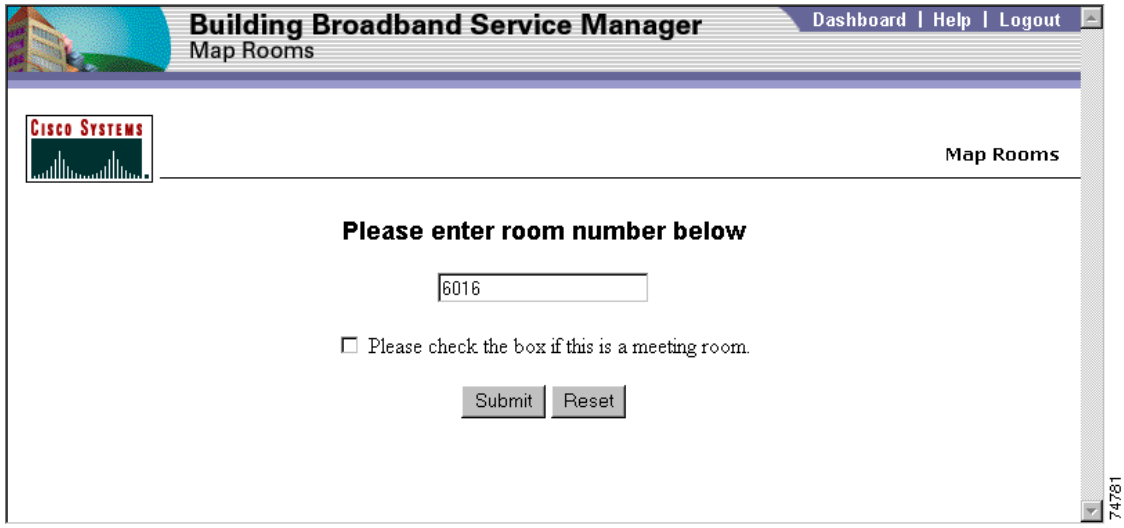
Step 2 Launch the web browser. You are redirected to the BBSM Connect page.

Step 3 Click **Connect** to be authenticated by the BBSM server.

Step 4 Access the Dashboard using the address **http://<serverIP>:9488/www** where <server IP> is the IP address of the BBSM server.

Step 5 Click **Map Rooms**. The Map Rooms web page appears. (See Figure 3-13.)

Figure 3-13 Map Rooms Web Page



Note The first time you perform the room mapping procedure (enterroom.asp) on an installer's laptop, BBSM automatically installs AtBroadcast.exe, which is used to run the port tests. Follow the wizard to complete the installation.

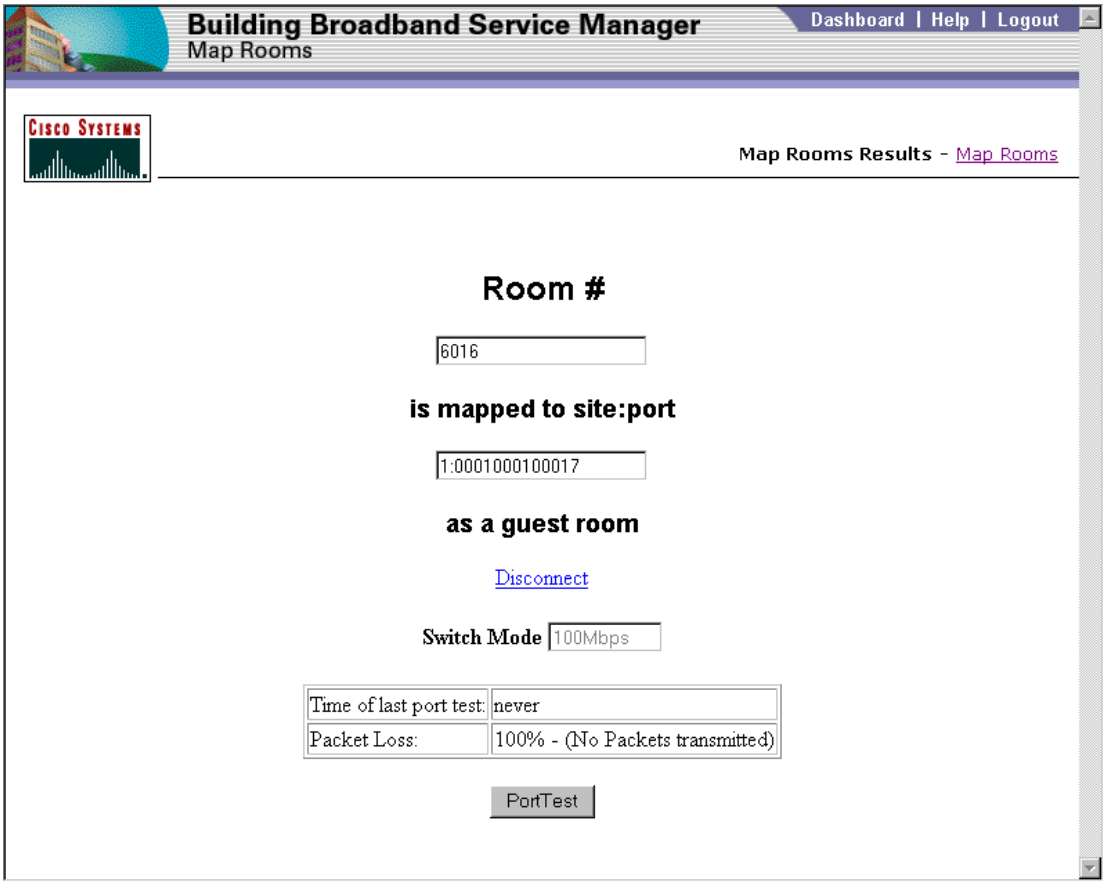
Step 6 Enter the room number of the room port that you are mapping. (If you need to correct the room number, click **Reset**.)

Step 7 If the room being mapped is a meeting room and not a guest room, check the **Is this a Meeting Room** check box.

Step 8 Click **Submit**. A confirmation web page appears, indicating that the port was mapped correctly. (See Figure 3-14).

Note If the room to port mapping failed, the port number will show ERROR rather than a valid port number. If this message appears, the current room-to-port mapping will not be changed.

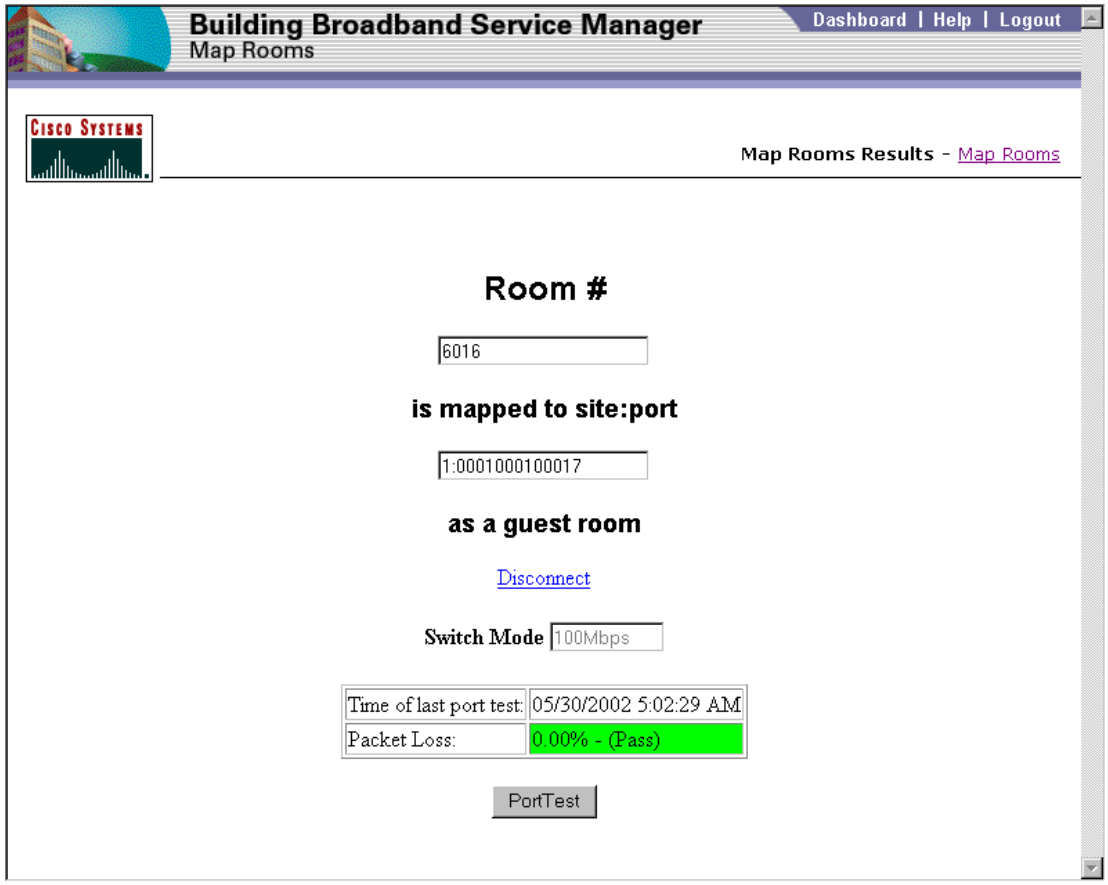
Figure 3-14 Correctly Mapped Room Confirmation Web Page



Step 9 Click **Port Test**. Wait several seconds for the test to complete. A test confirmation web page appears, indicating that the test was successful. (See Figure 3-15.)

Note Make sure the administrator has updated the Port Tests web page in WEBconfig. Otherwise, the test will fail.

Figure 3-15 Port Test Confirmation Web Page



Note If the port test fails, repeat this step. If repeated attempts to map the ports fail, contact the Cisco TAC. See the "Obtaining Technical Assistance" section in the Preface to this user guide.)

Step 10 When the port test is complete, click **Disconnect**.

Step 11 Close the browser.

Step 12 Disconnect from the in-room jack or BBSM connectivity device.

Completing the Configuration

After the rooms have been mapped, only the following procedures remain before the system is ready to use:

- Configuring BBSM for billing—either to the PMS or through direct billing
- If desired, customizing page sets by using the SDK software and documentation

Configuring BBSM for Hotel Billing

This section explains how to configure your BBSM server for hotel property PMS or local billing for single or multiple sites. It also describes how to configure the PMS call type codes.

Whether you are using single or multiple sites, BBSM supports two types of property billing:

- PMS Billing—When the hotel guest logs off a BBSM session, the billing record of the room charges is sent to a Property Management System (PMS) through a one-way serial connection, and the guest room is billed directly for the charges. As part of the billing record, a one-letter call type code is sent to the PMS to classify the service that was used, such as Internet access charges or web printing. Although the PMS integrator determines the actual call types, you can add, change, or delete the call types that are used by BBSM. The desired call type codes and their descriptions are configured in WEBconfig.

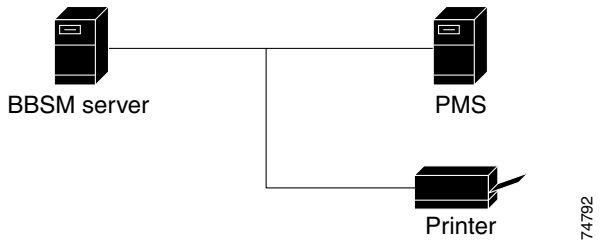
Note If your PMS protocol is not supported, you can create a custom PMS module by using the BBSM SDK. For a list of the PMS modules that BBSM supports, see Chapter 4, "Testing the PMS Interface (WEB PMS Test)." You can download the Cisco BBSM SDK software through Cisco.com. See the following URL:
http://www.cisco.com/warp/public/570/comlob/bbsm/bbsmdown.shtml

- Local bill printing—When the hotel guest logs off a BBSM session, the billing record of the room charges is sent to a local printer. The bill that is printed consists of the following information printed on a single line: date, time, room number, site number, port ID, and charge. Note that the format and content of the print report cannot be changed. (If you want to change the default to print the bill at the start of the session, refer to the DailyHotel page set documentation in the *Cisco BBSM SDK Developer Guide*.)

If you are using a multiple sites, the configuration is different from the configuration when using a single site:

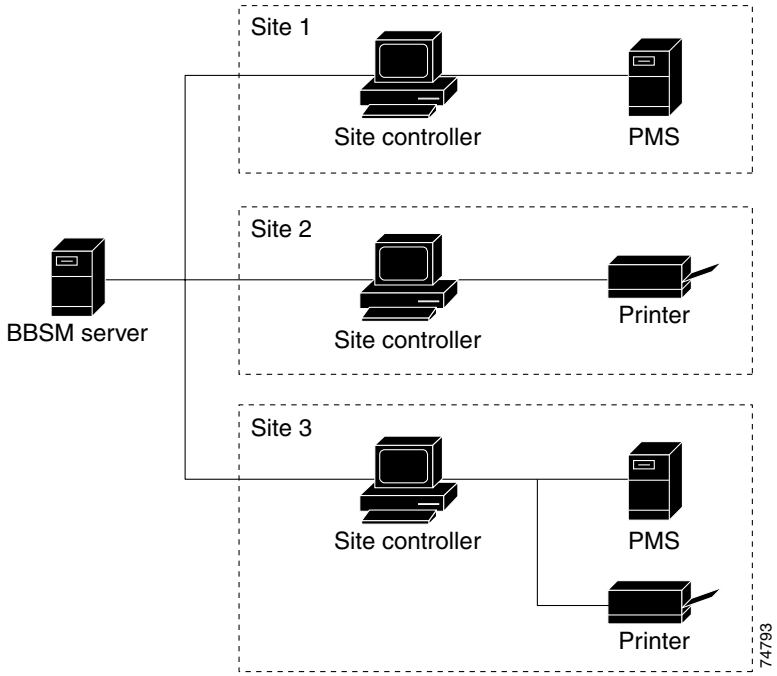
- If your BBSM server supports a single property site, the PMS system or your printer is connected directly to the server. (See Figure 3-16.)

Figure 3-16 BBSM Configuration for a Single Site



- If your BBSM server supports multiple property sites, a separate computer, called a *site controller* is used at each site, to support onsite printing and billing. (See Figure 3-17.)

Figure 3-17 BBSM Configuration for a Multiple Sites



Use the following procedure to configure the BBSM server for hotel billing.

Step 1 Open a DOS window to clear any pending charges that may have been generated during room mapping.

a. Type the following commands to display any pending hotel charges:

osql -E -d atdial (You will be at a 1> prompt.)
select * from pendinghotelsale
go

b. Type the following commands to clear these charges:

delete from pendinghotelsale
go

Figure 3-18 shows an example of pending hotel charges and the DOS commands that are used to delete them.

Figure 3-18 DOS Commands for Deleting Pending Charges

```
CMD - osql -E -d atdial
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator\desktop>osql -E -d atdial
1> select * from pendinghotelsale
2> go
 ID          Action          SiteNumber  PortID
 ----------- --------------- ----------- ------------------------------
           1 pms                       1 0001000100008
           2 pms                       1 0001000100004

(2 rows affected)

1> delete from pendinghotelsale
2> go
(2 rows affected)

1> select * from pendinghotelsale
2> go
 ID          Action          SiteNumber  PortID
 ----------- --------------- ----------- ------------------------------

(0 rows affected)

1> _
```

81010

Step 2 Start the Athdmn service. From the Windows task bar, choose **Start > Programs > Administrative Tools > Services > athdmn**. Click **Play** to start the service.

Note For hotel billing using either a PMS or a local printer, the Athdmn service must be started to post charges to the PMS or the local printer. By default, the service is set to manual and is not started. The reason is that if the Athdmn service were started automatically, charges would accumulate when rooms are being mapped. (Charges also accumulate when the PMS or printer is offline so that charges are not lost.)

Step 3 From the Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

Step 4 Click the **Sites** button. The BBSM Sites web page appears.

Step 5 In the Hotel Billing section, make the desired billing selections, as described in Table 3-2.

Table 3-2 BBSM Sites, Hotel Billing Options

Option	Description
Athdmn IP Address	Choose one of the following options: • If BBSM supports one site and the connection between BBSM and the PMS is a direct serial connection, leave this field blank. Athdmn is only used for remote connections through a site controller. • If BBSM supports multiple sites and the connection between BBSM is remote and uses site controllers, enter the IP address of the site controller where the hotel PMS interface software resides.
PMS Billing	If you are using PMS billing, check this check box.
PMS Protocol	If you are using PMS billing, selected the desired PMS protocol from the drop-down menu.
Print Billing	If you are using local billing (printing to a local printer), check this check box to print to a local printer. BBSM supports a serial, USB, or LAN connection.
Billing Printer	If you are using local billing, enter the printer name. Note that the printer name entered in this field must *exactly* match the default printer name as it is defined in the Printers folder for printing to work.

Step 6 Click **Update.**

Step 7 Click **Dashboard** in the upper right-hand corner. The Dashboard appears.

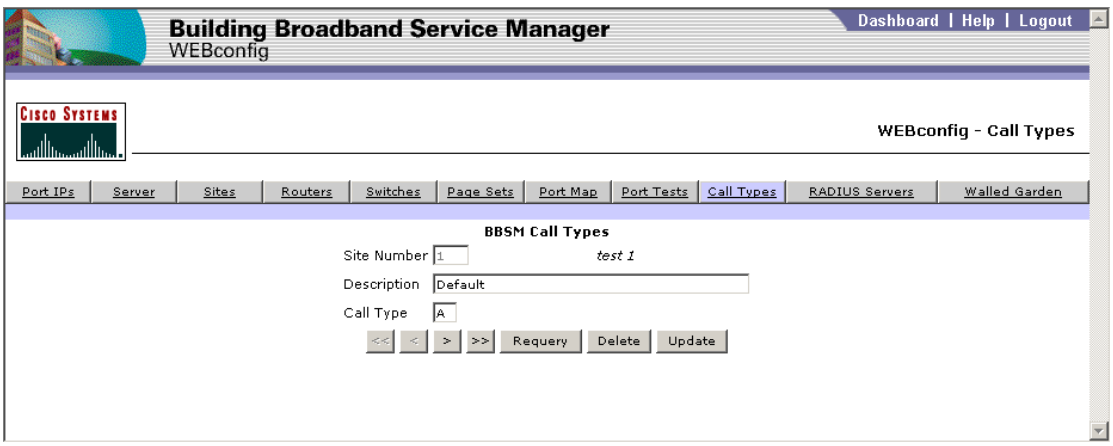
Step 8 If you are using PMS billing and you want to add, change, or delete PMS call types, follow the steps below. Note that you do not need to make any changes to the call types:

a. Contact the hotel or the PMS integrator to find out what call types are defined for the PMS.

a. On the BBSM server, from the Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

b. Click the **Call Types** button. The BBSM Call Types web page appears. (See Figure 3-19.)

Figure 3-19 Call Types Web Page



Step 9 Configure the call types, based on the information shown in Table 3-3. Note that multiple call types can exist for the same site number; for example, A for Internet charges and W for web printing.

Table 3-3 BBSM Call Type Options

Option	Description
Site Number	Enter the site number for the call type you want to add or change. The default site number is the "1."
Description	For the existing call type code, keep the default description, which is the word "Default." As mentioned above, a default call type record is automatically created when a site record is created on the BBSM Sites web page. You can create a new call type description with a new call type code (letter). However, to change the name of the existing call type description from the word Default, you must change the name in the page set.
Call Type	Specify the one-letter call type code: • If you are not given another specific value to use with your hotel PMS, enter the letter "A," which is the default call type code. For information on changing page sets, refer to the *Cisco BBSM SDK Developer Guide.* • If the hotel PMS uses other codes, enter the one-letter values for them.

Step 10 Click **Update**.

BBSM Page Sets

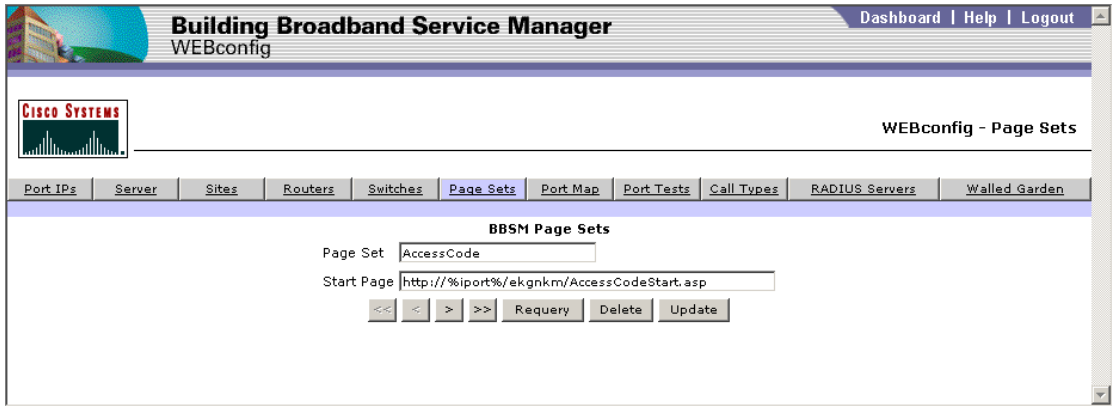
BBSM ships with default page sets. These default web pages can be used to represent the Internet service that you are offering, or your web developers can create customized page sets by modifying the BBSM default web pages or creating entirely new web pages. The BBSM Page Sets web page specifies the location of the customized page sets that your web developers designed. (See Figure 3-20.)

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

Note For complete details and field descriptions, see Appendix B, "Using the BBSM Interfaces."

Caution Before attempting to use a nonstandard (custom) page set, see the *Cisco BBSM SDK Developer Guide*. If needed, contact the Cisco TAC to be sure that your web page can be supported. See the "Obtaining Technical Assistance" section in the Preface to this user guide.)

Figure 3-20 BBSM Page Sets Web Page Main Component



Testing the PMS Interface (WEB PMS Test)

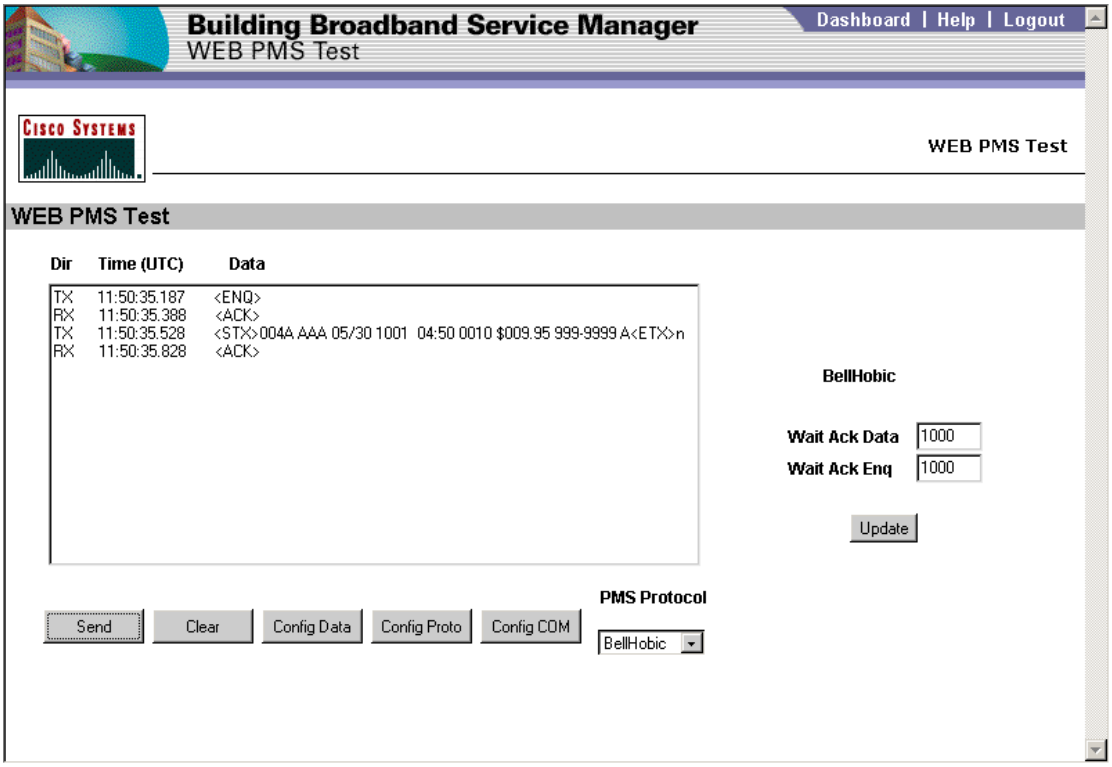
This chapter discusses how to test the serial connection and delivery of data from the BBSM server to the PMS by using the WEB PMS Test feature accessed under the Administration feature on the BBSM Dashboard. Table 4-1 describes the WEB PMS Test web page options. Figure 4-1 shows the WEB PMS Test web page with an example Bell Hobic protocol output.

Table 4-1 WEB PMS Test Options

Option	Description
Send	Sends a test charge posting to the PMS.
Clear	In the WEB PMS Test web page data area, clears the contents of the "Dir," "Time UTC," and "Data" columns.
Config Data	Enables the Hotel Data area of the web page to become visible, which enables you to specify the data for a charge posting that you want to send to the PMS.
Config Proto	*This feature is for internal use only.* For additional information, contact the Cisco TAC. See the "Obtaining Technical Assistance" section in the Preface to this user guide.
Config COM	Enables the COM Port Data of the web page to become visible, which enables you to specify the serial communication settings for the selected PMS protocol.
PMS Protocol	Selects the protocol used by your PMS. Possible drop-down menu selection values are BellHobic, Fidelio Serial, Hilton, and Xiox.
Update	Commits the changes made to Config Data, Config Proto, or Config COM.

Note For information on connecting BBSM to a PMS, see "Connecting to a PMS" section on page 2-6. For information on configuring the PMS connection, see "Configuring BBSM for Hotel Billing" section on page 3-24.

Figure 4-1 WEB PMS Test Web Page



The following PMS systems are currently supported:

- Protocol Technologies (Bell Hobic)
- MSI (Bell Hobic)
- Promus 21 (Bell Hobic)
- Encore (Bell Hobic)
- Logistics (Bell Hobic)
- XIOX
- Fidelio 6.0 and 7.0
- Hilton H1 and H2 (Hilton)

Note To create a new PMS module, you can download the Cisco BBSM SDK software through Cisco.com. See the following URL: http://www.cisco.com/warp/public/570/comlob/bbsm/bbsmdown.shtml

Verifying the BBSM-PMS Configuration

Check to make sure that all of the BBSM and PMS settings are correct.

Step 1 From the BBSM Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

Step 2 Click the **Sites** button.

Step 3 Verify that PMS Billing is checked.

Step 4 Click **Call Types.**

Step 5 Verify that the correct call type is entered for your vendor. (Note that the PMS vendor determines the call type settings.)

Testing the BBSM-to-PMS Interface

To ensure that your PMS is communicating clearly with the BBSM system, the interface between the BBSM server and the PMS interface must be tested before the system becomes operational.

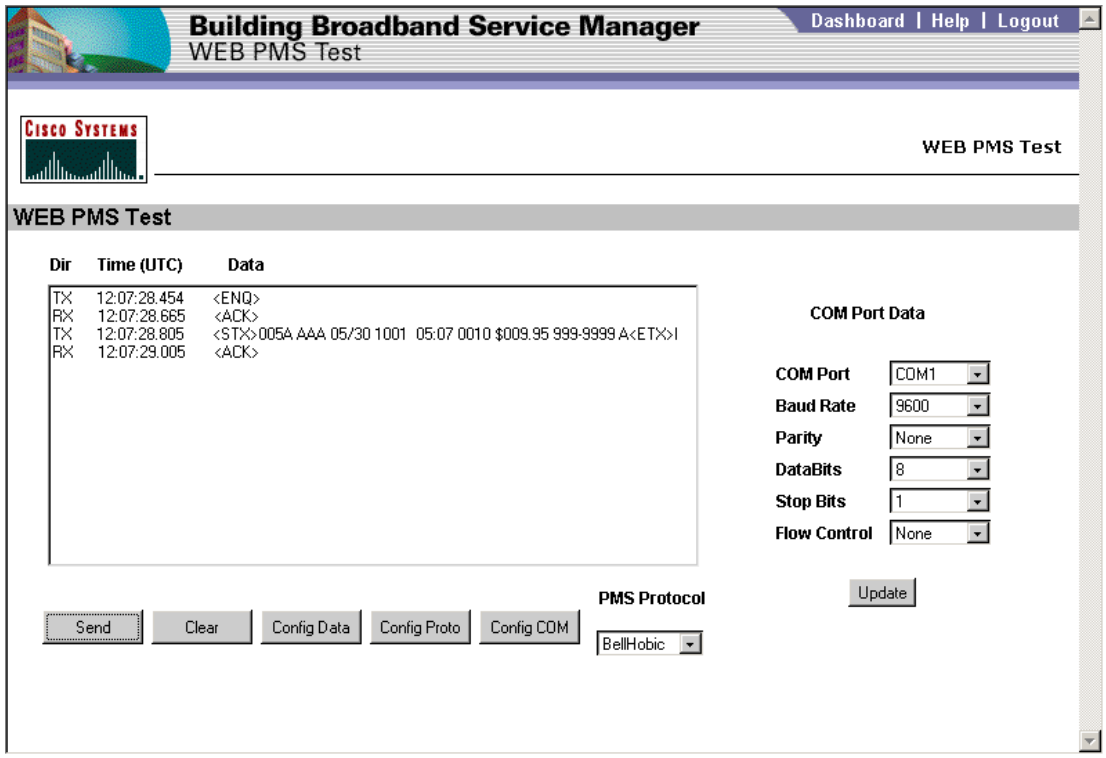
Use the following procedure to set up the test parameters and send a simulated charge posting from BBSM to the PMS interface.

Step 1 From the BBSM Dashboard, click **WEB PMS Test**. The WEB PMS Test web page appears.

Step 2 From the PMS Protocol drop-down menu, select the desired PMS protocol.

Step 3 Click **Config COM**. The COM Port Data area of the web page appears. (See Figure 4-2.)

Figure 4-2 COM Port Data Area of WEB PMS Test Web Page

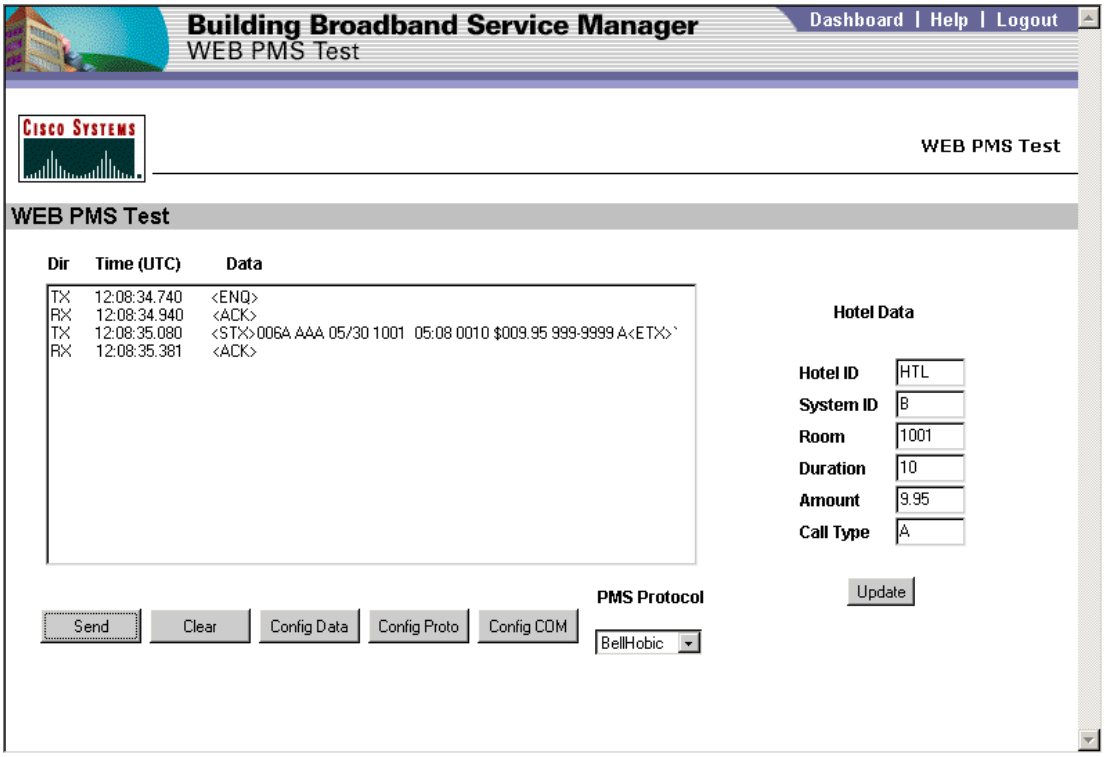


Step 4 Configure the serial communication parameters according to the PMS vendor's hotel specifications.

Step 5 Click **Update** to view the changes.

Step 6 Click **Config Data.** The Hotel Data area of the web page appears. (See Figure 4-3.)

Figure 4-3 Updated Hotel PMS Data



Step 7 Configure the test charge posting data to be sent to the PMS.

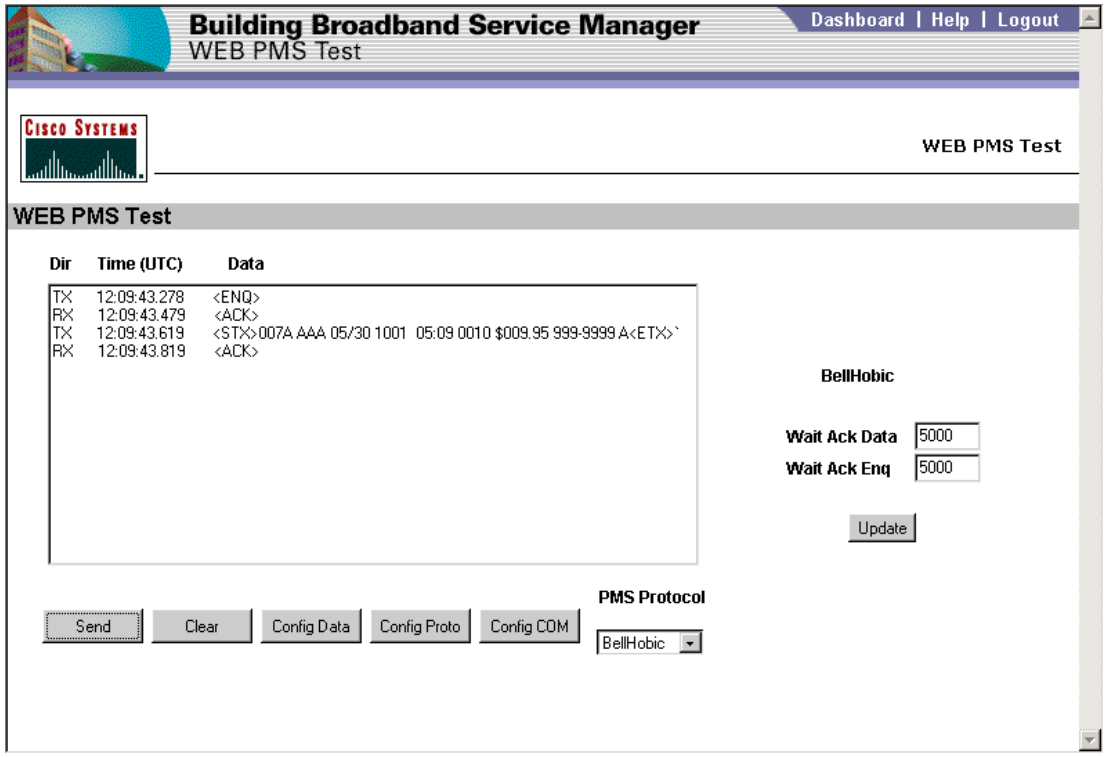
Step 8 Click **Update** to view the changes.

Step 9 To test the BBSM to PMS interface, send a simulate posting a charge to PMS:

a. Confirm that the selected PMS protocol is correct.

b. To send a charge posting to the PMS, click **Send**. If the charge posts successfully, PMS protocol data specific to each kind of protocol appears in the data area of the web page. (See Figure 4-4.)

Figure 4-4 PMS Protocol Data Displayed



c. To erase the contents of the Dir, Time (UTC), and Data columns, click **Clear**.

d. Close the browser to exit the program.

Testing the PMS Charge Posting

To test the PMS configuration, two engineers need to work together to post a charge through the Internet from BBSM to the PMS. One engineer, the installation engineer, is located in a room on the property. The other engineer is located at the BBSM server to post an charge through the Internet from BBSM to the PMS.

Use the following procedure to run the test:

Step 1 In the room, the installation engineer performs the following steps:

a. Connect a laptop with an Ethernet cable to the BBSM wall jack or Ethernet connection device in the room.

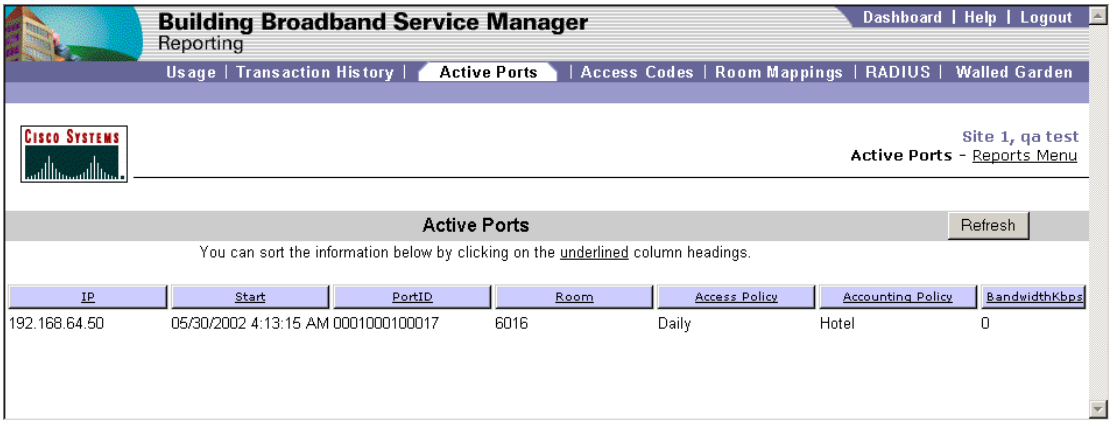
b. Open Internet Explorer and connect to the Internet through the Connect screen.

Step 2 At the BBSM server, the BBSM engineer then performs the following steps:

a. On the BBSM Dashboard, click **Reporting Pages**. A splash screen appears, followed by the BBSM Reporting web page.

b. On the navigation bar, click **Active Ports**. The Active Ports web page appears. (See Figure 4-5.)

Figure 4-5 Active Ports Report



c. Verify that the active port matches the room where the installation engineer is connected.

Step 3 In the room, the installation engineer performs the following steps:

a. Disconnect from the Internet.

b. If the “Thank You, You are disconnected” web page appears, but the port is still active, clear all the cached pages on the laptop and retry the disconnect.

Step 4 At the BBSM server, the BBSM engineer clicks **Refresh** and verifies the disconnection. The hotel charges should now post to the Hotel PMS.

Step 5 Ask the hotel staff to print out a copy of the PMS charge to the room. Then ask the hotel staff to delete the fake room charge.

Installing Service Packs, Patches, and Upgrades (WEBpatch)

This chapter describes how to install, transfer, and remove service packs, patches, and upgrades for the BBSM software by using the WEBpatch feature accessed under the Administration section on the BBSM Dashboard. The feature also allows the user to view any current or previous installation log entries.

Note that only administrators can install BBSM service packs.

Caution Make sure that the proper file is selected when transferring, installing, or removing a service pack. Selecting an incorrect file can corrupt the database or prevent BBSM from operating correctly. Install service packs during low-use time periods to minimize service interruptions and ensure proper functionality.

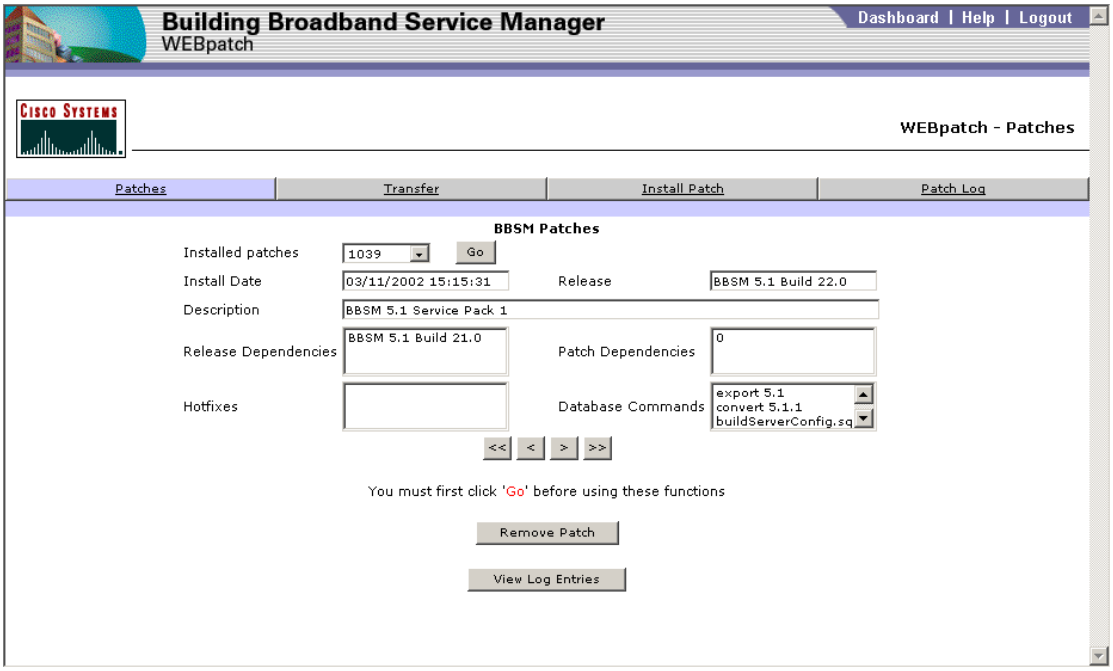
Accessing WEBpatch

WEBpatch is accessed on the Dashboard of your BBSM server or directly through a web-based GUI. After clicking WEBpatch on the Dashboard, the WEBpatch splash screen appears, followed by the WEBpatch Patches web page. Note that you can click the splash screen to skip it. (See Figure 5-1.)

Step 6 Note that you can access WEBpatch from a remote location or locally. In the IE browser Address field, enter **http://<IP_address>:9488/www**, where IP_address is 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**.

Figure 5-1 Patches Web Page



Using the WEBpatch Web Pages

Four WEBpatch web pages can be accessed through WEBpatch. These are accessed by clicking the navigation bar at the top of any of the WEBpatch web pages.

Table 5-1 WEBpatch Web Page Buttons

Web Page	Description
Patches	Shows the specifics of previously installed service packs and allows for the removal of selected service packs. This is the initial page shown when WEBpatch is launched.
Transfer	Moves a service pack onto the server and prepares it for installation.
Install Patch	Installs a selected service pack.
Patch Log	Displays message log information that can be sorted.

Viewing Installed Service Packs

Installed service packs can be viewed by selecting the Patches button. When you select a service pack and click the Go button, the remaining fields are populated with the service pack specifics.

Table 5-2 WEBpatch Patches Web Page Fields

Field	Description
Installed patches	Used to select an installed service pack.
Install Date	Shows the date that the service pack was originally installed.
Release	Lists the BBSM release for which the service pack is intended.
Description	Displays a brief description of the service pack.
Release Dependencies	Indicates the release or range of releases for BBSM that must be installed on the target server before installing the service pack.
Patch Dependencies	Lists the previous service packs that must be installed before the current service pack can be implemented.
Hotfixes	Shows the Microsoft *hotfixes* that are installed with the service pack.
Database Commands	Displays the commands performed to modify or update the BBSM database during the service pack installation.

Step 1 From the BBSM Dashboard, click **WEBpatch**. The WEBpatch splash screen appears, followed by the Patches web page appears.

Step 2 From the Installed patches drop-down menu, select the desired service pack. (Note that the navigation buttons near the bottom of the web page can also be used to select a service pack.)

Step 3 Click **Go**. The fields on the page are populated with the data for the specified service pack, and the Remove Patch and View Log Entries buttons are activated for the service pack.

Installing Service Packs

Installing a service pack is a two-step process. First the file is transferred using the Transfer web page. Then it is installed from the Install Patch web page. Multiple files can be transferred to the BBSM server before they are installed.

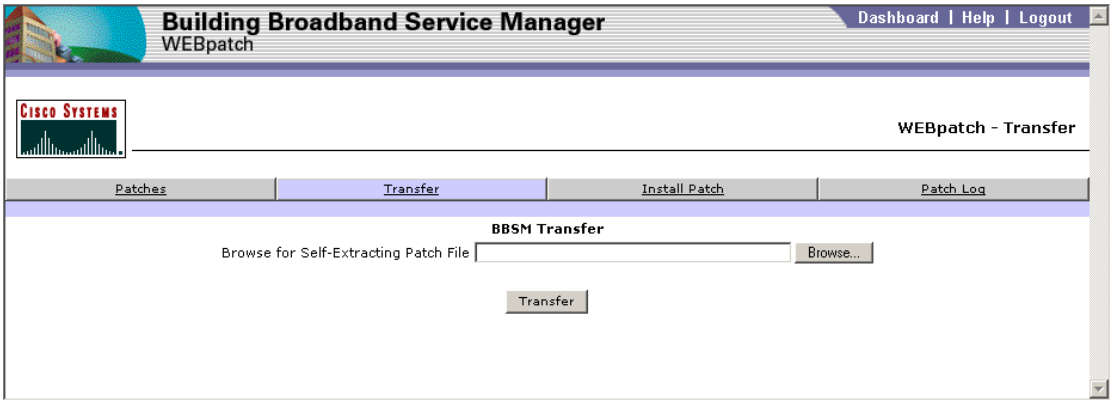
Caution Transfer and install only service packs properly obtained from Cisco Systems to ensure successful updates to the BBSM server.

Step 1 Confirm that the service pack executable file is accessible. Most BBSM service packs are available over the Internet. Be sure the file has been downloaded before continuing.

Step 2 From the BBSM Dashboard, click **WEBpatch**. The WEBpatch splash screen appears, followed by the Patches web page appears.

Step 3 Click the **Transfer** button. The BBSM Transfer web page appears. (See Figure 5-2.)

Figure 5-2 Transfer Web Page



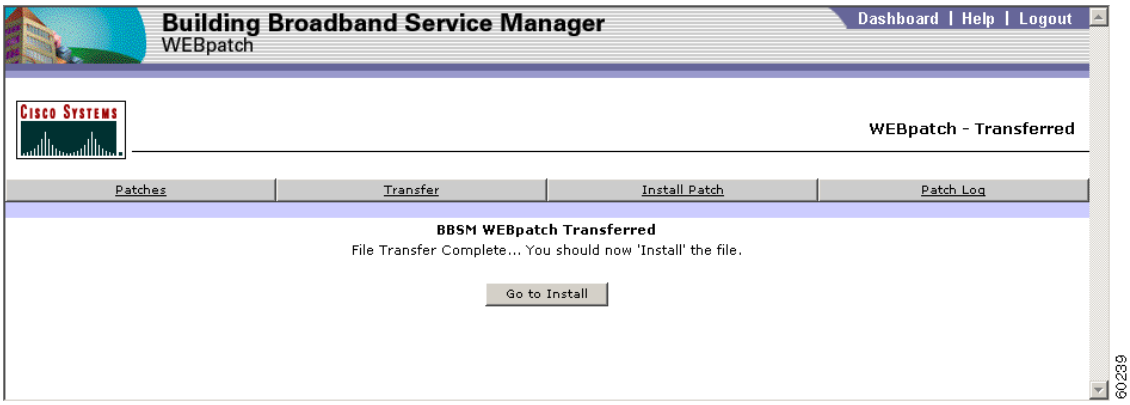
Step 4 In the BBSM Transfer field, click the **Browse...** button.

Step 5 Navigate to the service pack being installed and select it. Click **Open**. The service file name appears in the BBSM Transfer field.

Step 6 Click the **Transfer** button under the service pack file name.

- If the transfer is successful, the BBSM WEBpatch Transferred web page appears, prompting you to install the service pack. Go to Step 7. (See Figure 5-3.)
- If the service pack does not transfer, an error message appears. For information about the error, click the Patch Log button to view the error log. Also, see the "Viewing WEBpatch Logs" section on page 5-6.

Figure 5-3 BBSM WEBpatch Transferred Web Page



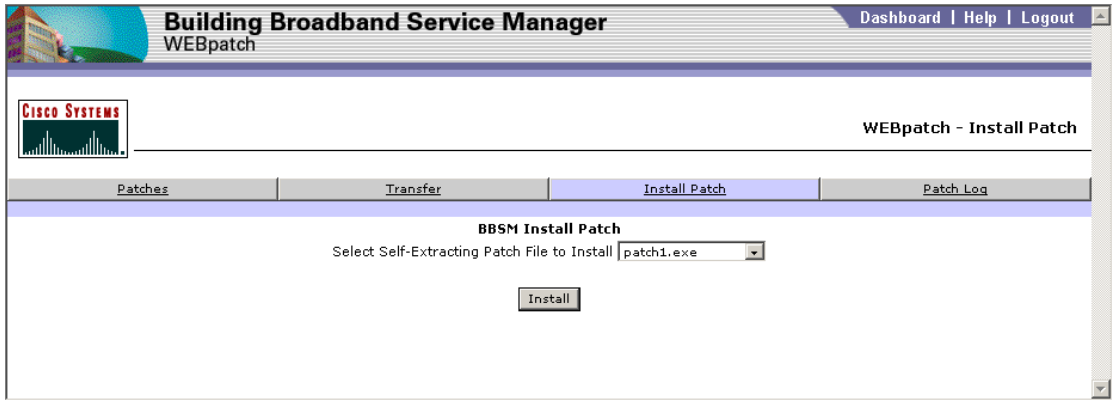
Step 7 To install the service pack at this time, click **Go to Install**. If more than one service pack is being transferred at this time, click the Transfer button again to continue transferring files. After all files are transferred, continue with the install.

Step 8 To install the files at a later time, follow the steps below:

a. Click the **BBSM Install Patch** button. The BBSM Install Patch web page appears. (See Figure 5-4.)

b. At the BBSM Install Patch web page, from the drop-down menu, select the desired service pack.

Figure 5-4 Install Patch Web Page



Step 9 Click the **Install** button. The service pack is automatically verified and installed.

Step 10 If desired, click the **Patch Log** button and review the patch log for confirmation and any messages.

Note After the service pack or patch has been installed, the BBSM server may automatically reboot. While the server is rebooting, you cannot access the BBSM server

Removing Service Packs

If necessary, service packs can be removed from the Patches web page, although we do not recommend removing them. (See Figure 5-1.) Note that service packs can no longer be removed if you have installed the MSFix1 patch.

Step 1 From the BBSM Dashboard, click **WEBpatch**. The WEBpatch splash screen appears, followed by the Patches web page appears.

Step 2 From the Installed patches drop-down menu, select the service pack to be removed.

Step 3 Click **Go**.

Step 4 Click **Remove Patch**.

- If the patch is removed successfully, you can click the Patch Log button and check for confirmation and any messages.
- If the service pack is not removed, an error message appears. Again, click the Patch Log button to review the error log. See the "Viewing WEBpatch Logs" section on page 5-6.

Note If the server needs to be rebooted to finish the removing the service pack, a message appears telling you to reboot. Click the appropriate button to continue. Access to the BBSM server and WEBpatch is not available while the server is rebooting.

Viewing WEBpatch Logs

All WEBpatch activity log entries for the BBSM server can be viewed by using the Patch Log web page in WEBpatch. (See Figure 5-5.) Selected messages are retrieved by using the three drop-down menus at the top part of the page. (See Table 5-3.)

Figure 5-5 WEBpatch Patch Log Page

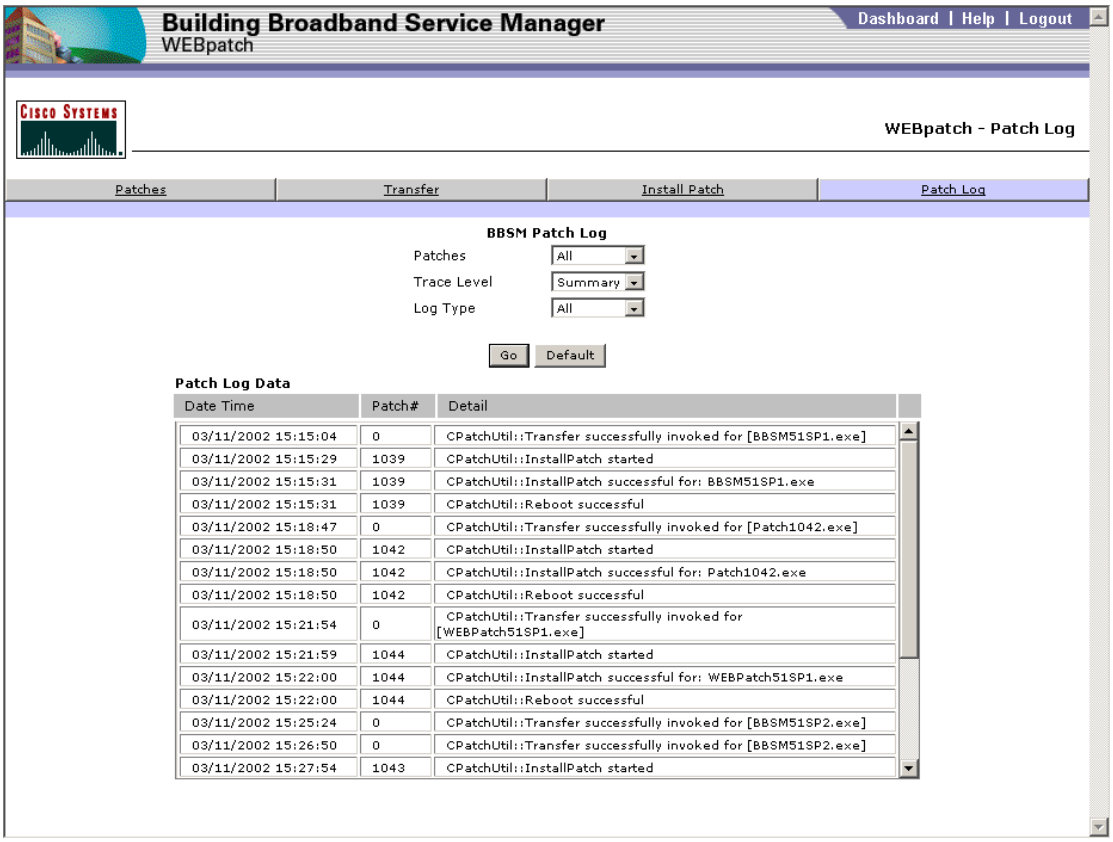


Table 5-3 Patch Log Parameters for Retrieving Messages

Parameter	Options for Retrieval
Patches	• All (default setting)—Shows messages for all service packs • <service_pack_number>—Shows only PatchLog entries for the specific service pack
Trace Level	• All—Shows all trace levels • Summary (default setting)—Lists only the high level summary • Detail—Shows all the messages for all actions performed during WEBpatch activities. • Debug—Not applicable (used by Cisco Support)
Log Type	• All (default setting)—Shows all entries for all log types • Transfer—Shows only entries for file transfers • Install—Lists only installation related entries • Remove—Shows messages concerning files removed • Other—Displays messages generated by Windows and other programs during WEBpatch activities

Use the following procedure to view the WEBpatch logs.

Step 1 From the BBSM Dashboard, click **WEBpatch**. The WEBpatch splash screen appears, followed by the Patches web page appears.

Step 2 Click the **Patch Log** button. (This page can also be accessed from the Patches page by using the View Log Entries button.)

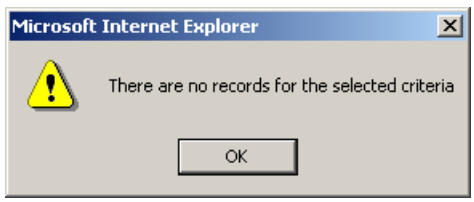
Step 3 From the Patches drop-down menu, select the desired service pack (or **All).**

Step 4 From the Trace Level drop-down menu, select the desired trace level data.

Step 5 From the Log Type drop-down menu, select the desired log type.

Step 6 Click **Go**. The messages are displayed in the Patch Log Data table. If needed, scroll to view all the messages. Note that if no log information meets the selected criteria, a dialog box appears, stating that there are no records for the selected criteria. (See Figure 5-6.) Click **OK** to return to the Patch Log page to change the search parameters.

Figure 5-6 WEBpatch Patch Log Page



Note Clicking the **Default** button selects All patches, the Summary trace level, and All log types and then automatically displays the appropriate messages.

BBSM Operations

The Operations section of the BBSM Dashboard allows you to view port data, perform port maintenance, change port assignments, and manage access codes on an operating BBSM server. The following four Operations options require administrator or operator privileges for access:

- Port Control
- Map Rooms
- Subscription Port Control
- Access Code Management

These options are described in the sections that follow.

Port Control

The Port Control web pages allow you to view port control data and perform port maintenance for all policies except for subscription policies. Port control information is displayed in either the List View format or the Form View format. The List View is the default format that is used to view the port information. The Form View is used to change the port information for a specific port. Note that administrator or operator privileges are required to access the Form View web pages.

Note To use either of the port control web pages, you must first generate a port map.

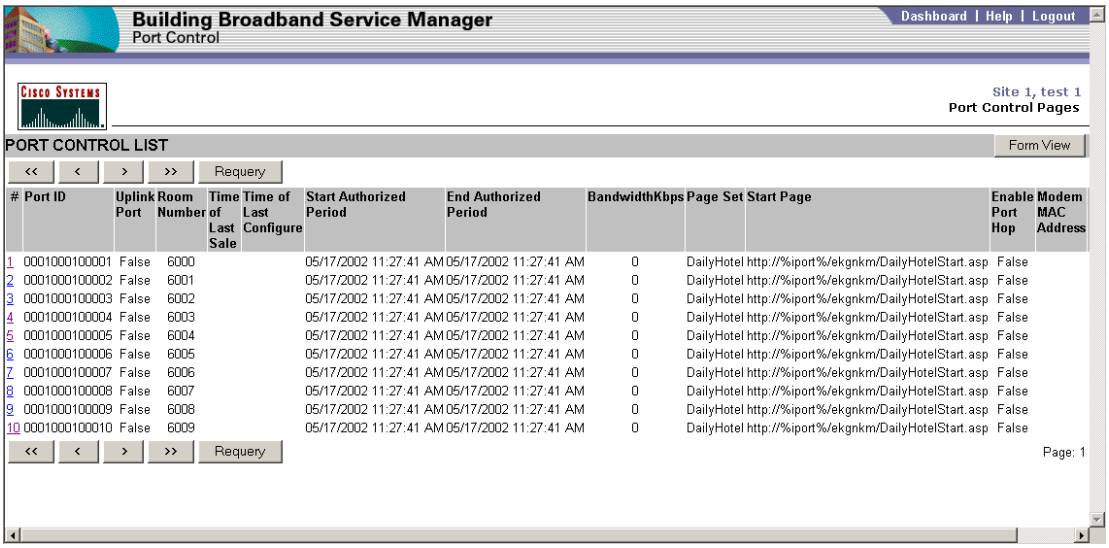
Using the Port Control List View

The Port Control List View allows you to view the behavior of individual ports. It displays all the ports for a site in groups of ten.

Note Information cannot be changed in List View. You must switch to Form View for editing.

Step 1 From the BBSM Dashboard, click **Port Control**. The List View web page appears. (See Figure 6-1.)

Figure 6-1 Port Control List View Web Page



Step 2 Use the navigation buttons to scroll through the list until you find the desired entry.

Using the Port Control Form View

The BBSM port settings for access policies, except for a Subscription access policies, can be viewed and/or changed by using the Form View of the Port Control option, which is accessed on the BBSM Dashboard. The Form View displays the settings for a single port in a data entry form. It is accessed from the List View web page.

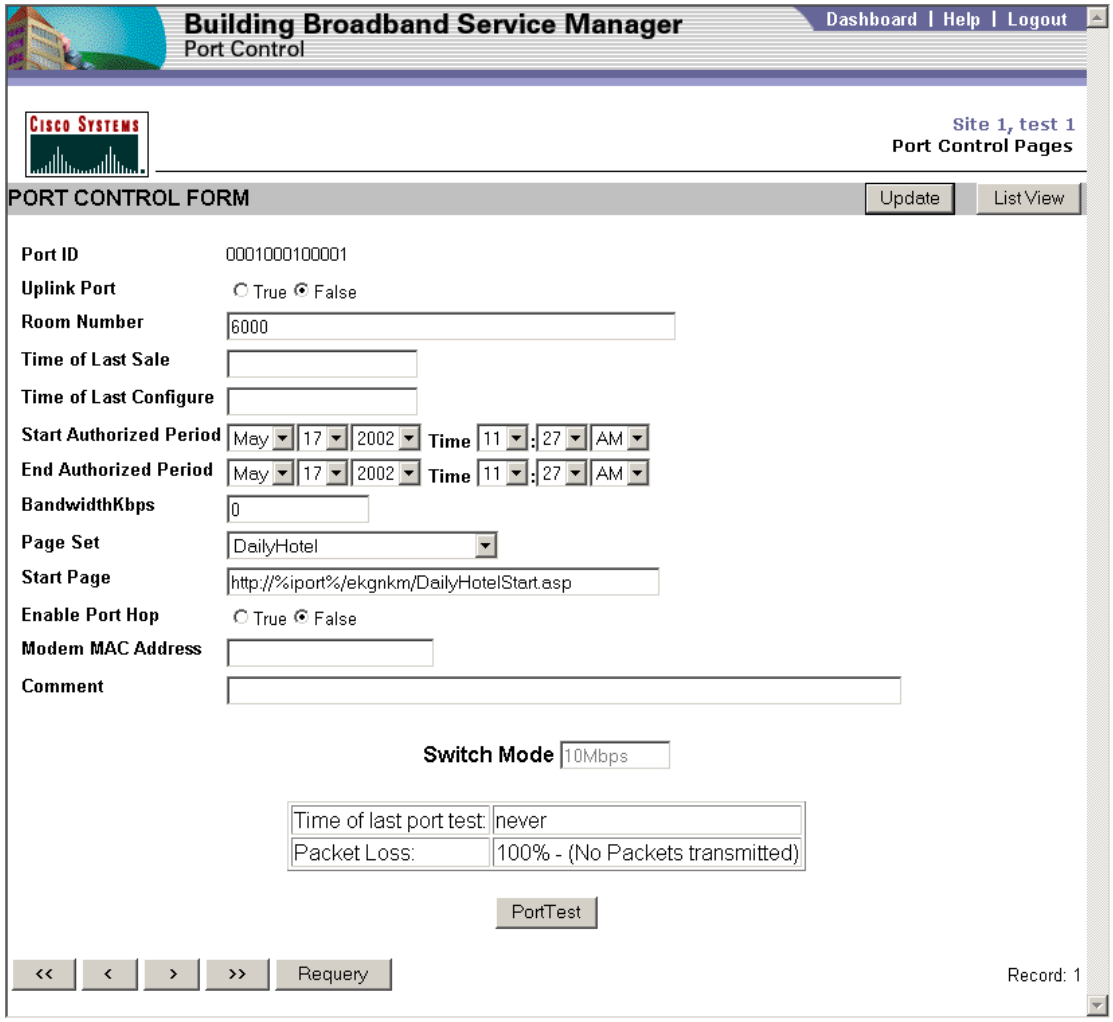
Note Only those with administrator or operator privileges can access and use the Form View.

Use the following procedure to view and/or change the Port Control Form View data for each port.

Step 1 From the List View web page, click the desired port number (below the # column). The Port Control Form View web page appears. (See Figure 6-2.)

Caution Before making any changes, be sure the Port ID and room number shown correspond to the port you want to change. If they do not, use the navigation buttons or the List View to find the correct port.

Figure 6-2 Port Control Form View Web Page



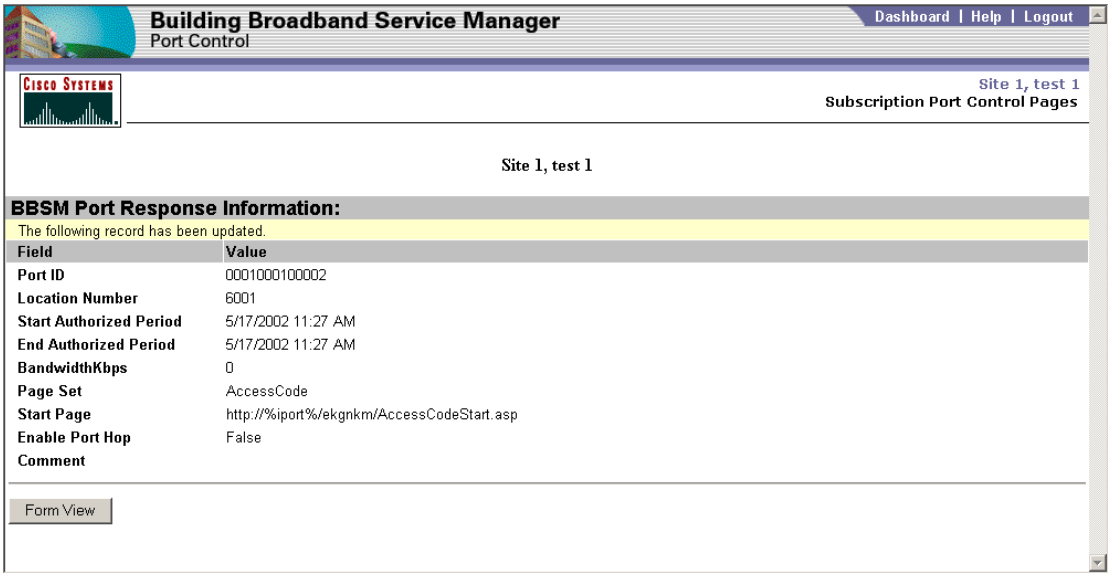
Step 2 In the Port Control Form fields, enter the appropriate information. (See Table 6-1.)

Table 6-1 Port Control Form View Descriptions

Field	Description
Port ID	Unique number assigned to each port using the Switches web page. This number cannot be changed. The port ID incorporates the stack, switch, and port number on the switch. Usually recorded as xxxxyyyyzzzzz. Where xxxx is the stack, yyyy is the switch, and zzzzz is the port.
Uplink Port	Select True or False. Indicates whether or not the port is used as an uplink to another switch. BBSM ignores MAC addresses learned on uplink ports so that it does not report that clients are connected to these ports.
Room Number	Type the room number associated with this port. You can also enter text rather than a number.
Time of Last Sale	Enter the time of the last transaction on this port. You must use the standard time format. The BBSM server maintains this number. This field does not usually need to be changed.
Time of Last Configure	Enter the time of the last configuration changes made on this port. You must use the standard time format. The BBSM server maintains this number. This field does not usually need to be changed.
Start Authorized Period	Enter the start date and time of the interval during which the port is authorized for use if port is configured for Subscription page sets. Use the standard time format. Note that the default entry is the time that the port map was generated.
End Authorized Period	Enter the end date and time of the interval during which the port is authorized for use if port is configured for Subscription page sets. Use the standard time format. Note that the default entry is the time that the port map was generated.
Bandwidth Kbps	This field is only used with the Subscription and RADIUS access methods. When it is used, it specifies the bandwidth (in kbps) that the port uses if the bandwidth is not specified through the web page. The value is an integer from 1 to 2000000 (2 Gbps) or 0 to represent the maximum bandwidth available. The default entry is “0 Full.”
Page Set	Select the desired page set. This field specifies the page set used by the site.
Start Page	The URL that the BBSM system client software displays at the start of the session. The user can click Connect to request access to the Internet. See the Start Page field on the Port Map web page for more details.
Enable Port Hop	Select True or False. Indicates whether or not a user is allowed to hop to another port.
Modem MAC Address	This field is used in cable modem or DSL installations. Type the physical Ethernet address of the modem that connects this port to the system. The BBSM server maintains this number.
Comment	Blank area for entering extra information concerning this port.

Step 3 Click **Update**. The Port Control update confirmation web page appears. (See Figure 6-3.)

Figure 6-3 Port Control Update Confirmation Web Page



Step 4 Click **List View** to return to the Port Control List.

Tip You can click **Requery** at any time to refresh the list.

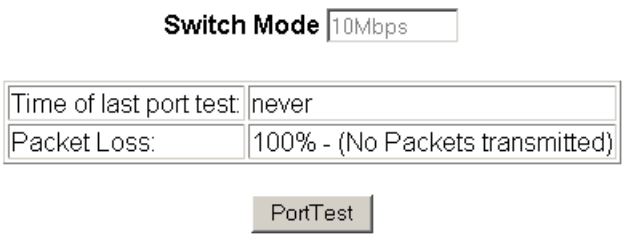
Port Test

You can test the port using the information at the bottom of the Port Control Form View web page. (See Figure 6-4.)

The information at the bottom of the page shows the “Time of the last port test” and “Packet Loss” in the left column and the related information displayed in the right column. Below the table is the Port Test button. When you click this button, the port is tested and the results are shown in the table.

Note A client must be active on the port for the port test to work.

Figure 6-4 Port Test Information on the Form View Web Page



Mapping Rooms

Room can be mapped or remapped by using the Map Rooms option under Operations on the BBSM Dashboard. This option is allows you to change port assignments for a room, meeting room, or public space. Because this option is part of the initial BBSM configuration, it is discussed in detail in the "Mapping Rooms and Port Testing" section on page 3-20.

Subscription Port Control

The Subscription Port Control option allows you to view port control data and/or perform maintenance for ports that are associated with a Subscription access policy. For access policies other than the Subscription access policy, use the Port Control option.

Using the Subscription Port Control option, you can obtain information to:

- Activate or deactivate BBSM port connections in any room within a site that use a subscription access policy.
- Specify a different policy.

Subscription Port Control information is displayed in either List View format or Form View format. The List View is the default format and is used to view the port information. The Form View is used to change the port information on a specific port. Note that administrator or operator privileges are required to access the Form View web pages.

Note To use either of the port control web pages, you must first generate a port map.

Using the Subscription Port Control List View

Subscription Port Control Lists are on a site basis and are used to view port information. It displays all the ports for a site using a subscription access policy in groups of ten.

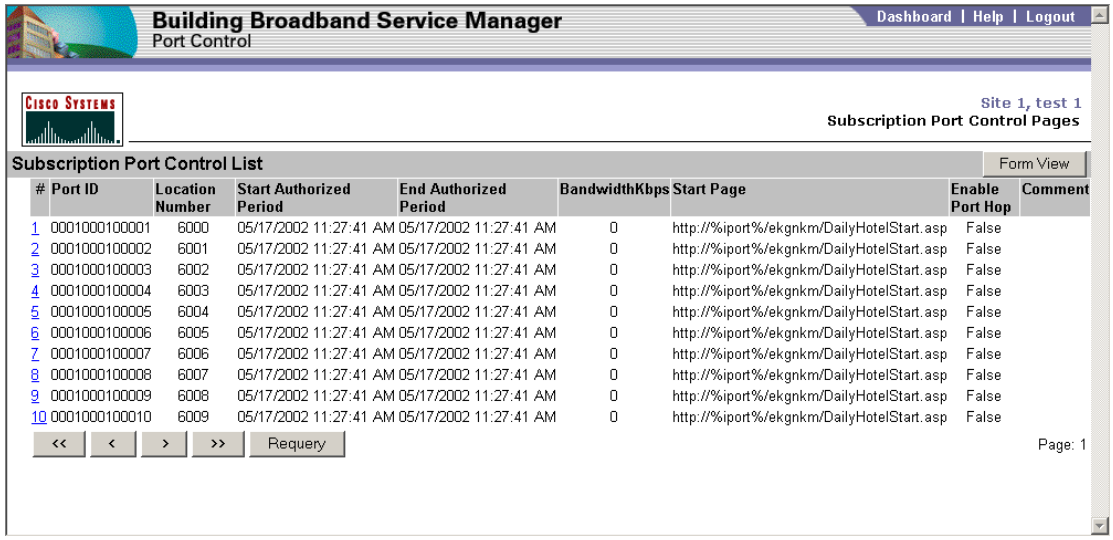
Note Information cannot be changed in List View. You must switch to Form View for editing.

Use the following procedure to view and/or change the Subscription Port Control List View data for each port.

Step 1 From the BBSM Dashboard, click **Subscription Port Control**.

Step 2 If prompted, enter a valid user login and password. The Subscription Port Control List View web page appears. (See Figure 6-5.)

Figure 6-5 Subscription Port Control List View Web Page



#	Port ID	Location Number	Start Authorized Period	End Authorized Period	BandwidthKbps	Start Page	Enable Port Hop	Comment
1	0001000100001	6000	05/17/2002 11:27:41 AM	05/17/2002 11:27:41 AM	0	http://%iport%/ekgnkm/DailyHotelStart.asp	False	
2	0001000100002	6001	05/17/2002 11:27:41 AM	05/17/2002 11:27:41 AM	0	http://%iport%/ekgnkm/DailyHotelStart.asp	False	
3	0001000100003	6002	05/17/2002 11:27:41 AM	05/17/2002 11:27:41 AM	0	http://%iport%/ekgnkm/DailyHotelStart.asp	False	
4	0001000100004	6003	05/17/2002 11:27:41 AM	05/17/2002 11:27:41 AM	0	http://%iport%/ekgnkm/DailyHotelStart.asp	False	
5	0001000100005	6004	05/17/2002 11:27:41 AM	05/17/2002 11:27:41 AM	0	http://%iport%/ekgnkm/DailyHotelStart.asp	False	
6	0001000100006	6005	05/17/2002 11:27:41 AM	05/17/2002 11:27:41 AM	0	http://%iport%/ekgnkm/DailyHotelStart.asp	False	
7	0001000100007	6006	05/17/2002 11:27:41 AM	05/17/2002 11:27:41 AM	0	http://%iport%/ekgnkm/DailyHotelStart.asp	False	
8	0001000100008	6007	05/17/2002 11:27:41 AM	05/17/2002 11:27:41 AM	0	http://%iport%/ekgnkm/DailyHotelStart.asp	False	
9	0001000100009	6008	05/17/2002 11:27:41 AM	05/17/2002 11:27:41 AM	0	http://%iport%/ekgnkm/DailyHotelStart.asp	False	
10	0001000100010	6009	05/17/2002 11:27:41 AM	05/17/2002 11:27:41 AM	0	http://%iport%/ekgnkm/DailyHotelStart.asp	False	

Step 3 Use the navigation buttons to scroll through the list until you find the desired entry.

Using the Subscription Port Control Form View

The BBSM port settings for a Subscription access policy can be viewed and/or changed by using the Form View of the Subscription Port Control option, which is accessed on the BBSM Dashboard. The Form View displays the settings for a single port in a data entry form. It is accessed from the List View web page.

Note Only users with administrator or operator privileges can access and use the Form View.

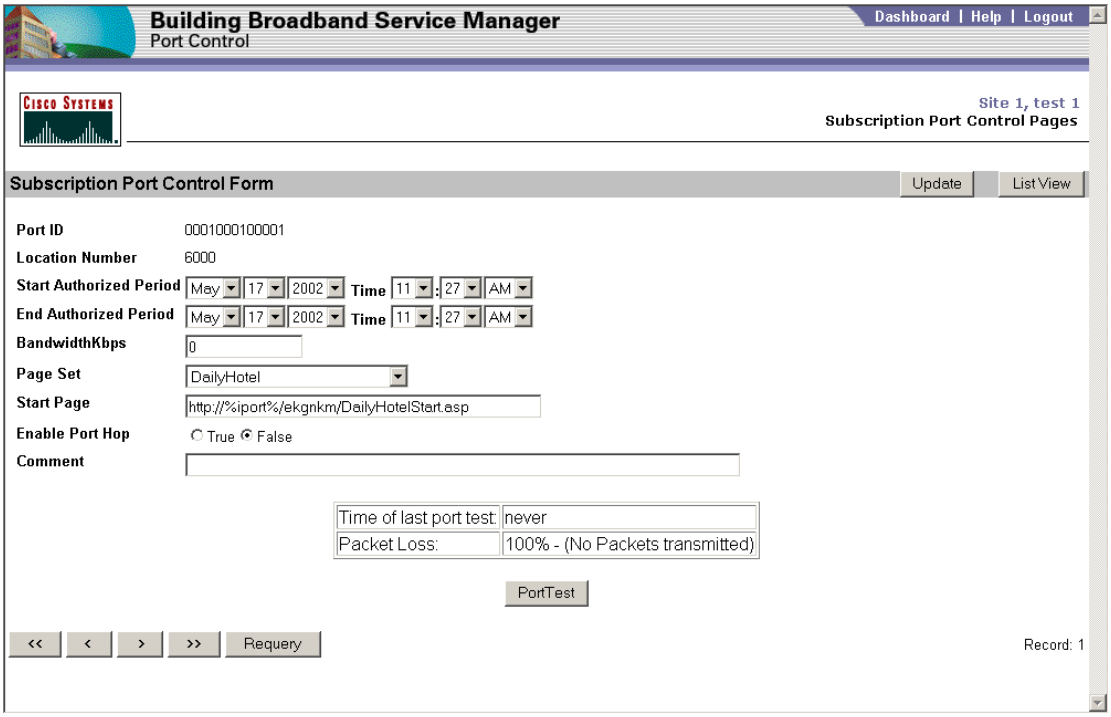
Use the following procedure to view and/or change the Subscription Port Control Form View data for each port.

Step 1 From the List View web page, do one of the following.

- Click **Form View**.
- Click the number (below the # column). The Subscription Port Control Form appears. (See Figure 6-6.)

Caution Before making any changes, be sure that the Port ID and location number shown correspond to the port you want to change. If they do not, use the navigation buttons or List View to find the correct port.

Figure 6-6 Subscription Port Control Form View Web Page



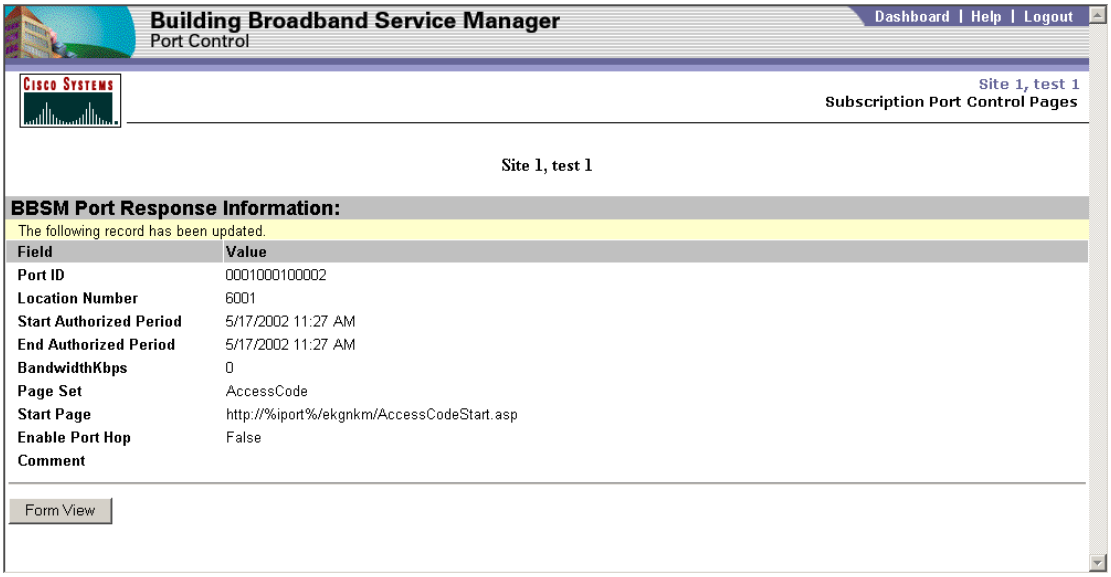
Step 2 In the Subscription Port Control Form fields, enter the appropriate information. (See Table 6-2.)

Table 6-2 Subscription Port Control Form View Descriptions

Field	Description
#	Record number
Port ID	ID of the port as defined when the property is port mapped. For reference only. You can't change this field from the BBSM Subscription Port Control page. The port ID incorporates the stack, switch, and port number on the switch. Usually recorded as xxxxyyyyzzzzz. Where xxxx is the stack, yyyy is the switch, and zzzzz is the port.
Location Number	Location number of the port (for example, an apartment number or meeting room, or default) as defined when the property is port mapped. This is for reference only. You cannot change this field from the BBSM Subscription Port Control page. This is known as the room number on other reports. Location number appears because the Subscription method is often used with apartments.
Start Authorized Period	Starting date and time during which this BBSM port can be used. (The port cannot be used before this date and time.) Default: The time that the port map was generated.
End Authorized Period	Ending date and time during which this BBSM port can be used. (The port cannot be used after this date and time.) Default: The time that the port map was generated.
BandwidthKbps	Bandwidth in kilobits per second that the port will use if the bandwidth is not specified. This applies to the Subscription model only.
Start Page	Specify 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.
Enable Port Hop	True/False
Comment	A user-defined comment describing this port (optional).

Step 3 Click **Update**. The Subscription Port Control update confirmation web page appears. (See Figure 6-7.)

Figure 6-7 Subscription Port Control Update Confirmation Web Page



Step 4 Click **Form View**.

Step 5 Click **List View** to return to the Subscription Port Control List.

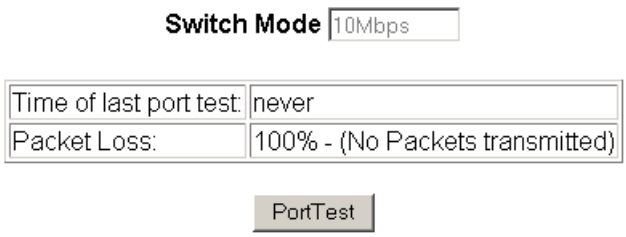
Tip You can press **Requery** at any time to refresh the list.

Subscription Port Control Port Test

You can test a specific port using the information at the bottom of the Subscription Port Control Form View web page. (See Figure 6-8.)

The information at the bottom of the page shows the "Time of the last port test" and "Packet Loss" in the left column and the related information is displayed in the right column. Below the table is the Port Test button. When you click this button, the port is tested and the results are shown in the table.

Figure 6-8 Port Test Information on the Form View Web Page



Note A client must be active on the port for the port test to work.

Access Code Management

The Access Code Management option under Operations on the Dashboard allows you to provide high-speed Internet access for meeting or conference rooms. It also allows you generate, edit, and delete access codes. This option also provides control and accountability for end users viewing access codes and retrieving transaction history.

Configuring Access Codes for Meeting Rooms

The administrator or operator can configure access so that either multiple users or only one person at a time can use a particular access code. This is determined by the page set selected for the meeting room site or ports:

- For exclusive access by only one person at a time, select the MeetingRoom page set.
- For multiple access by more than one person per code, select the AccessCode page set.

BBSM Access Code Management can be configured one of two ways:

- Configure Site 1 so that Site 1 consists of only meeting rooms.
- Configure by port so that a mixture of meeting rooms and guest rooms exists on the site.

Note that configuring your meeting rooms by site or by port does not depend on the physical layout of the property but on how you want to manage your BBSM server.

Note When using access codes, all of the BBSM sites must be located in the same time zone.

Configuring Site 1 to Only Support Meeting Rooms

If you want to configure your meeting rooms so that they are all on the same site, use the following steps. Assuming that your guest rooms are in Site 1, the following steps use Site 2 for meeting rooms.

Note Site 1 must be created before it can be configured.

Step 1 From the BBSM Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

Step 2 Click the **Port Map** button.

Step 3 Verify that the site number is “2.”

Step 4 From Page Set drop-down menu, select **MeetingRoom** or **AccessCode**.

Step 5 Make all other necessary selections for your site.

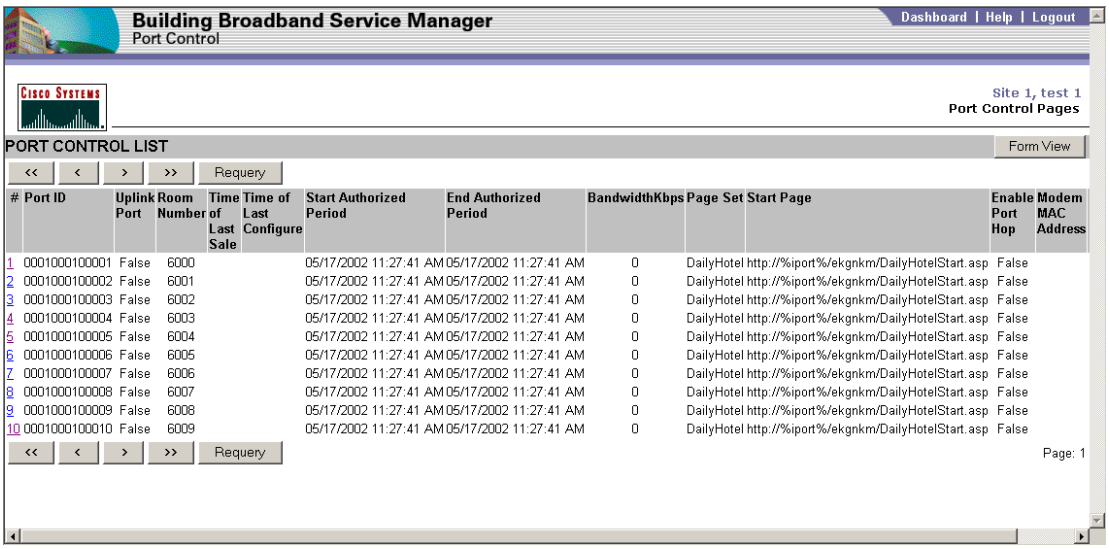
Step 6 Click **Generate**.

Configuring Individual Ports as Meeting Rooms

If you want to configure your meeting rooms in the same sites as your guest rooms, you must configure the port for each meeting room separately. Use the following procedure to configure each port as a meeting room.

Step 1 From the BBSM Dashboard, click **Port Control**. The Port Control List View web page appears. (See Figure 6-9.)

Figure 6-9 Port Control List View Web Page



Note The user must be a member of the BBSM Operator or Administrators group to access the Port Control web page.

Step 2 Use the navigation buttons to select the meeting room port. Note that the meeting room ports can be identified by their page sets, which will be either MeetingRoom or AccessCode.

Step 3 In the Port Control List View web page, click the desired port number (below the **#** column). The Port Control Form View web page appears. (See Figure 6-2 on page 6-3.)

Step 4 From the Page Set drop-down menu, select **MeetingRoom**.

Note The Start Page field is automatically set based on the Page Set selection.

Step 5 Enter any other changes as needed.

Step 6 Click **Update**, which is located in the top right corner of the web page.

Step 7 Close the browser when finished.

Access Code Functions

The Access Code Management screens are designed to be used to issue access codes to clients. A local administrative computer is typically configured within the property, and the default home page of the browser is set to http://localhost:9488/accesscodes.

The BBSM Access Code Management provides three different functions:

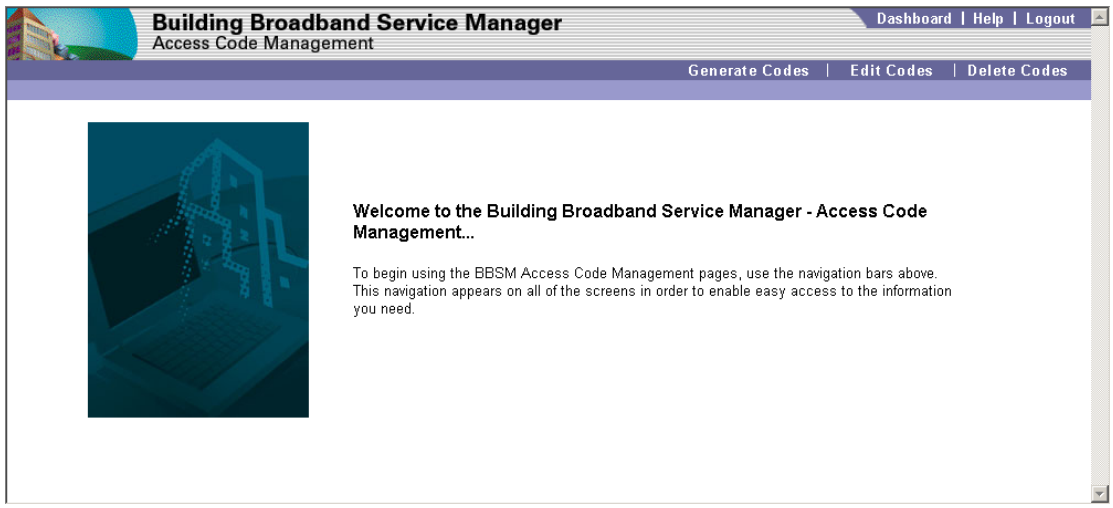
- Generate Codes
- Edit Codes
- Delete Codes

Generating Access Codes

This option provides the hotel manager or administrator with the ability to generate access codes from the BBSM Access Code Management startup web page. Access codes are generated for the end user for a specific date, bandwidth, and price (if applicable).

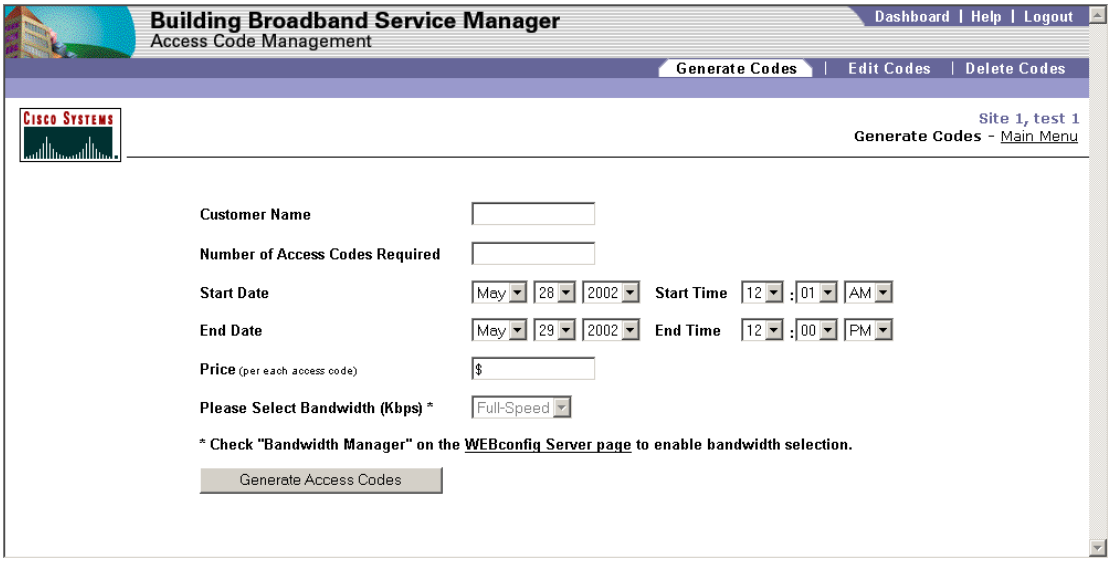
Step 1 From the BBSM Dashboard, click **Access Code Management**. The Access Code Management startup web page appears. (See Figure 6-10.)

Figure 6-10 BBSM Access Code Management Start Up Web Page



Step 2 From the primary navigation buttons, click **Generate Codes**. The Generate Codes web page appears. (See Figure 6-11.)

Figure 6-11 Generate Codes



Step 3 Enter the desired values or select from drop-down menus.

Step 4 Click **Generate Codes**.

Note If the default MeetingRoom page set is being used, another user cannot use access codes at the same time.

The following table explains the fields and various settings available on the Access Codes Management Generate Codes page.

Table 6-3 Generate Codes Field Descriptions

Field	Description
Customer Name	Enter the name of the end user being supplied with the access codes. Note that customer names can be reused. Punctuation, such as apostrophes and quotation marks, in customer names cannot be used, because they are reserved characters.
Number of Access Codes Required	Enter the quantity of access codes being assigned or sold to this end user. If a particular end user is requesting more than one bandwidth option, access codes must be generated separately for each bandwidth option.
Start Date and Start Time	Select the start date from the drop-down menu. The start time settings are available in hour and minute increments. The default date is the current date. The default time is "12:01 AM."
End Date and End Time	Select the end date from the drop-down menu. The end time settings are available in hour and minute increments. The default date is the current date plus one day. The default time is "12:00 PM."
Price (per each access code)	The administrator sets the price value.
Please Select Bandwidth (Kbps)	Select the desired bandwidth speed from the drop-down menu: Full-Speed, 512 Kbps, 256 Kbps, 128 Kbps, or 64 Kbps. If Bandwidth Manager on the Server web page is enabled, the bandwidth options are displayed. If Bandwidth Manager is not enabled, this field is grayed out. Note that the settings are only bandwidth maximums and not guaranteed speeds. The default speed is Full-Speed.

Editing Access Codes

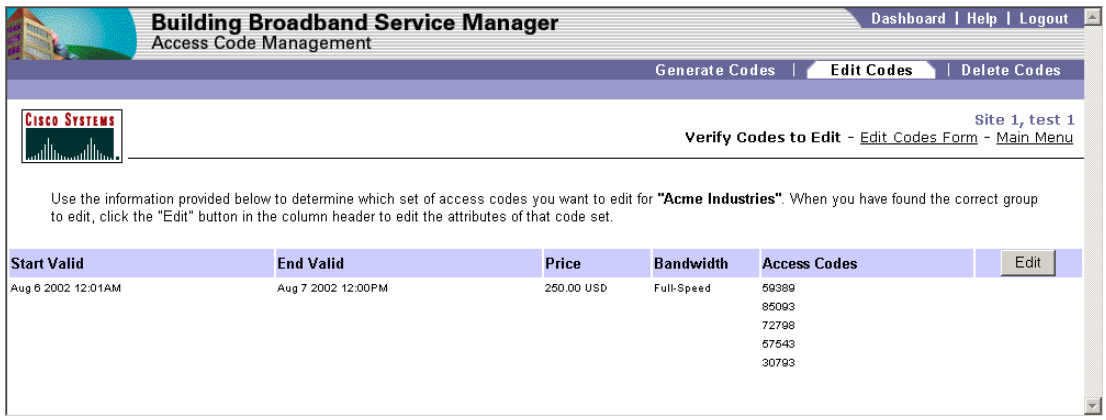
Use the following procedure to edit the access codes, if necessary.

Step 1 From the primary navigation bar for Access Code Management, click **Edit Codes**.

Step 2 Select **Customer Name** from the drop-down menu.

Step 3 Click **Find Codes**. The Verify Codes to Edit web page appears. (See Figure 6-12.)

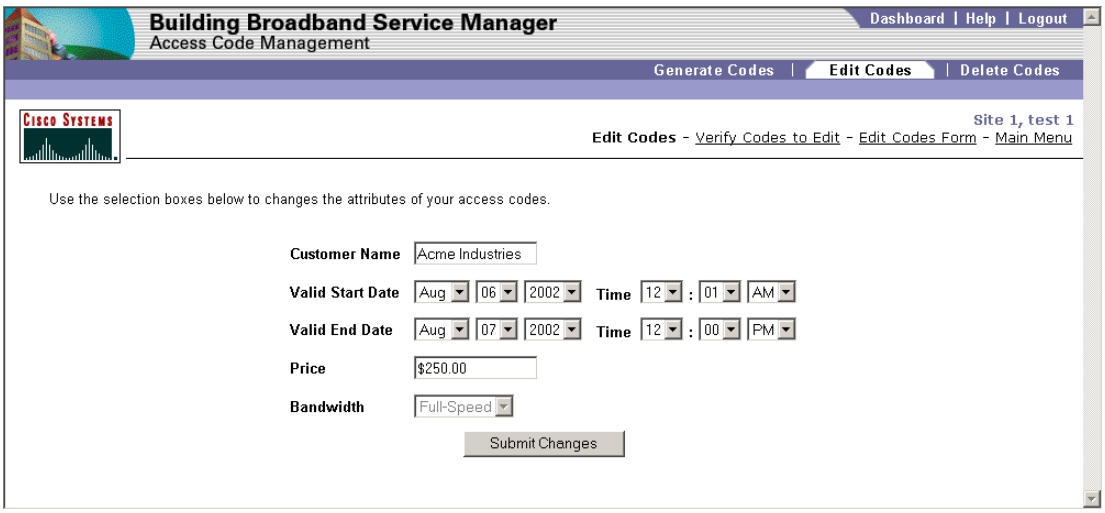
Figure 6-12 Verify Codes to Edit Web Page



Step 4 Locate the set of access codes to edit.

Step 5 Click **Edit**. The Edit Codes web page appears. (See Figure 6-13.)

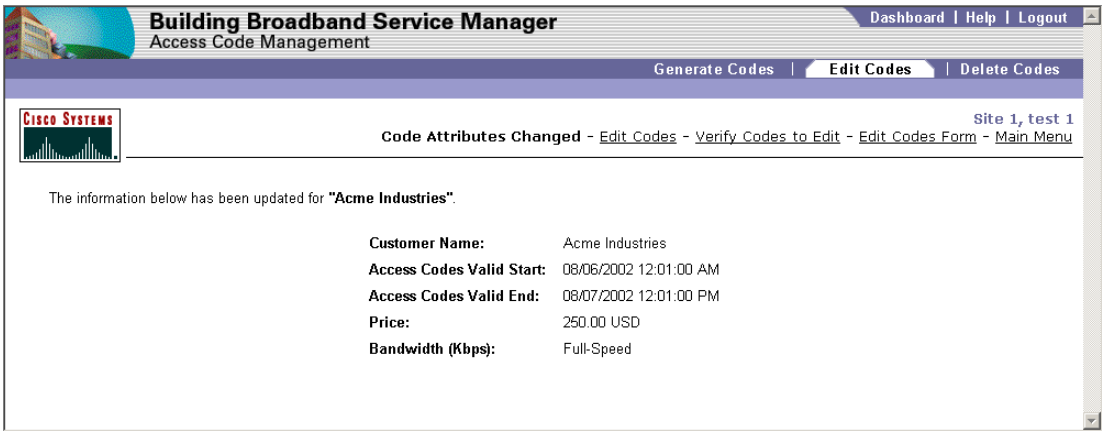
Figure 6-13 Edit Codes Web Page



Step 6 Enter any desired changes.

Step 7 Click **Submit Changes**. The Code Attributes Changed web page appears. (See Figure 6-14.)

Figure 6-14 Code Attributes Changed Web Page



Deleting Access Codes

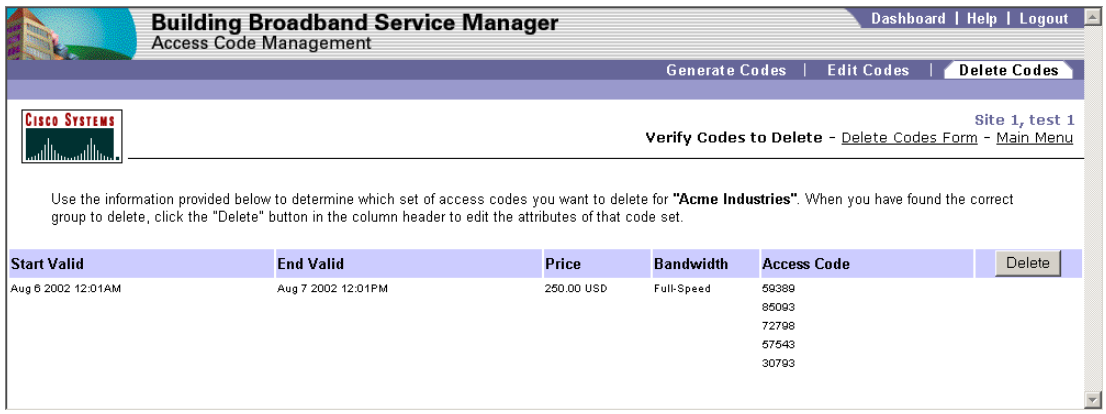
Follow this procedure to delete access codes.

Step 1 From the primary navigation bar for Access Code Management, click **Delete Codes**.

Step 2 From the Select **Customer Name** from the drop-down menu.

Step 3 Click **Find Codes**. The Verify Codes to Delete web page appears. (See Figure 6-15.)

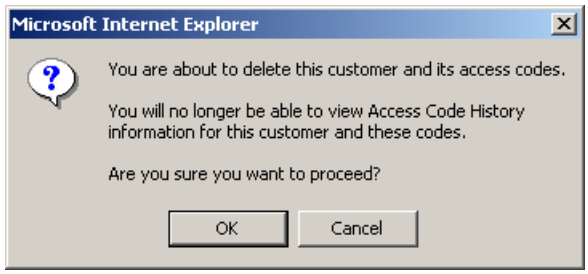
Figure 6-15 Verify Codes to Delete Web Page



Step 4 Locate the set of access codes to delete.

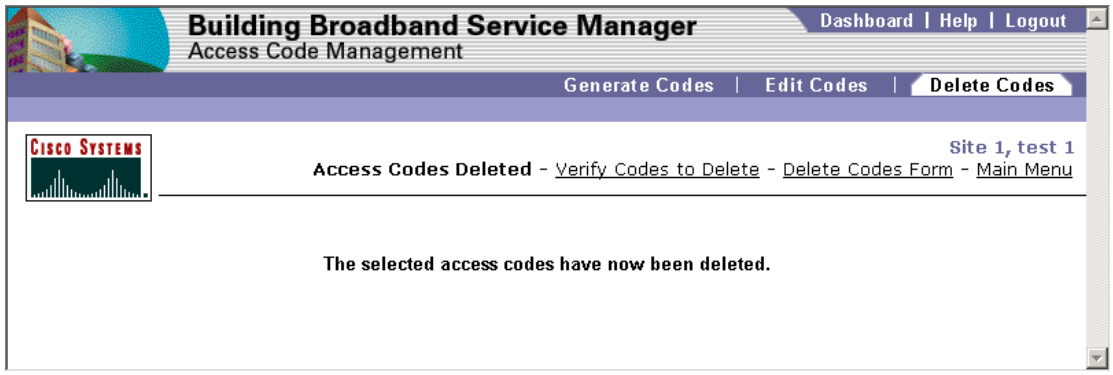
Step 5 Click **Delete**. A warning dialog box appears. (See Figure 6-16.)

Figure 6-16 Deletion Warning Dialog Box



Step 6 Click **OK**. A confirmation dialog box appears. (See Figure 6-17.)

Figure 6-17 Access Codes Deleted Confirmation Web Page



Generating Access Codes Example

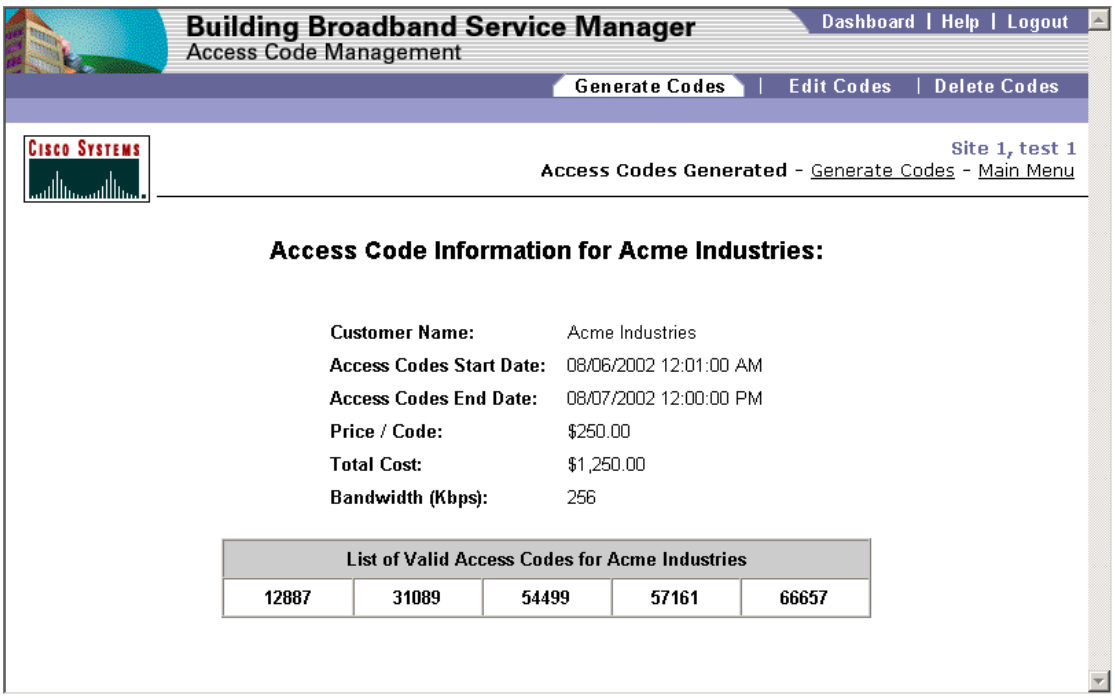
The following is an example of how to generate access codes. To use this example, enter the field values on the Generate Codes web page, as indicated in the following steps. (See Figure 6-11.)

Example 6-1 Generating Access Codes for Acme Industries

Acme Industries wants five access codes for $250 each at 256 Kbps bandwidth on August 6, 2001 from midnight to midnight. In addition, they want five access codes for $500 each at 512 Kbps bandwidth, also on August 6th, 2001 from midnight to midnight.

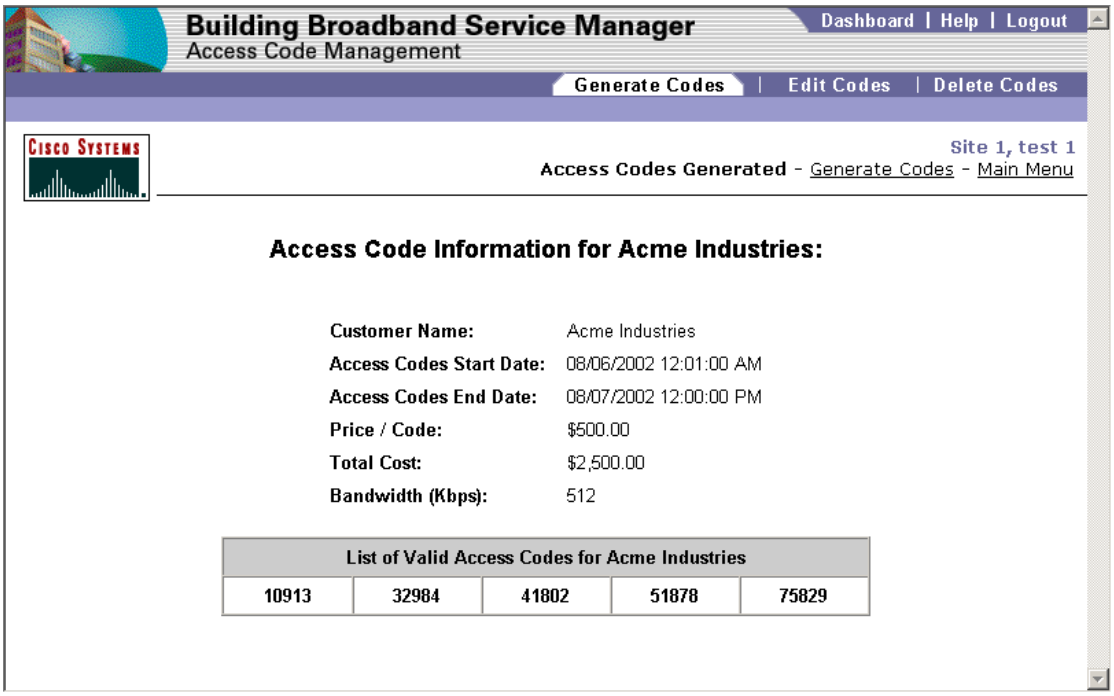
1. Launch Access Code Management from the BBSM Dashboard.
2. Click **Generate Codes** from the primary navigation bar.
3. Enter the following information:
   - Customer Name: **Acme Industries**
   - Number of Access Codes Required: **5**
   - Start Date: **Aug 6 2002**
   - Start Time: **12:01 AM**
   - End Date: **Aug 7 2002**
   - End Time: **12:00 PM**
   - Price: **250**
   - Bandwidth/KBPS: **256 Kbps**
4. Click **Generate Access Codes**. The access code information appears. (See Figure 6-18.)

Figure 6-18 Acme Industries 256 Kbps Access Code Confirmation



5. To generate additional access codes for Acme Industries, click **Main Menu** in the upper right corner of the web page. The Access Code Management web page appears.
6. Click **Generate Codes** again.
7. Enter the following information:
   - Customer Name: **Acme Industries**
   - Number of Access Codes Required: **5**
   - Start Date: **Aug 6 2002**
   - Start Time: **12:01 AM**
   - End Date: **Aug 7 2002**
   - End Time: **12:00 PM**
   - Price: **500**
   - Bandwidth/KBPS: **512 Kbps**
8. Click **Generate Access Codes**. The access code information appears. (See Figure 6-19.)

Figure 6-19 Acme Industries 512 Kbps Access Code Confirmation



Viewing and Printing BBSM Reports

Reports of BBSM activities and functions can be viewed and printed on a site basis by using the Reporting Pages option under the Reports section of the BBSM Dashboard. The following are the reports you can select:

- Usage
- Transaction History
- Active Ports
- Access Codes
- Room Mappings
- RADIUS
- Walled Garden

Use your Internet Explorer web browser to access the web pages to view or to print the available reports.

Accessing the Reporting Pages Interface

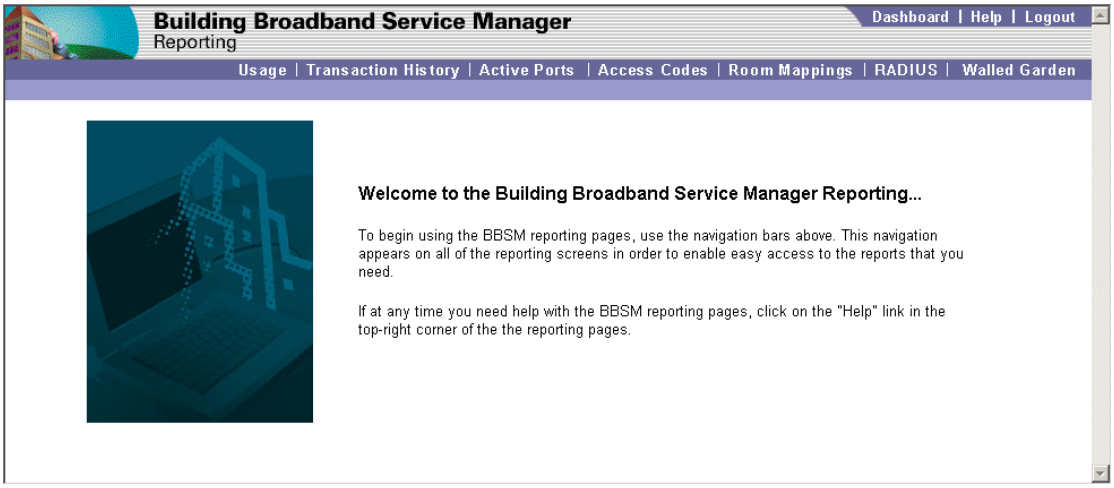
Use the following procedure to access the Reporting pages.

Step 1 For a multisite configuration, click the drop-down arrow on the BBSM Dashboard to select a site.

Step 2 Click **Reporting Pages**. The Reporting splash screen appears, followed by the BBSM Reporting web page. (You can click the splash screen to skip it.)

Step 3 To request a report, click an option from the top of the BBSM Reporting web page. (See Figure 7-1.)

Figure 7-1 Building Broadband Service Manager Reporting Web Page

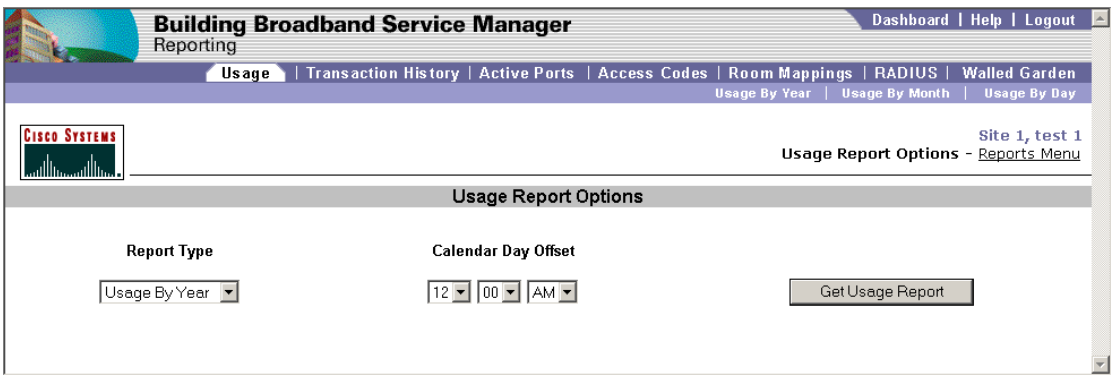


Once a report web page appears, you can sort the report by clicking on the underlined item in the header (light purple) button for any column. Clicking the same heading again switches between ascending and descending order. The sorting capability applies to all reports.

Usage Reports

Usage reports allow authorized personnel to study the use of the Internet facilities at the site. Figure 7-2 shows an example of the Usage Report web page for a site.

Figure 7-2 Usage Report Options



You can request three different reports from the Usage web page.

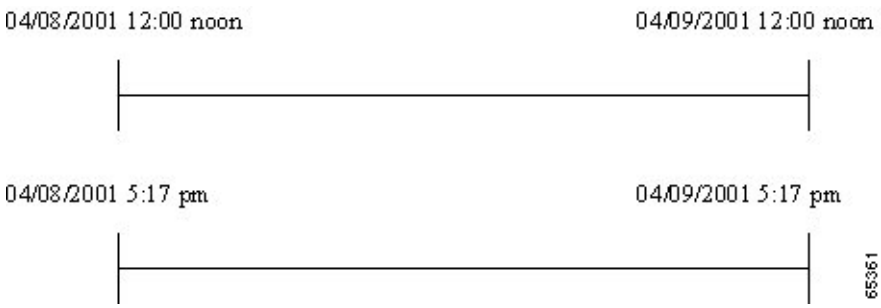
- Usage By Year
- Usage By Month
- Usage By Day

Usage Reports Calendar Day Offset

Charges posted to a PMS often do not correspond to calendar day boundaries. For example, if a hotel sends its PMS data to its data processing department at 4 a.m. each day, the charges posted will include data from the previous day after 4 a.m. up to the current day at 4 a.m. The calendar day offset feature makes it easier to reconcile BBSM accounting records with PMS records. Using the calendar day offset features, you can also choose to align the day boundaries with the checkout time at a site.

When requested, usage reports can provide reporting information for viewing by a calendar day offset. The calendar day offset can show data either from noon until noon or from a specified start time (24-hour period). Figure 7-3 shows an example of these two ways of displaying data as it occurs on 04/09/2001.

Figure 7-3 Calendar Day Offset Data Options



Usage By Year Report

The Usage By Year report lists a yearly summary of usage activity. Use the following procedure to view the report.

Step 1 From the BBSM Dashboard, click **Reporting Pages**. The Reporting splash screen appears, followed by the BBSM Reporting web page. (You can click the splash screen to skip it.)

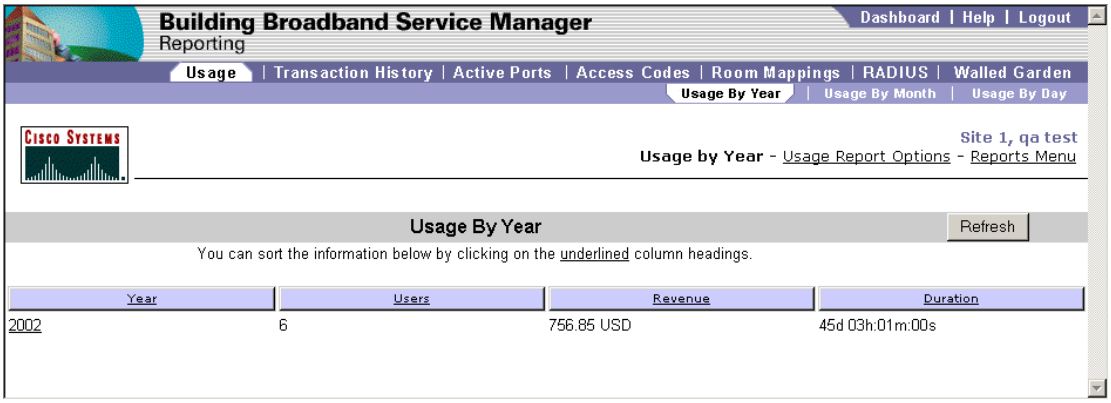
Step 2 Click **Usage**. The Usage Report Options web page appears.

Step 3 To access the usage reports, choose one of these options:

- From the secondary navigation bar, click **Usage By Year**.
- From the Report Type drop-down menu, select **Usage By Year**.

The usage report appears. (Figure 7-4 shows an example Usage By Year usage report.)

Figure 7-4 Usage By Year Report



Step 4 If desired, use the **Calendar Day Offset** option to indicate the boundary of a day for reporting purposes. Typically, you set this to match the billing cycle of a hotel PMS system.

Step 5 To view the report, click **Get Usage Report**.

Usage By Month Report

The Usage by Month report lists the monthly activity for a specific year. Use the following procedure to view the report.

Step 1 From the BBSM Dashboard, click **Reporting Pages**. The Reporting splash screen appears, followed by the BBSM Reporting web page. (You can click the splash screen to skip it.)

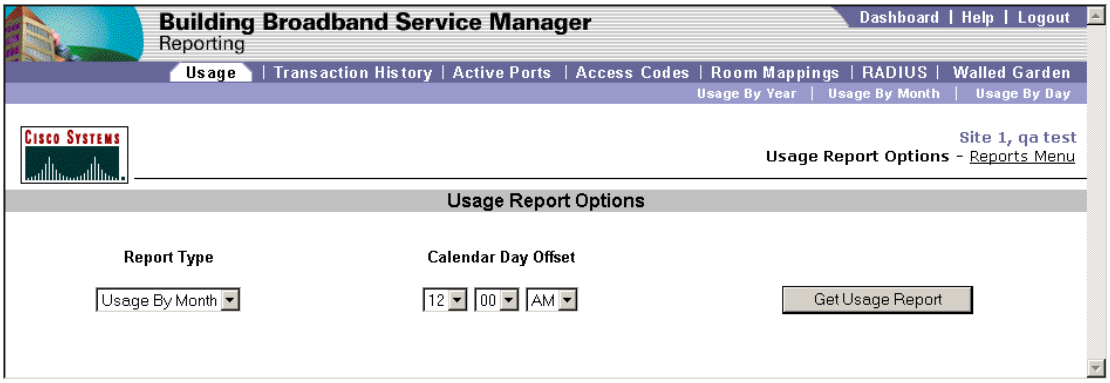
Step 2 Click **Usage**. The Usage Report Options web page appears.

Step 3 To access the usage reports, choose one of these options:

- From the secondary navigation bar, click **Usage By Month**.
- From the Usage By Year report, click the number of the desired year to see the monthly usage for that year.

The usage report appears. (Figure 7-5 shows an example Usage By Month usage report.)

Figure 7-5 Usage By Month Report



Step 4 If desired, use the **Calendar Day Offset** to indicate the boundary of a day for reporting purposes. Typically, you set this to match the billing cycle of a hotel PMS system.

Step 5 To view the report, click **Get Usage Report**.

Usage by Day Report

The Usage by Day report lists all the usage days for the specified month. Use the following procedure to view the Usage By Day report.

Step 1 From the BBSM Dashboard, click **Reporting Pages**. The Reporting splash screen appears, followed by the BBSM Reporting web page. (You can click the splash screen to skip it.)

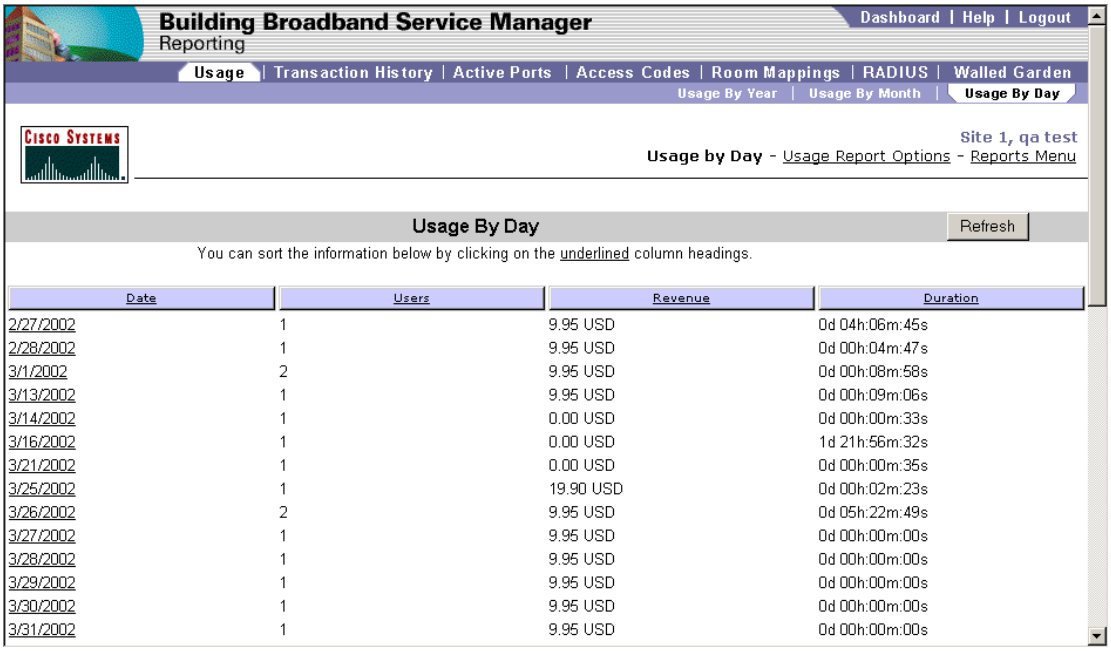
Step 2 Click **Usage**. The Usage Report Options web page appears.

Step 3 To access the usage reports, choose one of these options:

- From the secondary navigation bar, click **Usage By Day**.
- From the Usage By Month report, click the name of a month to see the daily usage for that month.

The usage report appears. (Figure 7-6 shows an example Usage By Day usage report.)

Figure 7-6 Usage By Day Report



Date	Users	Revenue	Duration
2/27/2002	1	9.95 USD	0d 04h:06m:45s
2/28/2002	1	9.95 USD	0d 00h:04m:47s
3/1/2002	2	9.95 USD	0d 00h:08m:58s
3/13/2002	1	9.95 USD	0d 00h:09m:06s
3/14/2002	1	0.00 USD	0d 00h:00m:33s
3/16/2002	1	0.00 USD	1d 21h:56m:32s
3/21/2002	1	0.00 USD	0d 00h:00m:35s
3/25/2002	1	19.90 USD	0d 00h:02m:23s
3/26/2002	2	9.95 USD	0d 05h:22m:49s
3/27/2002	1	9.95 USD	0d 00h:00m:00s
3/28/2002	1	9.95 USD	0d 00h:00m:00s
3/29/2002	1	9.95 USD	0d 00h:00m:00s
3/30/2002	1	9.95 USD	0d 00h:00m:00s
3/31/2002	1	9.95 USD	0d 00h:00m:00s

Step 4 If desired, use the **Calendar Day Offset** to indicate the boundary of a day for reporting purposes. Typically, you set this to match the billing cycle of a hotel PMS system.

Step 5 To view the report, click **Get Usage Report**.

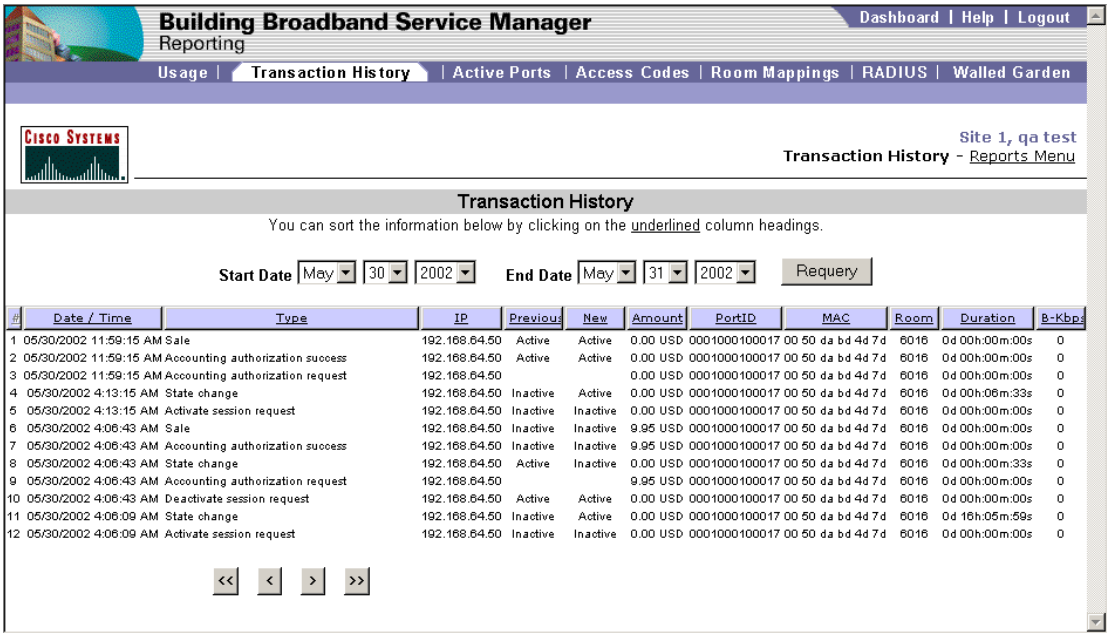
Transaction History Report

The Transaction History report lists one line per transaction showing the date/time, transaction type, IP address, previous status, new status, amount, port ID, MAC, room, duration, and bandwidth KBPS. shows an example of the report. Use the following procedure to view the report.

Step 1 From the BBSM Dashboard, click **Reporting Pages**. The Reporting splash screen appears, followed by the BBSM Reporting web page. (You can click the splash screen to skip it.)

Step 2 Click **Transaction History**. The Transaction History web page appears. (See Figure 7-7.)

Figure 7-7 Transaction History Report



Step 3 From the Start Date drop-down menu, select the desired start date for the report.

Step 4 From the End Date drop-down menu, select the desired end date for the report.

Step 5 Click **Requery** to view the results.

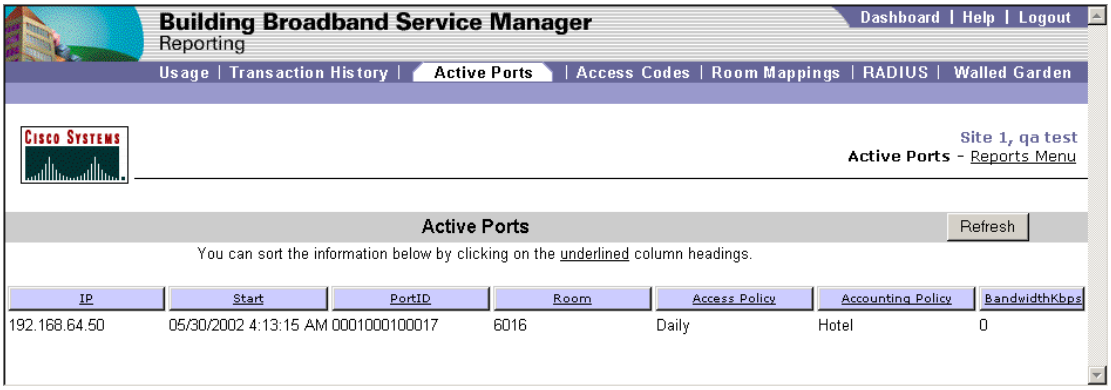
Active Ports Report

The Active Ports report shows the rooms that are connected to BBSM at the time the report is produced. Use the following procedure to view the Active Ports report.

Step 1 From the BBSM Dashboard, click **Reporting Pages**. The Reporting splash screen appears, followed by the BBSM Reporting web page. (You can click the splash screen to skip it.)

Step 2 Click **Active Ports**. The Active Ports web page appears. (See Figure 7-8.)

Figure 7-8 Active Ports Reports



Step 3 Click a column heading to sort the data in ascending or descending order.

Access Code Reports

Access Code reports list current, unused, and expired access codes. The following are the three access code report options:

- Access Code Report
- Unused Code Report
- Access Code History

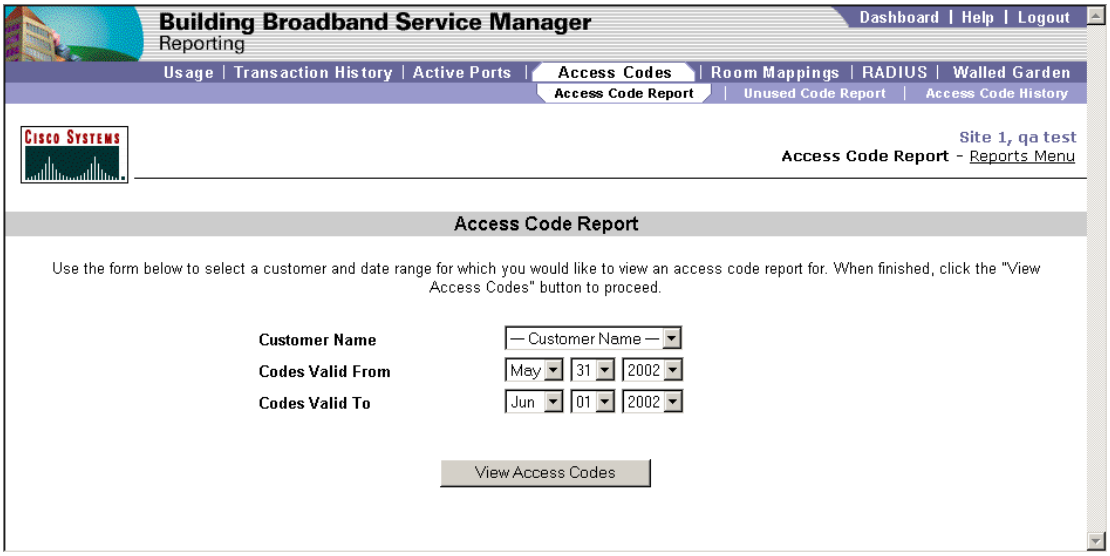
Access Code Report

The Access Code report shows the current access codes assigned to a customer. Use the following procedure to view the Access Code report.

Step 1 From the BBSM Dashboard, click **Reporting Pages**. The Reporting splash screen appears, followed by the BBSM Reporting web page. (You can click the splash screen to skip it.)

Step 2 Click **Access Codes**. The Access Code Report web page appears. (See Figure 7-9.)

Figure 7-9 Access Code Report Web Page



Step 3 From the Customer Name drop-down menu, select the desired Customer Name.

Step 4 From the Codes Valid From drop-down menu, select the desired date.

Step 5 From the Codes Valid To drop-down menu, select the desired date.

Step 6 To view the report, click **View Access Codes**.

Unused Code Report

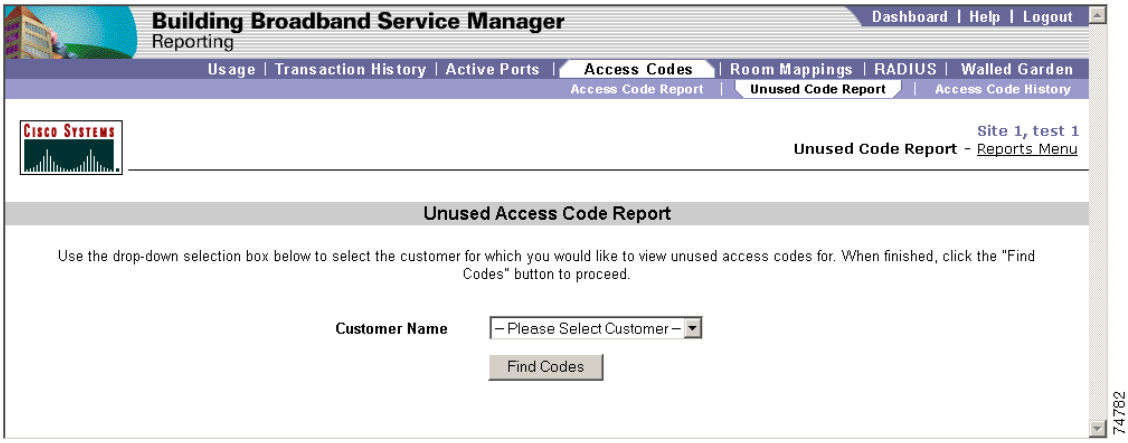
The Unused Code Report shows the unused access codes assigned to a customer. Use the following procedure to view the Unused Code report.

Step 1 From the BBSM Dashboard, click **Reporting Pages**. The Reporting splash screen appears, followed by the BBSM Reporting web page. (You can click the splash screen to skip it.)

Step 2 Click **Access Codes**. The Access Code Report web page appears. (See Figure 7-9.)

Step 3 Click **Unused Code Report**. The Unused Code Report appears. (See Figure 7-10.)

Figure 7-10 Unused Access Code Report Web Page



Step 4 From the Select Customer Name drop-down menu, select the desired customer.

Step 5 To view the report, click **Find Codes**.

Access Code History Report

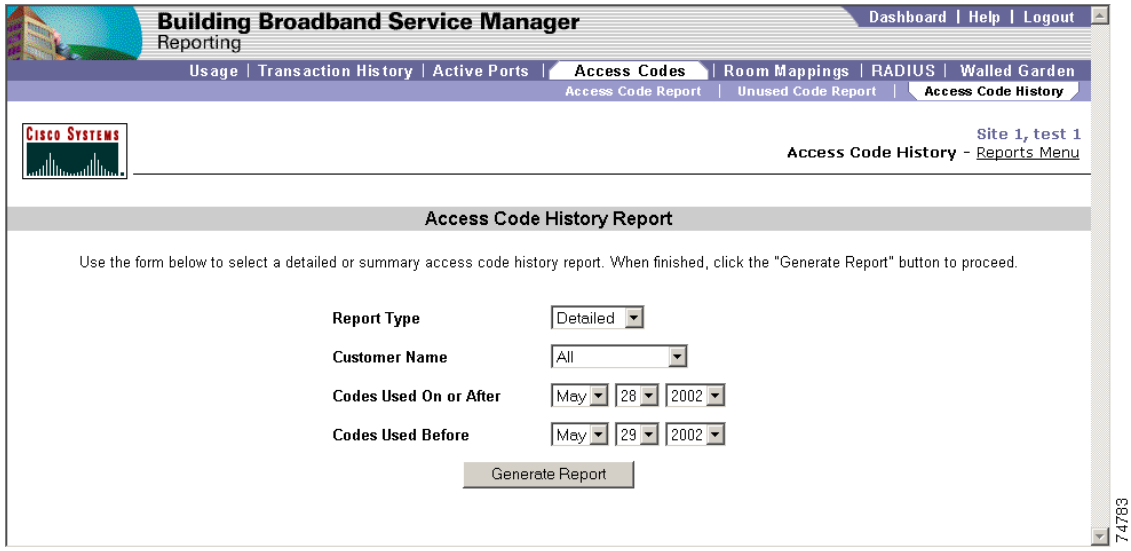
The Access Code History report shows the access codes that have expired. Use the following procedure to view the report.

Step 1 From the BBSM Dashboard, click **Reporting Pages**. The Reporting splash screen appears, followed by the BBSM Reporting web page. (You can click the splash screen to skip it.)

Step 2 Click **Access Codes**. The Access Code Report web page appears. (See Figure 7-9.)

Step 3 Click **Access Code History**. The Access Code History web page appears. (See Figure 7-11.)

Figure 7-11 Access Code History Report Web Page



Step 4 From the Report Type drop-down menu, select the desired report type: **Detailed** or **Summary**.

Step 5 From the Customer Name drop-down menu, select the desired customer name.

Step 6 From the **Codes Used On or After** drop-down menu, select the start date.

Step 7 From the **Codes Used Before** drop-down menu, select the desired end date.

Step 8 To view the report, click **Generate Report**.

Room Mappings Report

The Room Mappings report lists room numbers with their corresponding port numbers and port configuration information. There are two options available from the secondary navigation bar:

- View List—Shows a complete list of mappings
- Edit Record—Allows you to change a selected record

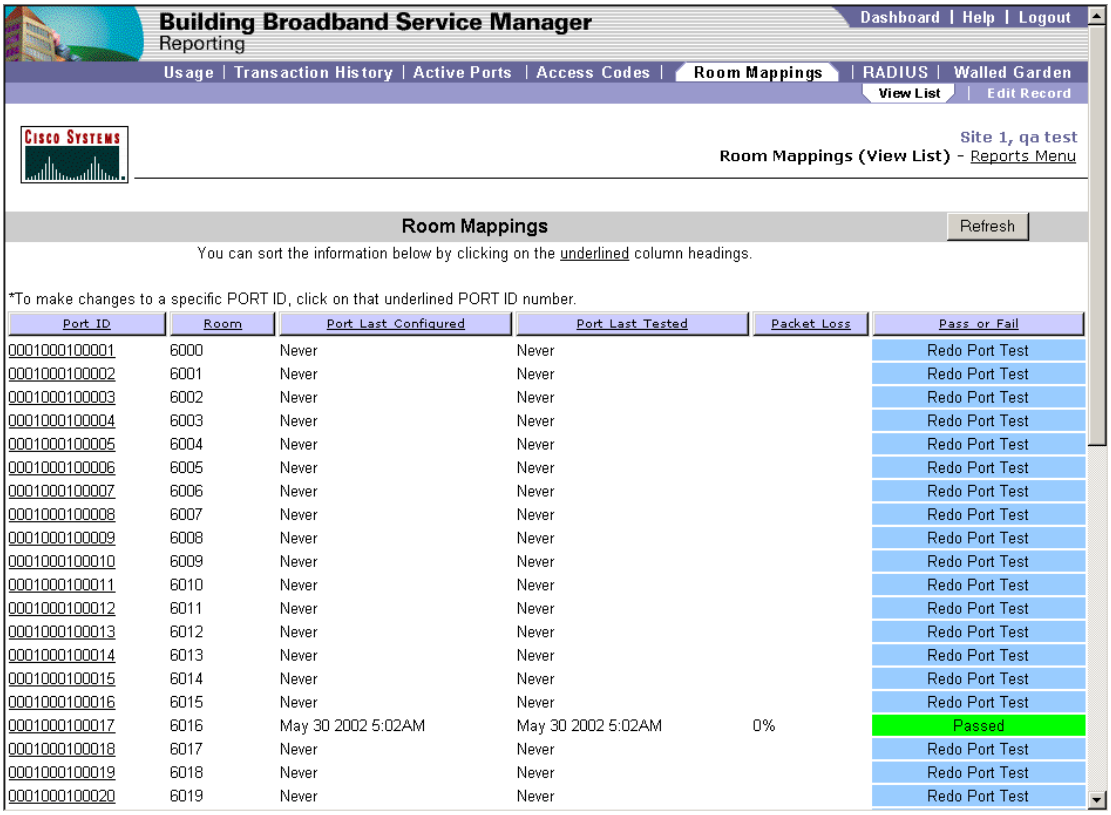
Room Mappings View List

The View List option lists the room numbers and their associated port IDs. Use the following procedure to view the Room Mappings report.

Step 1 From the BBSM Dashboard, click **Reporting Pages**. The Reporting splash screen appears, followed by the BBSM Reporting web page. (You can click the splash screen to skip it.)

Step 2 Click **Room Mappings**. The View List of the Room Mappings report web page appears. (See Figure 7-12.)

Figure 7-12 Room Mappings Report



Port ID	Room	Port Last Configured	Port Last Tested	Packet Loss	Pass or Fail
0001000100001	6000	Never	Never		Redo Port Test
0001000100002	6001	Never	Never		Redo Port Test
0001000100003	6002	Never	Never		Redo Port Test
0001000100004	6003	Never	Never		Redo Port Test
0001000100005	6004	Never	Never		Redo Port Test
0001000100006	6005	Never	Never		Redo Port Test
0001000100007	6006	Never	Never		Redo Port Test
0001000100008	6007	Never	Never		Redo Port Test
0001000100009	6008	Never	Never		Redo Port Test
0001000100010	6009	Never	Never		Redo Port Test
0001000100011	6010	Never	Never		Redo Port Test
0001000100012	6011	Never	Never		Redo Port Test
0001000100013	6012	Never	Never		Redo Port Test
0001000100014	6013	Never	Never		Redo Port Test
0001000100015	6014	Never	Never		Redo Port Test
0001000100016	6015	Never	Never		Redo Port Test
0001000100017	6016	May 30 2002 5:02AM	May 30 2002 5:02AM	0%	Passed
0001000100018	6017	Never	Never		Redo Port Test
0001000100019	6018	Never	Never		Redo Port Test
0001000100020	6019	Never	Never		Redo Port Test

Step 3 To sort the data in ascending or descending order, click a column heading.

Room Mappings Edit Record

The Room Mappings Input Form allows you to edit data for an individual entry on the Room Mapping list. Note that administrator or operator privileges are required to view and use this form. Use the following procedure to edit the Room Mappings Input Form.

Step 1 From the BBSM Dashboard, click **Reporting Pages**. The Reporting splash screen appears, followed by the BBSM Reporting web page. (You can click the splash screen to skip it.)

Step 2 Click **Room Mappings**. The View List of the Room Mappings report web page appears. (See Figure 7-12.)

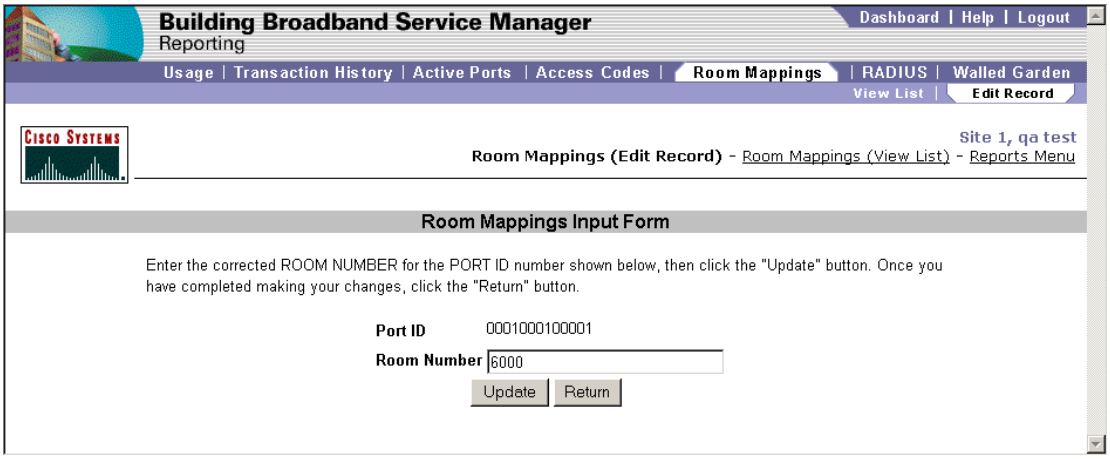
Step 3 From the Room column, select a room number.

Step 4 Do one of the following.

- From the secondary navigation bar, click **Edit Record**.
- Select a **Port ID** entry.

The Room Mappings Input Form web page appears. (See Figure 7-13.)

Figure 7-13 Room Mappings Input Form



Step 5 Enter changes as necessary.

Step 6 To save the changes, click **Update**.

Step 7 To return to the View List of the Room Mappings report, click **Return**.

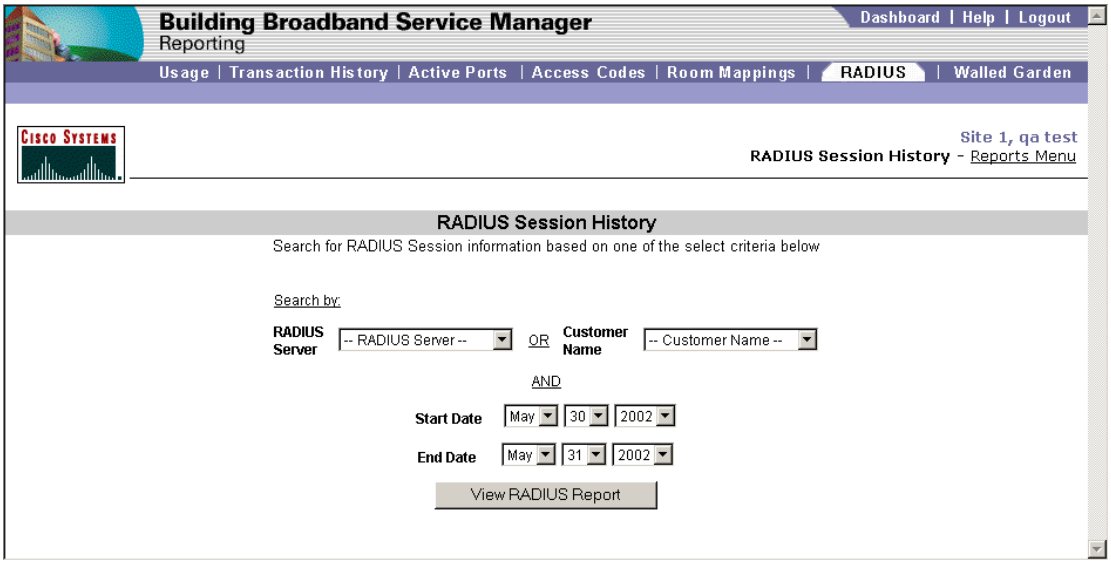
RADIUS Report

The RADIUS report provides a history of all RADIUS sessions based on either a particular RADIUS server or user. Use the following procedure to view the report.

Step 1 From the BBSM Dashboard, click **Reporting Pages**. The Reporting web page appears.

Step 2 Click **RADIUS**. The RADIUS Session History web page appears. (See Figure 7-14.)

Figure 7-14 RADIUS Session History Options Web Page



Step 3 From one of the following drop-down menus, select the desired search criteria:

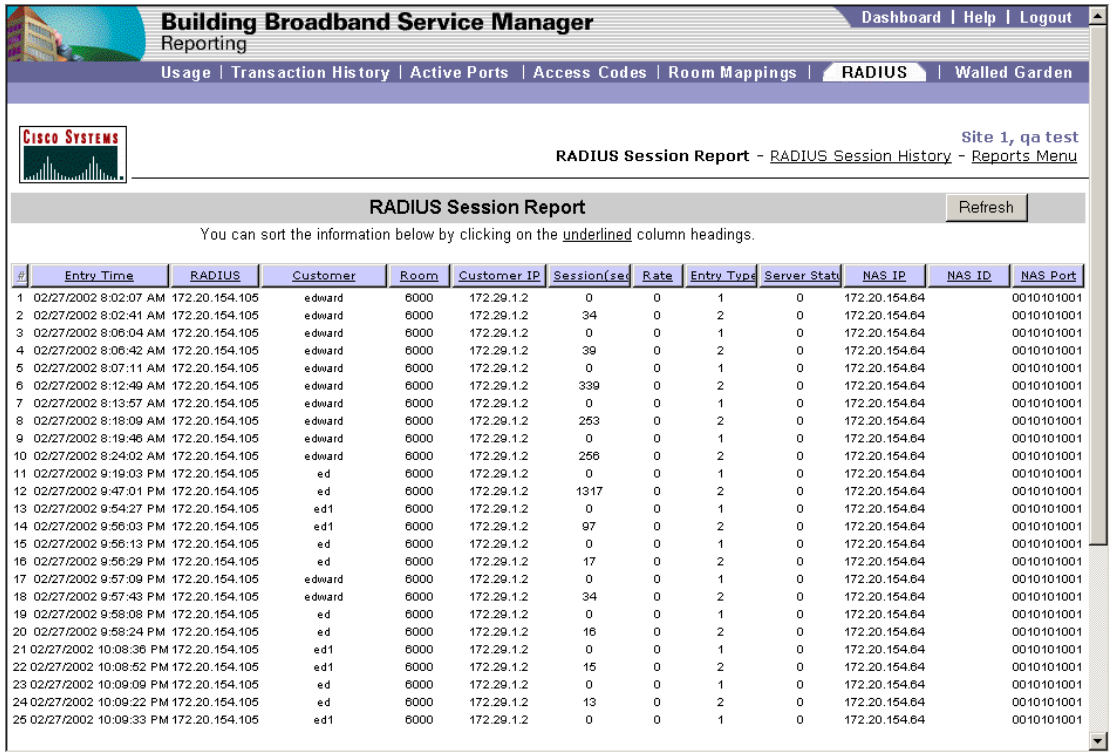
- RADIUS Server
- Customer Name

Step 4 From the Start Date drop-down menu, select the desired report start date.

Step 5 From the End Date drop-down menu, select the desired report end date.

Step 6 Click **View RADIUS Report**. The RADIUS Session report appears. (See Figure 7-15.)

Figure 7-15 RADIUS Session History Report



#	Entry Time	RADIUS	Customer	Room	Customer IP	Session(sec	Rate	Entry Type	Server Statu	NAS IP	NAS ID	NAS Port
1	02/27/2002 8:02:07 AM	172.20.154.105	edward	6000	172.29.1.2	0	0	1	0	172.20.154.64		0010101001
2	02/27/2002 8:02:41 AM	172.20.154.105	edward	6000	172.29.1.2	34	0	2	0	172.20.154.64		0010101001
3	02/27/2002 8:06:04 AM	172.20.154.105	edward	6000	172.29.1.2	0	0	1	0	172.20.154.64		0010101001
4	02/27/2002 8:06:42 AM	172.20.154.105	edward	6000	172.29.1.2	39	0	2	0	172.20.154.64		0010101001
5	02/27/2002 8:07:11 AM	172.20.154.105	edward	6000	172.29.1.2	0	0	1	0	172.20.154.64		0010101001
6	02/27/2002 8:12:49 AM	172.20.154.105	edward	6000	172.29.1.2	339	0	2	0	172.20.154.64		0010101001
7	02/27/2002 8:13:57 AM	172.20.154.105	edward	6000	172.29.1.2	0	0	1	0	172.20.154.64		0010101001
8	02/27/2002 8:18:09 AM	172.20.154.105	edward	6000	172.29.1.2	253	0	2	0	172.20.154.64		0010101001
9	02/27/2002 8:19:46 AM	172.20.154.105	edward	6000	172.29.1.2	0	0	1	0	172.20.154.64		0010101001
10	02/27/2002 8:24:02 AM	172.20.154.105	edward	6000	172.29.1.2	256	0	2	0	172.20.154.64		0010101001
11	02/27/2002 9:19:03 PM	172.20.154.105	ed	6000	172.29.1.2	0	0	1	0	172.20.154.64		0010101001
12	02/27/2002 9:47:01 PM	172.20.154.105	ed	6000	172.29.1.2	1317	0	2	0	172.20.154.64		0010101001
13	02/27/2002 9:54:27 PM	172.20.154.105	ed1	6000	172.29.1.2	0	0	1	0	172.20.154.64		0010101001
14	02/27/2002 9:56:03 PM	172.20.154.105	ed1	6000	172.29.1.2	97	0	2	0	172.20.154.64		0010101001
15	02/27/2002 9:56:13 PM	172.20.154.105	ed	6000	172.29.1.2	0	0	1	0	172.20.154.64		0010101001
16	02/27/2002 9:56:29 PM	172.20.154.105	ed	6000	172.29.1.2	17	0	2	0	172.20.154.64		0010101001
17	02/27/2002 9:57:09 PM	172.20.154.105	edward	6000	172.29.1.2	0	0	1	0	172.20.154.64		0010101001
18	02/27/2002 9:57:43 PM	172.20.154.105	edward	6000	172.29.1.2	34	0	2	0	172.20.154.64		0010101001
19	02/27/2002 9:58:08 PM	172.20.154.105	ed	6000	172.29.1.2	0	0	1	0	172.20.154.64		0010101001
20	02/27/2002 9:58:24 PM	172.20.154.105	ed	6000	172.29.1.2	16	0	2	0	172.20.154.64		0010101001
21	02/27/2002 10:08:36 PM	172.20.154.105	ed1	6000	172.29.1.2	0	0	1	0	172.20.154.64		0010101001
22	02/27/2002 10:08:52 PM	172.20.154.105	ed1	6000	172.29.1.2	15	0	2	0	172.20.154.64		0010101001
23	02/27/2002 10:09:09 PM	172.20.154.105	ed	6000	172.29.1.2	0	0	1	0	172.20.154.64		0010101001
24	02/27/2002 10:09:22 PM	172.20.154.105	ed	6000	172.29.1.2	13	0	2	0	172.20.154.64		0010101001
25	02/27/2002 10:09:33 PM	172.20.154.105	ed1	6000	172.29.1.2	0	0	1	0	172.20.154.64		0010101001

Walled Garden Report

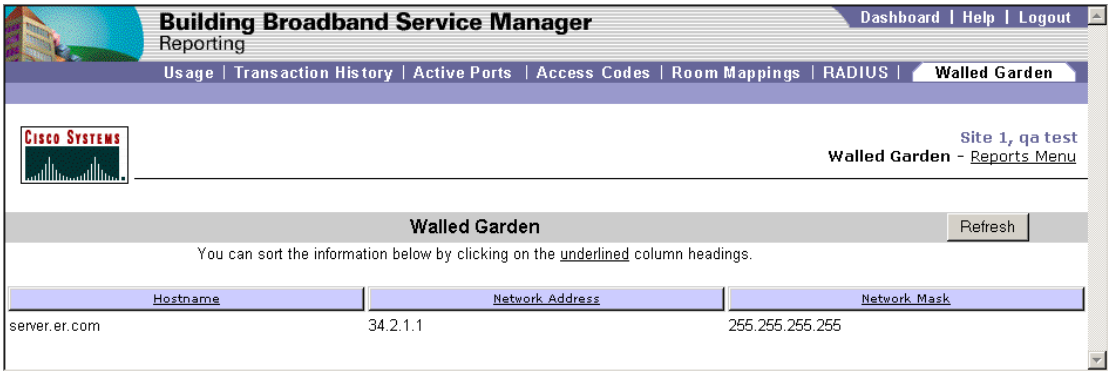
The Walled Garden report displays all of the current walled garden configurations that you created using the Walled Garden web page of WEBconfig. Figure 7-16 shows an example of the report.

Use the following procedure to view the Walled Garden report.

Step 1 From the BBSM Dashboard, click **Reporting Pages**. The Reporting splash screen appears, followed by the BBSM Reporting web page. (You can click the splash screen to skip it.)

Step 2 Click **Walled Garden**. The Walled Garden report web page appears. (See Figure 7-1.)

Figure 7-16 Walled Garden Report



Step 3 To sort the data in ascending or descending order, click a column heading.

Customizing Your BBSM System

Once your BBSM server has been set up and configured, you may want to configure additional parameters or customize your system. This chapter guides you to this information.

Customizing Page Sets

For complete information and instructions on customizing or creating page sets, refer to the *Cisco BBSM SDK Developer Guide.* In the Preface to this document, see the Obtaining Documentation section.

Using Walled Gardens

BBSM allows service operators to define various free access links to specific web sites. This functionality is known as Walled Gardens.

A Walled Garden offers the end-user valuable services and also generates incremental revenue or reduces costs for the operator. As an added dimension, the Walled Garden can be targeted using BBSM's location-based policies to present different links to users in different physical locations, such as the club floor of a hotel. The following are typical Walled Garden links:

- Local weather and attractions
- Online concierge services
- Online room service
- Hotel chain corporate or loyalty program portal

To add walled garden links to your start page, contact your web developer.

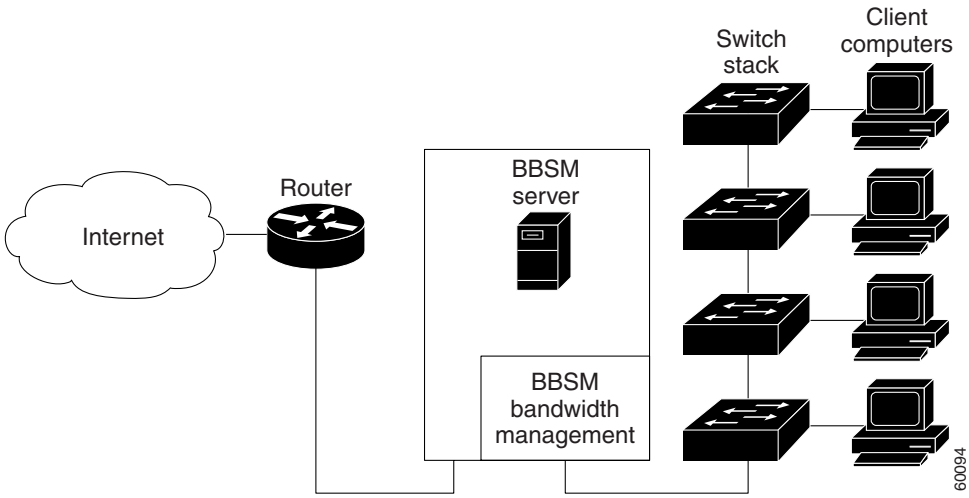
Managing Bandwidth

BBSM Bandwidth Management allows the administrator of the BBSM server to control the bandwidth allocated to end users.

Configuring the BBSM Server

This section explains how to configure and use the BBSM Bandwidth Management feature. Figure 8-1 shows BBSM Bandwidth Management on the BBSM server.

Figure 8-1 BBSM Bandwidth Management Installed on the BBSM Server



BBSM bandwidth management is located on the internal interface of the BBSM server. Because all packets pass through the internal interface, the BBSM Bandwidth Management feature can be used with any network topology.

Follow these steps to activate the Bandwidth Manager feature.

Step 1 From the BBSM Dashboard, select **WEBconfig**. The Port IP Addresses web page appears.

Step 2 Click the **Server** button.

Step 3 Check **Bandwidth Manager**.

Step 4 Click **Update**.

Step 5 Closes WEBconfig.

Tuning Bandwidth Manager through Optional Advanced Settings

If you are accepting the default settings for the parameters listed in the following table, you do not need to do anything more. However, if necessary, you can fine-tune BBSM Bandwidth Manager by changing parameter settings in the Windows 2000 registry on BBSM.

The parameters listed below can be adjusted. These parameters should be sized based on the peak number of users expected on the BBSM server. If this maximum is occasionally exceeded, performance is impacted but BBSM continues to operate correctly.

Table 8-1 BBSM Bandwidth Management Configurable Parameters

Parameter	Description
BWTQueueSize	Amount of data per link to queue before discarding. The default should be adequate for TCP clients. For UDP clients (streaming audio or video), the client must select a transmission rate below the bandwidth limit to avoid losing packets due to queue overflow. Default: 151,400 bytes
PacketPoolSize	Number of packet descriptors. See **LookaheadPoolSize**. Default: 50 descriptors
LookaheadPoolSize	Number of look-ahead buffer descriptors (indicated by the packet descriptor). Set PacketPoolSize and LookaheadPoolSize greater than the anticipated maximum number of packets queued for bandwidth management. • For TCP clients, this number is the TCP window divided by the packet size. • For UDP clients, this number is the BTWQueueSize divided by the packet size. Calculate both and select the larger of the two values. TCP Example: An Ethernet interface has a maximum packet size of 1514 bytes and a typical Windows TCP client uses a window of 8192 bytes. Divide the window size (8192 bytes) by the packet size (1514 bytes) to allocate 6 packets per TCP client. UDP Example: Assume BWTQueueSize is 15140kb. Since the Ethernet packet size is 1514 bytes, divide the BWTQueueSize (15140) by 1514 bytes to establish 10 packets per client. Since 10 is greater than 6, 10 packets per client would be used. Default: 50 descriptors

Editing Parameters in the Windows 2000 Registry

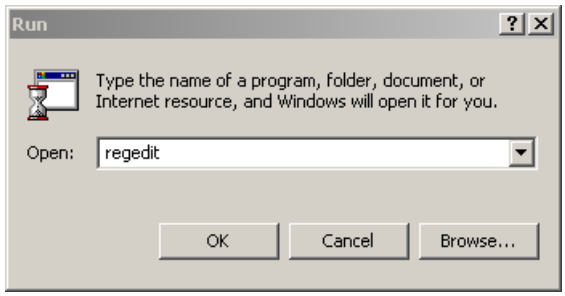
To change a parameter value, you must edit the AtNat parameters in the Windows 2000 registry. If you are accepting the default values, you do not need to edit the registry. Note that you can only make these changes locally, not from a remote server.

Caution Incorrect registry settings can render your BBSM server unusable. Alter only the parameters listed in Table 8-1 on page 8-3. Always backup the registry before making any changes.

The following procedure gives an example of how to change the registry to optimize Bandwidth Manager.

Step 1 Choose **Start > Run**. The Run window appears. (See Figure 8-2.)

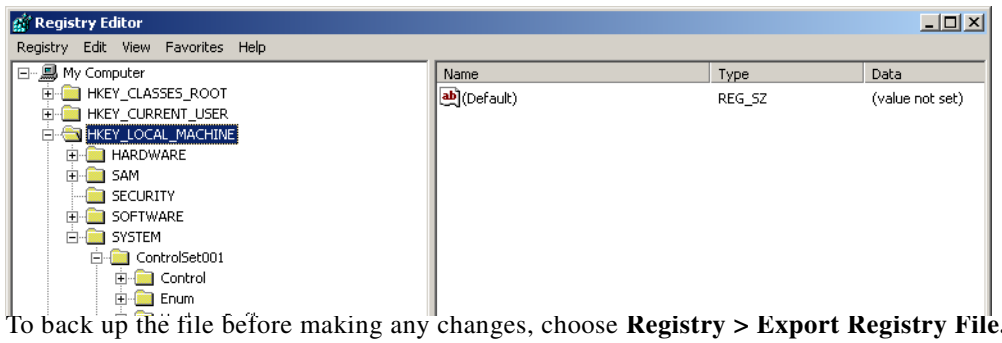
Figure 8-2 Run Window



Step 2 Enter **regedit**.

Step 3 Click **OK**. The Registry Editor window appears. (See Figure 8-3.)

Figure 8-3 Registry Editor Window



Step 4 To back up the file before making any changes, choose **Registry > Export Registry File.**

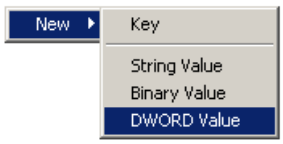
Step 5 Double-click **HKEY_LOCAL_MACHINE**.

Step 6 Navigate to **System > CurrentControlSet > Services > ATNAT > Parameters.**

Step 7 Right-click anywhere in the right pane of the Registry Editor window.

Step 8 From the New > drop-down menu, select **DWORD Value**. (See Figure 8-4.)

Figure 8-4 Registry Editor New Drop-Down Menu



Step 9 Rename the entry to the parameter name you want to change. For applicable parameter names, see Table 8-1 on page 8-3.

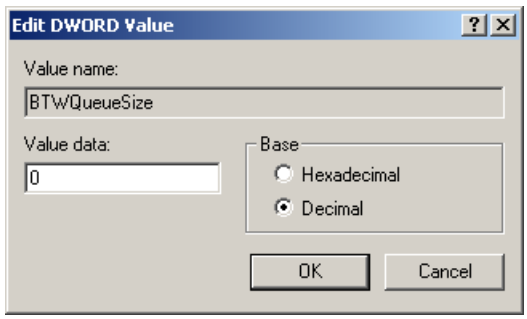
Step 10 Double-click the new parameter name. (See Figure 8-5. Note that BTWQueueSize is shown here only as an example.)

Figure 8-5 New Parameter Name

Name	Type	Data
(Default)	REG_SZ	(value not set)
ClientPage	REG_SZ	/ekgnkm/
ComputerName	REG_SZ	10.10.2.1
ConnectPage	REG_SZ	/ekgnkm/preconnect.asp
DebugLevel	REG_DWORD	0x00000000 (0)
DebugMask	REG_DWORD	0x00000000 (0)
DNSProxy	REG_DWORD	0x0a0a0201 (168428033)
EnableTransparentProxy	REG_DWORD	0x00000000 (0)
LocalMappedAddressEnd	REG_DWORD	0x0a0a02fe (168428286)
LocalMappedAddressStart	REG_DWORD	0x0a0a02ab (168428203)
PipServer	REG_DWORD	0x0a0a0102 (168427778)
SMTPServer	REG_DWORD	0x00000000 (0)
WebServer	REG_DWORD	0x0a0a0201 (168428033)
WebServerPort	REG_DWORD	0x00000050 (80)
BTWQueueSize	REG_DWORD	0x00000000 (0)

The **Edit DWORD Value** dialog box appears. (See Figure 8-6.)

Figure 8-6 Edit DWORD Value Dialog Box



Step 11 Click **Decimal.**

Step 12 In the Value data field, enter the new value in the appropriate units for that parameter name**.** See Table 8-1 on page 8-3 for a list of parameters.

Step 13 Click **OK.**

Step 14 To make other changes or additions, do one of the following.

- If you want to add another parameter, repeat Steps 7 through 13 for each new parameter.
- If you want to change other parameters, repeat Steps 10 through 13 for each parameter.

Step 15 When done, close the Registry Editor window.

Step 16 Select **Start > Shut Down > Restart.**

Web Printing

This chapter describes how to install network printers and configure the BBSM Web Printing utility. You must purchase and install the KeyView Pro software to support this feature. KeyView Pro is sold separately by most software vendors.

Caution BBSM supports a limited set of local printers and network printers. BBSM Version 5.1 also supports the HP JetDirect print server for network printers.

The normal order for installing and configuring the components for Web Printing is as follows:

1. Install KeyView Pro 6.5. (See the "Installing KeyView Pro 6.5 for Web Printing" section on page 2-15.)
2. By using WEBconfig, configure BBSM Web Printing.
3. Install or configure the default printer for each site.

Configuring BBSM Web Printing

Use the following steps to configure BBSM for web printing for each site and printer. (Note that the BBSM server must be properly configured before Web Printing can be configured.)

Step 1 From the BBSM Dashboard, click **WEBconfig**. The BBSM Port IP Addresses web page appears.

Step 2 Click the **Sites** button. The BBSM Sites web page appears.

Step 3 Note that if the Printing fields are grayed out, Key View Pro has not been installed, and you cannot configure web printing. (See Figure 3-4 on page 3-8.)

Step 4 Use the navigation buttons to select the site you want to configure for web printing.

Step 5 In the Printing section, enter the desired information for each site, as shown below:

a. In the BBSM Printer text box, enter the name of the BBSM printer you have assigned to the site.

Caution Note that this printer name must match *exactly* the default printer name as it is defined in the Printers folder for web printing to work.

b. Select the type of printer: **Network Printer** or **Local Printer**.

c. In the **Price Per Page** text box, enter the decimal number for the price of printing each page, such as **.10** for 10 cents. If printing is free, leave this text box blank or enter **0**.

d. In the **Max Price Per Job** text box, enter the decimal number for the maximum price per job. For example, enter **10.00** if the maximum price for a job is $10. If printing is free, leave this text box blank or enter **0**.

e. In the Printer Account User ID field, enter the account user ID.

f. In the Printer Account Password field, enter the account password.

g. In the Please Confirm Password field, re-enter the password.

Note For network printers, the user ID and the password must be valid for the server that has the printer connected to it. The printer account user ID should be different for each site.

Step 6 Click **Update**.

Step 7 When you have configured all sites and printers, click **OK** to close WEBconfig.

Step 8 Close the Printers window if it is open.

Adding a Custom Logo for Printing

You can install a custom logo that users will see when they activate the BBSM Web Printing utility. Use the following procedure to add a custom logo.

Step 1 Create your customized logo. Note that BBSM Web Printing GUI pages are designed to work with a GIF file that has the following attributes:

- 199 x 66 pixels
- 256 colors (indexed)
- White background

Step 2 Name the logo file, as follows: **hotel_logo.gif**.

Step 3 Copy the file to this folder: c:\atcom\Print

Installing Printers

As described previously, within the BBSM system, you can set up a printer for each site or you can associate a printer with more than one site. The two sections that follow describe how to install a printer. The first gives you a general procedure for installing a printer, and the second gives an example.

Most printers come with printer driver software that can install the printer for you automatically. Use these software instructions from the vendor to install either a local printer (plugged directly into the BBSM server) or a network printer. When you have installed the printer, set it to be the default printer.

Basic Printer Installation

If the printer cannot be automatically installed, use the procedure below as a general guide to installing the local printer.

Caution Before you start any printer installation, log on to BBSM with the printer account.

Step 1 Connect the printer to the USB port on the BBSM server and turn the printer on.

Step 2 Choose **Start > Settings > Printers** > **Add Printer**.

Step 3 To clear the Welcome screen, click **Next**.

Step 4 Select **Local printer** and click **Next**.

Step 5 In the Available ports dialog box, check the printer port connection (USB port) and click **Next**.

Step 6 At the manufacturer and printer model dialog, do one of the following:

- Select the manufacturer and printer model from the lists provided by Windows, and click **Next**.
- Click **Have Disk** and follow the instructions provided with your printer driver to select it. If you get a message that the driver is already installed, select **Keep existing driver**, and click **Next**.

Step 7 In the Printer name text box, enter a unique name for the printer.

Step 8 To set this printer as the printer, click **Yes** for the Default printer attribute.

Step 9 Do one of the following:

- For a printer connected directly to the BBSM server, select **Do not share this printer**, and then click **Next**.
- For a printer connected to another network computer, select **Share as** and enter a unique share name, and then click **Next**.

Step 10 Verify that **Yes** is checked to print a test page, and then click **Finish**. The printer appears in the Printers window. Confirm that this printer is the default printer.

Caution Note that, for each site that has Web Printing enabled, the name entered in the BBSM Printer field on the Sites page in WEBconfig must match *exactly* the default printer name as it is defined in the Printers folder for web printing to work.

Step 11 If you get a **Files Needed** prompt, insert the required disk(s) and click **OK**.

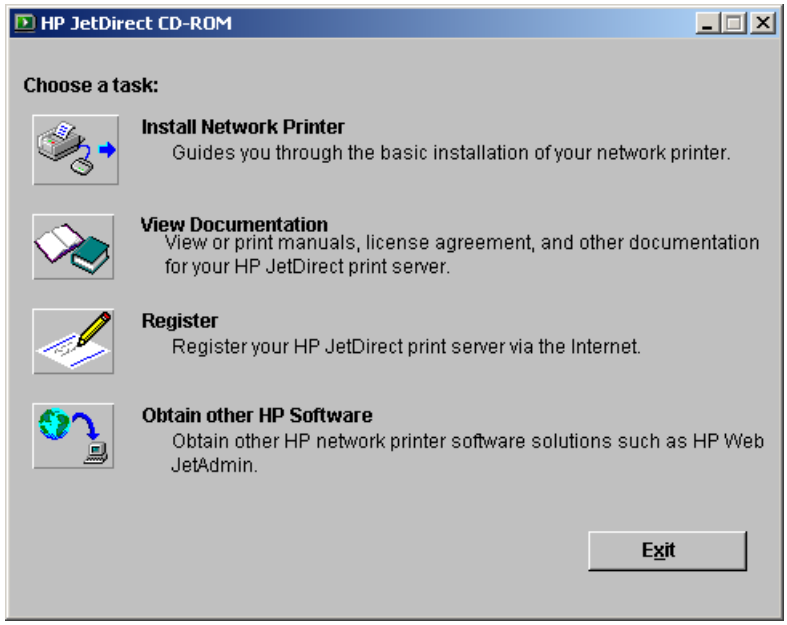
Step 12 If asked to reboot, click **OK** and reboot the server.

Example Printer Installation

The following is an example of how to install a HP LaserJet 5 network printer using the HP JetDirect Print Server.

Step 1 Insert HP JetDirect Print Server CD. If setup.exe does not launch automatically, choose **Start > Run** to launch it. The HP JetDirect CD-ROM dialog box appears. (See Figure 9-1.)

Figure 9-1 HP JetDirect Opening Dialog Box

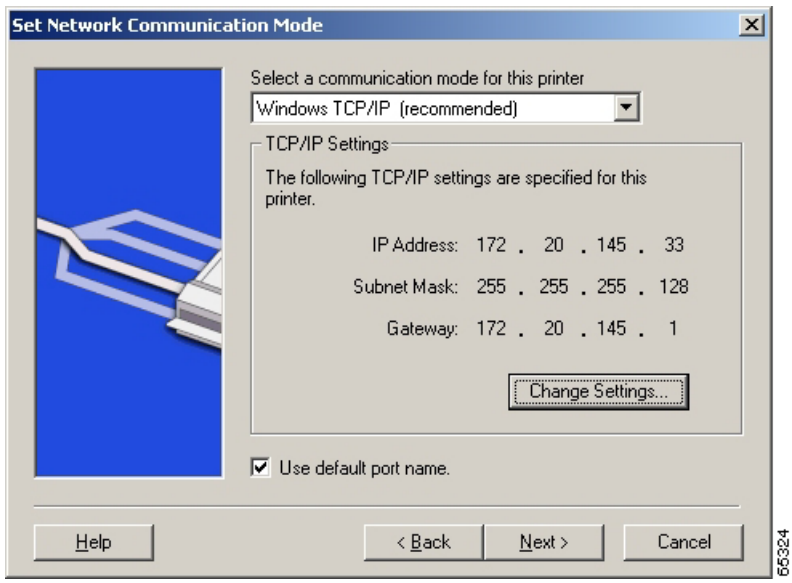


Step 2 Click **Install Network Printer** icon. The Welcome dialog box appears.

Step 3 Click **Search from a list of available printers** and click **Next.** When the search has finished, the Identify Printer dialog box appears.

Step 4 Select the appropriate printer. Click **Next**. The Set Network Communication Mode dialog box appears. (See Figure 9-2.)

Figure 9-2 Set Network Communication Mode Dialog Box



Step 5 Verify that the settings are correct. If necessary, click **Change Settings** and make the necessary changes.

Step 6 When the settings are correct, click **Next**. The Printer Drivers dialog box appears.

Step 7 From the Printer Drivers dialog box, select the appropriate printer and click **Next**. The Printer Name dialog box appears.

Step 8 Enter the name for your printer and click **Next**. The Printer Sharing dialog box appears.

Step 9 Do one of the following:

- For a printer connected directly to the BBSM server, select **Do not share this printer**, and then click **Next**.
- For a shared printer connected to another computer on the network, select **Share as** and enter a unique share name, and click **Next**.

4. Leave the "Print a test page" box checked and click **Finish**.

Note Always print a test page to make sure that printer installed correctly.

Refer to your printer's documentation if you have any problems installing the printer.

Using BBSM Web Printing to Print a File

Files cannot be printed directly from an application. To use this utility, save the document to be printed and close it. Then, use the Web Printing steps below to print the file.

Note You must close the file you intend to print before using Web Printing.

Step 1 Open the browser if it is not already open. Click **Connect**.

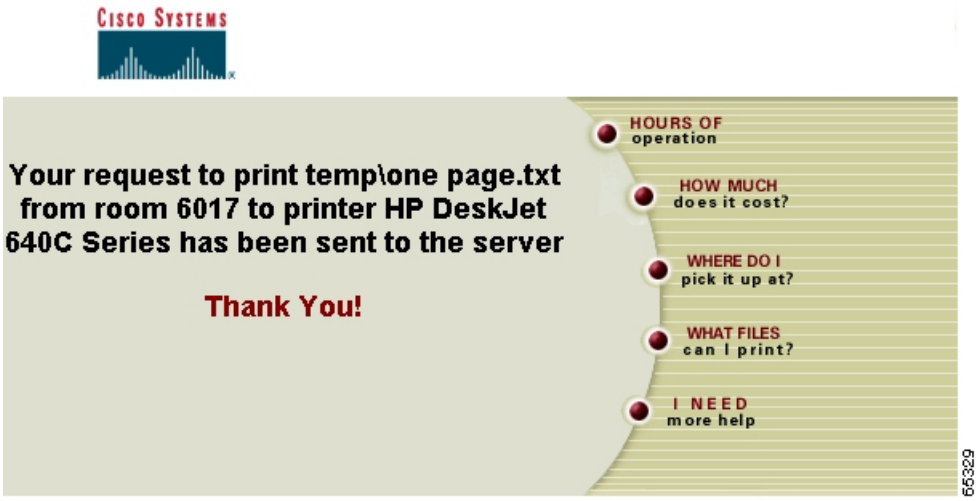
Step 2 In the separate BBSM window, click **Print**. The BBSM Web Printing page appears. (See Figure 9-3.)

Figure 9-3 BBSM Web Printing Page

Step 3 Click **Browse...** to navigate to the file to be printed or type the path and file name in the text box.

Step 4 Click **Print File**. A confirmation web page appears when the file has been sent to the Web Printing service. (See Figure 9-4.)

Figure 9-4 Print Confirmation Web Page



Supported Web Printing File Types

You can use BBSM Web Printing to print the file types described in the following tables. (See 9-1 through 9-7.)

Table 9-1 Web Printing Supported Document File Types

File Type	Version
ASCII and ANSI	All
Applix Words	4.2, 4.3, 4.4
Executables	NA
HTML	1.*x*, 2.*x*, 3.*x*
IBM DCA/RFT Displaywrite	 SC23-0758-1 4, 5
Lotus AMI Pro AMI Professional Write Plus Word Pro	 2, 3 NA 96, 97, R9
Maker Interchange Format (MIF)	5.5
Microsoft RTF Word Works Windows Write	 NA For PC: 2–5.5 For Windows: 2.*x*, 6.0, 95, 97, 2000 For Macintosh: 4–6, 98 1.0, 2.0, 3.0, 4.0 1.0, 2.0, 3.0
Unicode Text	NA
WordPerfect	Windows: Versions 5.*x*, 6–8 Macintosh: 2, 3
XyWrite	4.12

Table 9-2 Web Printing Supported Double-Byte File Types

File Type	Version
Lotus[1] Word Pro 1-2-3[1] Freelance[1]	 96, 97, R9 96, 97, R9 96, 97, R9
Microsoft[2]	6, 95, 97, 2000
Excel[2]	6, 95, 97, 2000
PowerPoint[2]	6, 95, 97, 2000

1. Japanese, Korean, Simplified and Traditional Chinese
2. Japanese

Table 9-3 Web Printing Supported Double-Byte File Types

File Type	Version
Lotus[1]	
Word Pro	96, 97, R9
1-2-3[1]	96, 97, R9
Freelance[1]	96, 97, R9
Microsoft[2]	6, 95, 97, 2000
Excel[2]	6, 95, 97, 2000
PowerPoint[2]	6, 95, 97, 2000

1. Japanese, Korean, Simplified and Traditional Chinese
2. Japanese

Table 9-4 Web Printing Supported Spreadsheet File Types

File Type	Version
Lotus[1]	
Word Pro	96, 97, R9
1-2-3[1]	96, 97, R9
Freelance[1]	96, 97, R9
Microsoft[2]	6, 95, 97, 2000
Excel[2]	6, 95, 97, 2000
PowerPoint[2]	6, 95, 97, 2000

1. Japanese, Korean, Simplified and Traditional Chinese
2. Japanese

Table 9-5 Web Printing Supported Presentation File Types

File Type	Version
Applix Presents	4.3, 4.4
Corel Presentations	7.0, 8.0
Lotus Freelance	96, 97, R9
PowerPoint[2]	6, 95, 97, 2000
Microsoft PowerPoint	For Windows: v4.0, 95, 97, 2000 For Macintosh: 98

Table 9-6 Web Printing Support Graphics File Types

File Type	Version
AMI Draw Graphics	(SDW)
Applix Graphics	4.3, 4.4
Fax Systems (CCITT)	Groups 3 & 4
Computer Graphics Metafile (CGM)	NA
Corel Draw CDR (TIFF Header)	NA
Encapsulated PostScript (EPS)	NA
Enhanced Metafile (EMF)	NA
JPEG File Interchange Format	NA
Lotus Pic (PIC)	NA
Mac PICT (raster content)	NA
MacPaint (MAC)	NA
Microsoft Excel Charts Windows Animated Cursor Windows Bitmap (BMP) Windows Cursor/Icon Sound (WAV) Windows Metafile (WMF)	NA
PC PaintBrush (PCX)	NA
Portable Network Graphics (PNG)	NA
Sun Raster	NA
SGI RGB	NA
Truevision Targa	NA
WordPerfect Graphics (WPG)	1, 2
Multimedia Formats	NA
Audio Interchange File Format (AIFF)	NA
MIDI (MID)	NA
MPEG 1 Video (MPG)	NA
NeXT/Sun Audio (AU)	NA
QuickTime Movie (MOV)	NA
Video for Windows (AVI)	NA

Table 9-7 Web Printing Supported Compression, Encapsulation, Fax, and Security File Types

File Type	Version
Fax (DCX)	NA
GZ-compression	NA
Z-compression	NA
ZipFax Systems (CCITT)	NA
BinHex	NA
MIME	NA
TAR	NA
UUencode	NA

Converting to a File Type Supported by BBSM Web Printing

If you are trying to print a file that has a nonsupported file type, use this procedure to convert the file type to one that is supported.

Step 1 Open the file as you normally would.

Step 2 Choose **File > Save As**.

Step 3 From the Save As Type (or similarly named) drop-down menu, choose a format that BBSM Web Printing supports from the tables in "Supported Web Printing File Types" section on page 9-6.

Step 4 Verify that the file name now shows the proper new extension for the new file type.

Step 5 Click **Save**. BBSM Web Printing may still not be able to print the file properly. In this case, assure the end user that they will not charged.

Printer Error Messages

Printer error messages are generated only when you are using printers that return error messages. Check the printer documentation to determine if your printer supports this feature. Note that printing can be time-consuming. For this reason, if users are printing a large file and want to print multiple copies, please have them wait a minute or two after the each job finishes.

If you are having trouble printing from BBSM Web Printing, error messages are placed in the Transaction History Report that can be accessed from the BBSM Reporting Pages option. (For more information, see the "Transaction History Report" section on page 7-6).

Table 9-8 Common Printer Error Messages

Message	Probable Cause and Recommendations
Printing Error	The is a general printing error message. It could be due to the printer's being out of paper, a paper jam, or the printer being offline. Check the printer. Usually when the problem is cleared up, the pages print out without the end user resending the file. If the problem persists, check the issues listed below to determine if one of them may be the problem.
ImpersonatingPrinterAcct Failed	You may not have logged on by using the printer account to install the printer. Log on as the printer account and reinstall the printer for the site setting to be the default printer.
Internet Explorer cannot open the Internet site http://server/ BBSMPrintResp.asp	The downloaded file is not available. This could be due to your security or language settings or because the server was unable to retrieve the requested file. **Tell the users this:** The end user probably tried to print while the file to be printed was open in another application. (In the error message, the word *server* is replaced by the name of the BBSM server to which users are connected.) **What the users should do:** The end user should exit the application, disconnect from the BBSM system, and close the browser. Then they can try printing from BBSM Web Printing again according to the printing procedure.
Network congestion error	**Tell the users this:** The system is busy processing requests. **What the users should do:** The end user should wait a minute or two and then try to print the document again.
SetDefaultPrinter Failed	The BBSM system cannot set the printer you assigned to the site as the default printer. The reason could be one of the following: • The printer name entered on the BBSM Sites web page in WEBconfig might be different from the printer name given when the printer was installed. Correct the name if necessary. • The printer account for the site is not in the administrator group for BBSM. Try going to the BBSM Sites page of WEBconfig, adding an extra letter to the printer name, and updating. Then change the printer name back to the original name and update again. This should add the printer account to the administrator group. If it does not, you must add it manually.
There is no printer installed	**Tell the users this:** The end user tried to print a file using the application's File > Print feature. Users cannot print files directly from an application unless they have connected a printer directly to their computers and installed the correct printer drivers. **What the users should do:** To print while using the BBSM Web Printing utility, users should exit their application and use the printing procedure. (Note that a technician might also see this message if the BBSM Web Printing was not installed correctly.)

Table 9-8 Common Printer Error Messages (continued)

Message	Probable Cause and Recommendations
Unsupported file type	**Tell the users this:** The end user tried to print a file that does not exist, or they tried to print a type of file that BBSM Web Printing does not support. (The user is not charged in either case.) • If the end user typed the name manually on the "Welcome to BBSM Web Printing" page, they should try printing again by using the Browse button to fill in the file name. • If a bad file name is not the problem, the user should be aware that some files are in a format that BBSM Web Printing cannot print or the files may contain macros or other information that BBSM Web Printing cannot interpret. **What the users should do:** The end user should try the following: • Convert the file to a format that BBSM Web Printing can print (see "Supported Web Printing File Types" section on page 9-6), and then try printing again. • Simplify the document (remove macros, for example) and then try printing again. If none of the above techniques is helpful, offer the user a refund.
We're Sorry! We were unable to print your file. Please try again later.	**Tell the users this:** A printing error occurred. **What the front desk staff should do:** The front desk staff should check the log to determine what error code, if any, appeared. If the Error Code text is not visible, maximize the browser window. • If the Error Code is not blank; for example, it shows a negative number, report the error code to contact the Cisco TAC. (See the "Obtaining Technical Assistance" section in the Preface to this user guide.). Tell the user to print again later after you have had a chance to correct the problem with Customer Support. • If the Error Code is blank, check the printer for the following problems. Note that the printing resumes when you fix the problem, and users do not need to reprint their jobs: – Paper jam—If the printer has a paper jam, clear the jam and be sure the printer is online. – Printer offline—If the printer is not online, put the printer back online. – Printer out of paper—If the printer is out of paper, refill the paper tray and be sure the printer is online. – Paper tray pulled out—If the paper tray is not pushed in completely, push it in and be sure the printer is online. **Tip** The printer's front panel often indicates the type of problem that has occurred. See your printer documentation for details.

When the Printed Output Does Not Look Correct

Occasionally, the printed output may not look correct. Table 9-9 lists some common problems and solutions.

Table 9-9 Common Printing Output Appearance Problems and Solutions

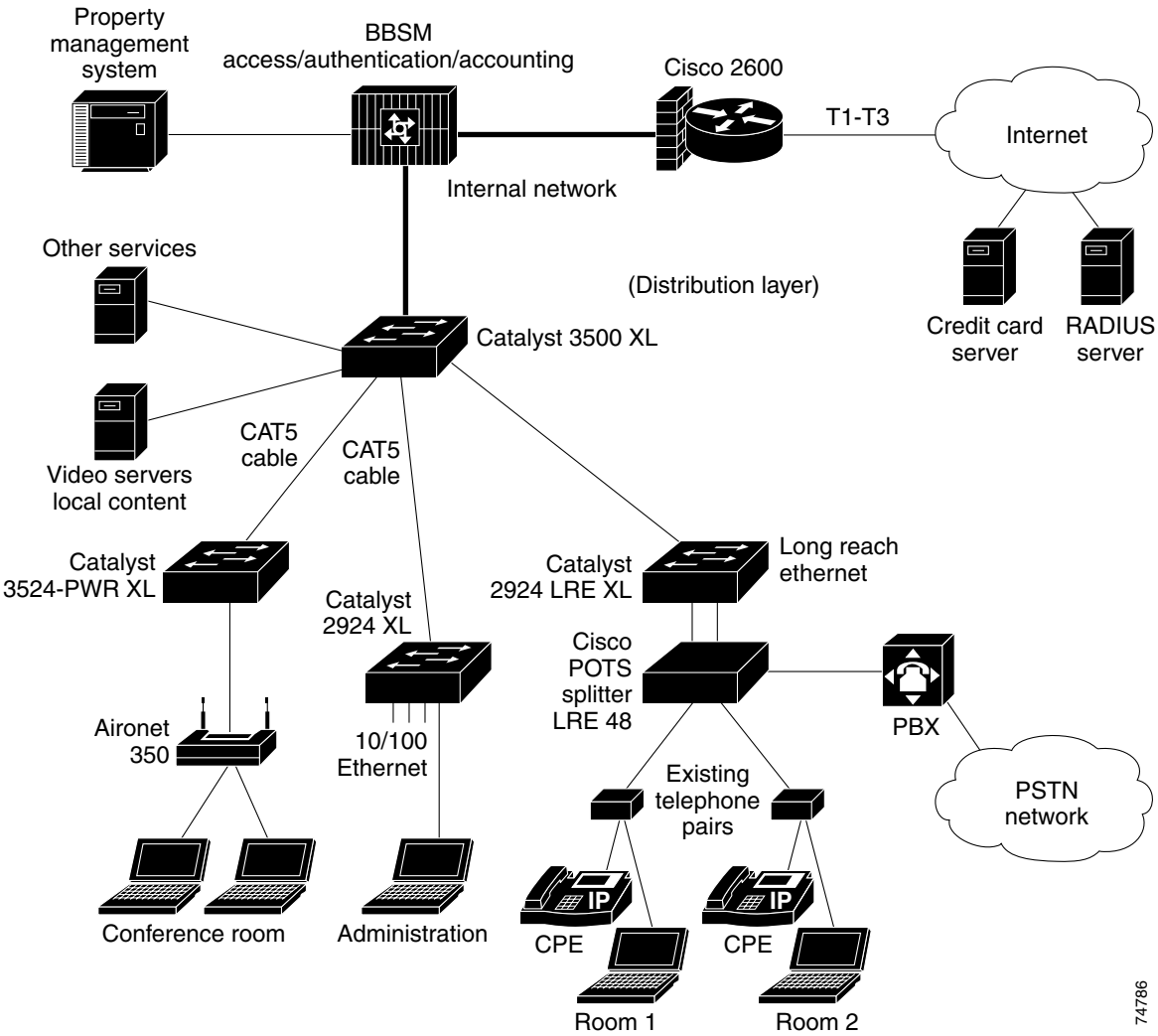
Problem	Solution
Banner page appears (at the front desk) without a printout after an "Unsupported file type" message is logged from BBSM Web Printing.	**Tell users this:** They probably tried to print a nonexistent file, or a type of file that BBSM Web Printing does not support. **What front desk staff should do:** Assure users that they are not charged for the empty printout.
Banner page is followed by a blank page.	**Tell users this:** They probably tried to print a nonexistent file, or left the file name blank in the BBSM Web Printing dialog box. **What front desk staff should do:** Assure users that they are not charged for the empty printout. Tell them to try printing again, using the Browse button in the dialog box to fill in the full path name automatically.
Every sheet of a multisheet workbook prints.	**Tell users this:** BBSM Web Printing always tries to print every sheet in a workbook. If users want to print just one sheet that does not depend on other sheets for its values, tell users to: 1. Copy their original workbook to a new file. 2. Next, delete the unwanted sheets. 3. Then print the new file.
A .log and .txt file does not print correctly or prints only a blank page.	**Tell users this:** Many log files (.log) and some text (.txt) files have header information that is not recognized by BBSM Web Printing. Tell the users to do this: 1. Copy the text into a Microsoft Word file. 2. Try printing again.
The printout is partially or completely black.	This problem usually occurs in spreadsheets or presentations that contain macros or other information that BBSM Web Printing cannot interpret. **Tell users this:** Try simplifying the document and print it again. It is possible that BBSM Web Printing is not able to print the file properly. In this case, assure the user they will not be charged.

BBSM Basics

This appendix provides a general overview of BBSM and its inner workings. For more detail, visit the BBSM web site at http://www.cisco.com.

Today's building networks require a complex combination of multiple technologies to deliver broadband services to end users. Service providers are pushing higher-and higher-speed bandwidth to the network edge. Many types of buildings; hotels, apartments, office buildings, airport concourses, even cruise ships benefit from the availability of T1, T3, and higher-speed network connections. As high-speed connections become universally available, service providers need to provide an effective solution for managing the provisioning and delivery of broadband services to building occupants.

Figure A-1 Typical Cisco BBSM Building Network



Cisco BBSM manages the delivery of broadband services and all network components required for broadband services delivery. Cisco BBSM is a software application that works with a general-purpose operating system and database platform that interact with policy servers as well as intelligent network devices to manage service delivery. Cisco BBSM allows service providers to deliver specific policies to each network access port where users connect. These policies, available on a per-port, per building, or per-user basis, include:

- Multiple access methods—Ethernet, wireless, Long Reach Ethernet (LRE), DSL, and cable
- Multiple authentication methods—port-based, RADIUS, prepaid accounts
- Multiple payment methods—charge to property management system, credit card, RADIUS account, access codes
- Multiple portal options—forced portal, “walled-garden,” free access, custom connect screens
- Multiple bandwidth options—multiple limited bandwidth options

Cisco BBSM essentially combines all network access control and management functions normally contained in multiple servers into one compact management device sized for deployment in the building network environment.

The Cisco BBSM server in Figure A-1 is the unifying agent that integrates the multiple in-building technologies into a complete solution. The Cisco BBSM server manages several key functions:

- Access—Cisco BBSM enables user access regardless of their network interface configurations.
- Authentication—Cisco BBSM supports multiple authentication methods.
- Accounting—Cisco BBSM accounts for usage and collects payment using multiple methods, including:
  - Direct posting of charges to a hotel property management system (PMS) for users connecting from guest rooms
  - Charge processing by a remote credit card processing service; this enables payment from any location on a property
  - Subscribers or prepaid users can authenticate via RADIUS and pay through offline methods
  - Meeting room attendees can use broadband access paid for via access codes

  PMS interface and credit card billing also enable “impulse” charges for additional bandwidth or future value-added services. Billing can be based on full-day or time-block increments.
- Portal—Cisco BBSM redirects all users through two steps during connection. First, they are directed to a Connect Screen, which explains the services available to them, including potentially multiple bandwidth and price options; Walled Garden free access areas, such as local sites, advertising, or weather; and a link to the hotel or property owners' home page. Once users select and purchase service, they are directed to a portal page as their first location on the Internet. This provides a second branding and marketing opportunity.
- Network Buildout and Configuration—Cisco BBSM includes multiple features designed to support network installation, configuration, and testing.

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: • 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.

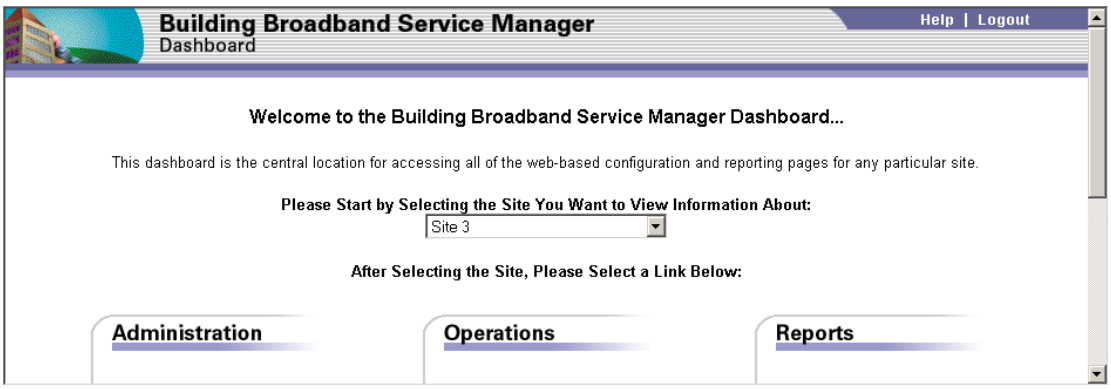
Using the BBSM Dashboard with Multiple Sites

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 *not* 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 *not* 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 *not* 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 *not* 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
Requery	Returns the last set of stored information to the web page from the database.
Delete	Deletes the currently displayed record and its related data (if any). Delete is disabled if no records exist.
Update	Saves the setting changes. Update is disabled if no records exist.
Defaults	Displays default settings for a particular web page. Review the defaults and make changes as necessary.
Generate	Creates a new port map.

Installing an SSL Certificate

This appendix describes how to install a Secure Sockets Layer (SSL) certificate. When you install an SSL certificate on a BBSM server, it enables visitors to verify the site's authenticity and communicate with it securely through SSL encryption, which protects confidential information, such as credit card numbers, online forms, and financial data from interception and hacking.

This protection is accomplished by using “HTTPS” when coding the page sets. SSL comes in two strengths, 40 bit and 128 bit, which refer to the length of the “session key” that every encrypted transaction generates. The longer the key, the more difficult it is to break the encryption code.

If you are using RADIUS or credit card page sets, you must install an SSL certificate for end users to gain access to the Internet.

Caution If you use Netscape for your web browser, because of known compatibility issues with Netscape 4.7x and earlier, you must use Netscape 4.8 or higher for BBSM to work properly.

Obtaining a Domain Name

Secure Server IDs can only be issued to registered owners of a domain name.

Note You can skip this section if you already have a fully qualified domain name.

Use the following procedure to purchase a domain name.

Step 1 Go to http://www.verisign.com.

Note Domain names can be purchased from other companies. Cisco Systems does not endorse any particular company.

Step 2 Click the link for **Business Domain Names**.

Step 3 Enter the domain name you want to purchase.

Step 4 Select the desired extension, such as .com.

Step 5 Click **Go**.

Note If the domain name you chose is already taken, select a name from the suggested list, and click **Search Again** to search for a different name.

Step 6 Once you find a domain name that you like, click **Continue**.

Step 7 Select an option, such as Domain Name Only, and click **Select**.

Step 8 Choose the length of time you would like to purchase the domain name, and then click **Place Your Order**.

Step 9 Proceed with Registration and Payment to complete your order. Be sure to print your receipt before closing your browser.

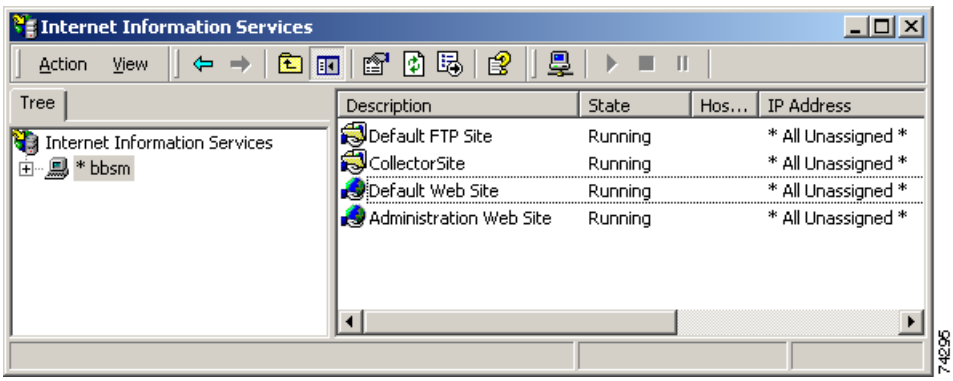
Generating a Certificate Signing Request

Use the following procedure to generate a Certificate Signing Request (CSR) for your web server certificate. This procedure should be performed by the BBSM administrator. Instructions for other supported servers can be found using this link: http://www.verisign.com/support/csr/index.html

Note BBSM servers use Microsoft IIS 5.0.

Step 1 From the BBSM desktop, choose **Start > Programs > Administrative Tools > Internet Services Manager**. The Internet Information Services window appears. (See Figure C-1.)

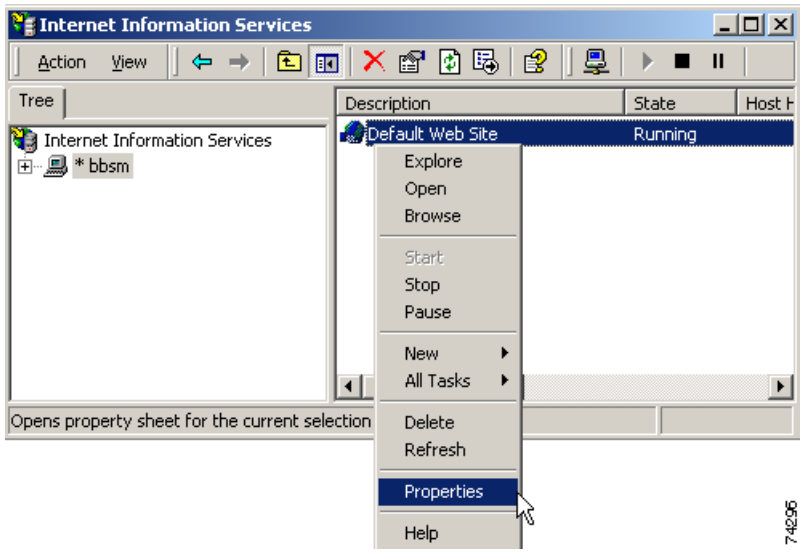
Figure C-1 Internet Information Services Window



Step 2 In the tree in the left pane, click the server name. The server description information appears in the right pane.

Step 3 In the right pane, right-click **Default Web Site**. The popup menu appears. (See Figure C-2.)

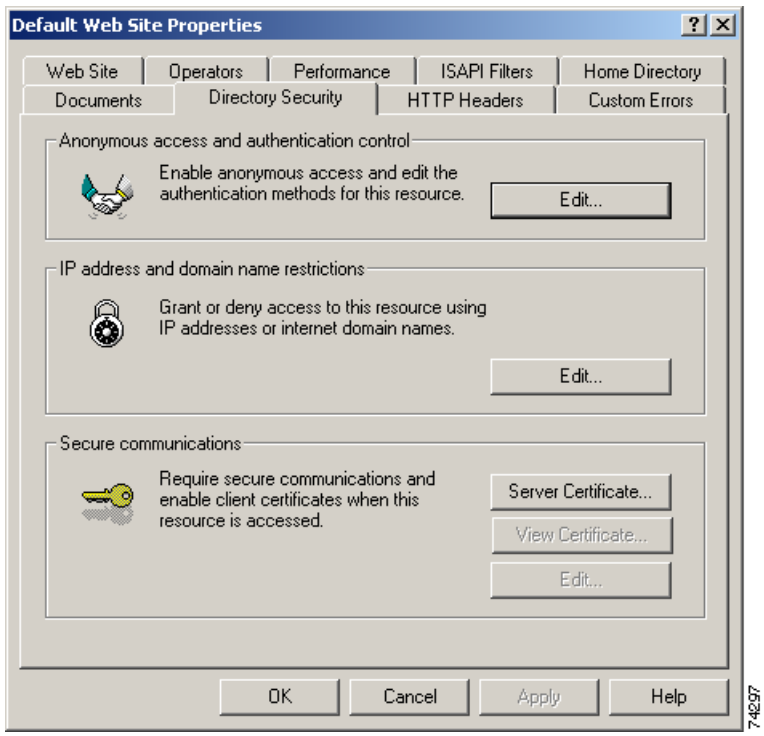
Figure C-2 Internet Information Services Window, Properties Drop-Down Menu



Step 4 From the pop-up menu, select **Properties**. The Default Web Site Properties window appears. (See Figure C-3.)

Step 5 Click the **Directory Security** tab.

Figure C-3 Default Web Site Properties Window

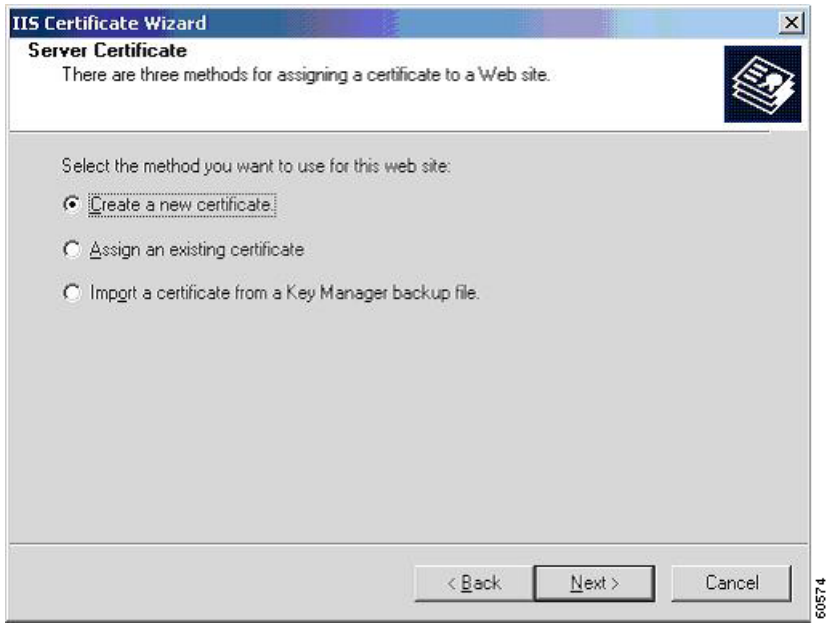


Step 6 In the Secure communications pane, click **Server Certificate...** The IIS Certificate Wizard, Welcome to the Web Server Certificate Wizard dialog box appears. (See Figure C-4.)

Figure C-4 Welcome to the Web Server Certificate Wizard Dialog Box

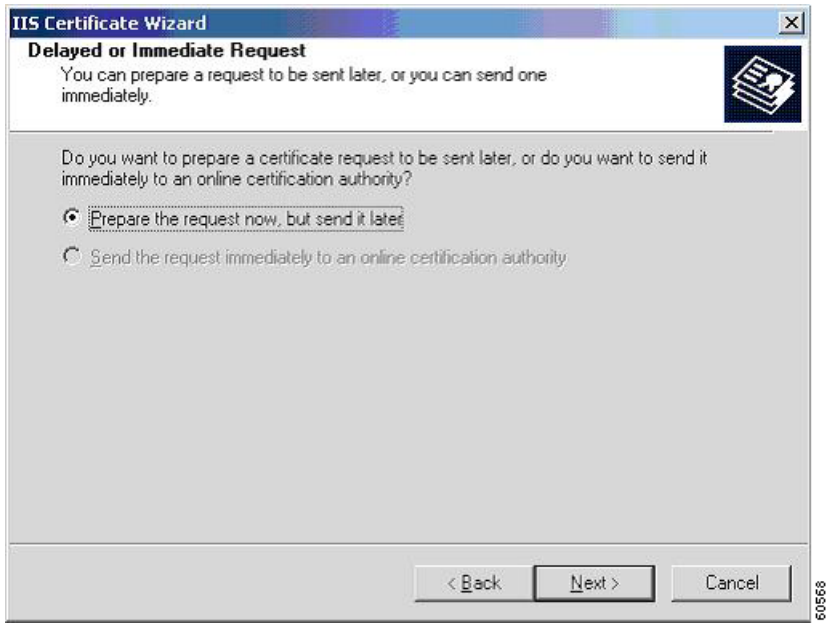
Step 7 Click **Next**. The IIS Certificate Wizard, Server Certificate dialog box appears. (See Figure C-5.)

Figure C-5 IIS Certificate Wizard, Server Certificate Dialog Box



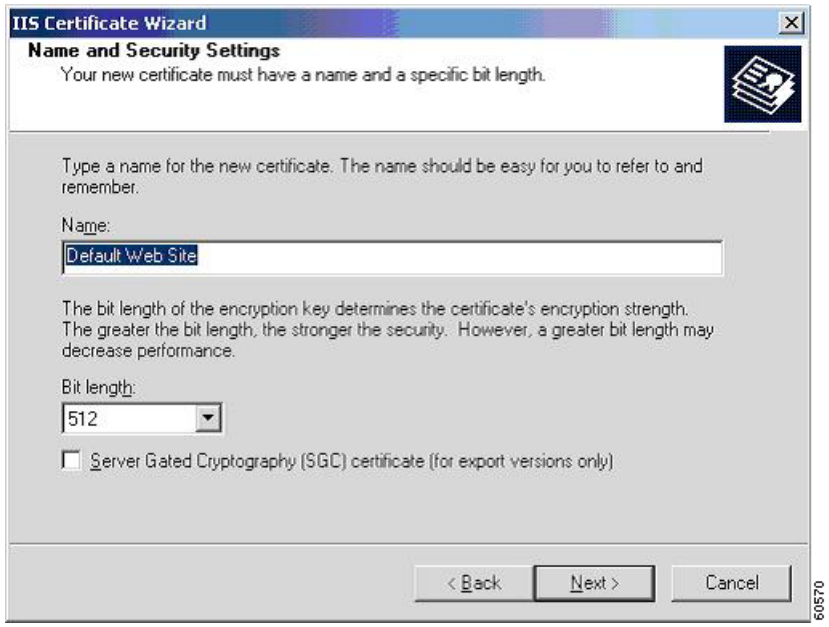
Step 8 Verify that the **Create a new certificate** radio button is selected. If it is not selected, click it. Then click **Next**. The IIS Certificate Wizard, Delayed or Immediate Request dialog box appears. (See Figure C-6.)

Figure C-6 IIS Certificate Wizard, Delayed or Immediate Request Dialog Box



Step 9 Verify that the **Prepare the request now, but send it later** radio button is selected. If it is not, click it, and then click **Next**. The IIS Certificate Wizard, Name and Security Settings dialog box appears. (See Figure C-7.)

Figure C-7 IIS Certificate Wizard, Name and Security Settings Dialog Box



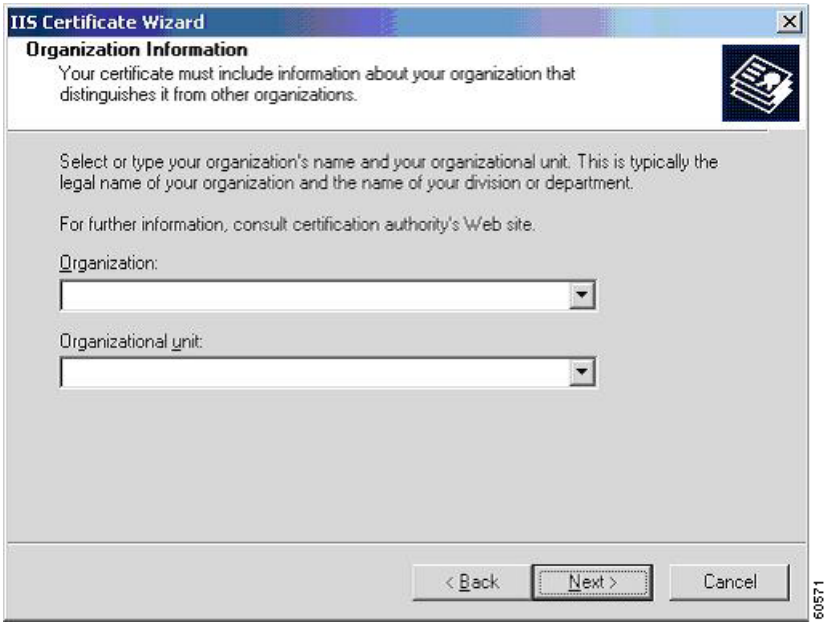
Step 10 Type a name for the new certificate.

Step 11 Click the Bit length drop-down arrow to select the bit length.

Note The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Step 12 Click **Next**. The IIS Certificate Wizard, Organization Information dialog box appears. (See Figure C-8.)

Figure C-8 IIS Certificate Wizard, Organization Information Dialog Box

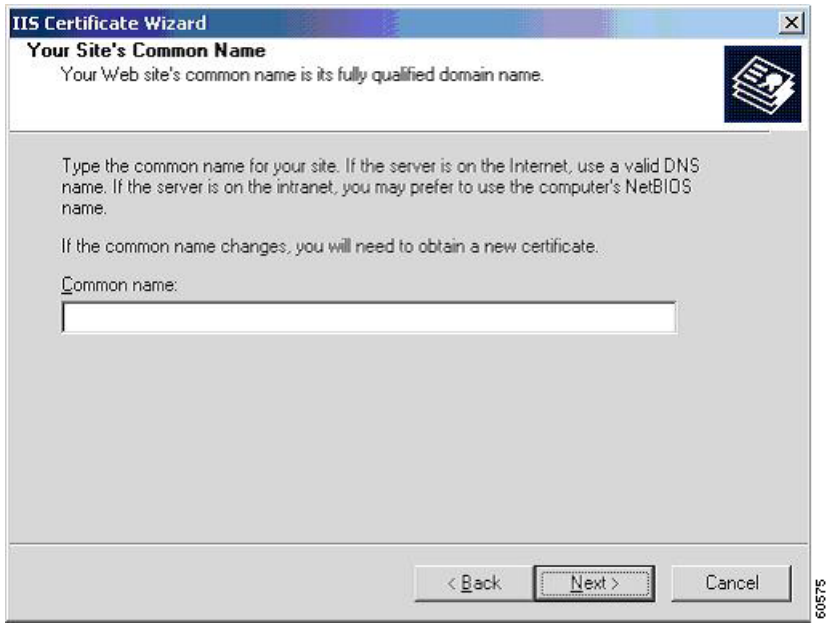


Step 13 In the Organization and Organizational unit fields, type your organization and organizational unit names.

Note You cannot use commas in these fields.

Step 14 Click **Next**. The IIS Certificate Wizard, Your Site's Common Name dialog box appears. (See Figure C-9.)

Figure C-9 IIS Certificate Wizard, Your Site's Common Name Dialog Box



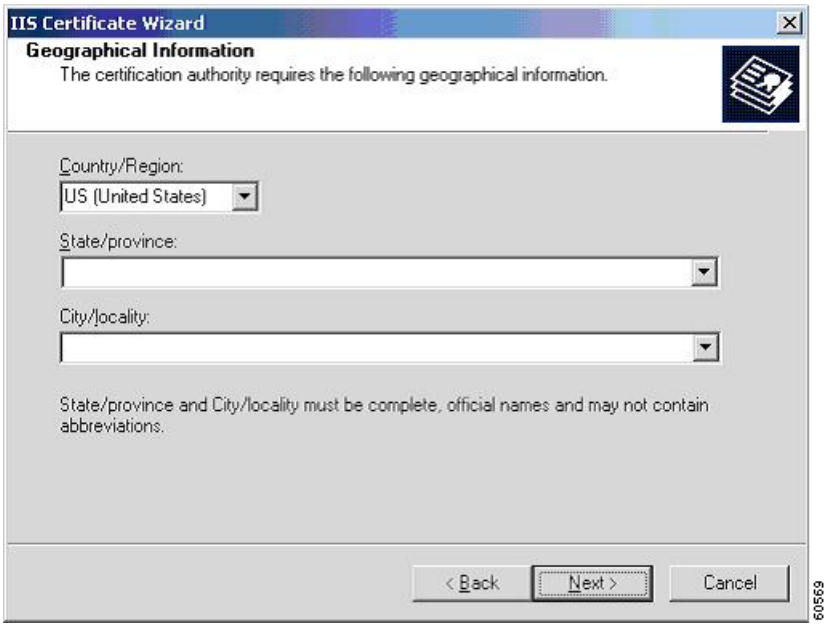
Step 15 In the Common name field, type in your website's common name, and then click **Next**. The IIS Certificate Wizard, Geographical Information dialog box appears. (See Figure C-10.)

Note Your website's common name is its fully qualified domain name. If the common name changes, you will need to obtain a new certificate.

Step 16 On the Server web page in WEBconfig, verify that the Enable Domain Name for SSL Page Sets check box is checked.

Note This box must be checked to test your SSL pages correctly.

Figure C-10 IIS Certificate Wizard, Geographical Information Dialog Box

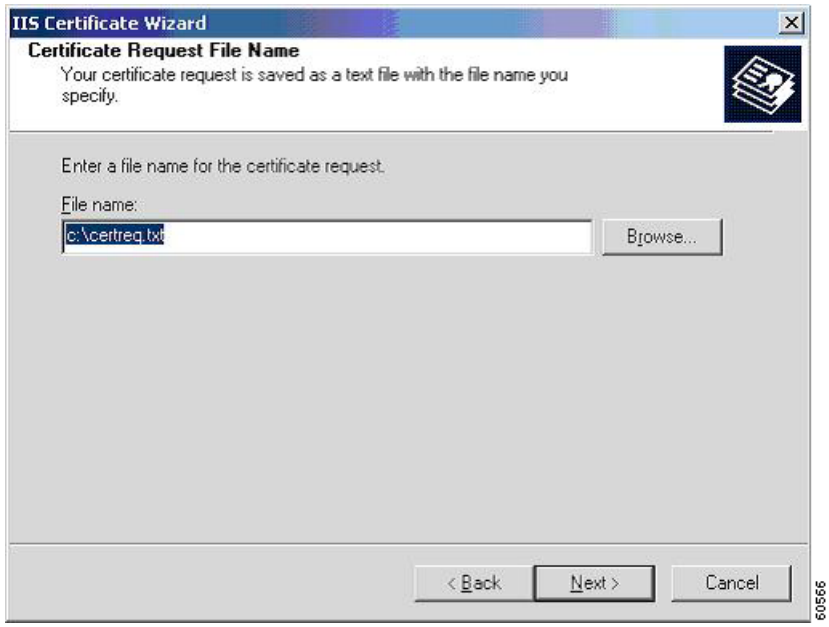


Step 17 In the geographical fields, type the requested information, and then click **Next**.

Note In the State/province field, you must use the full name, not the two-letter abbreviation; for example, California, not CA. You cannot use commas in any of these fields.

The IIS Certificate Wizard, Certificate Request File Name dialog box appears. (See Figure C-11.)

Figure C-11 IIS Certificate Wizard, Certificate Request File Name Dialog Box

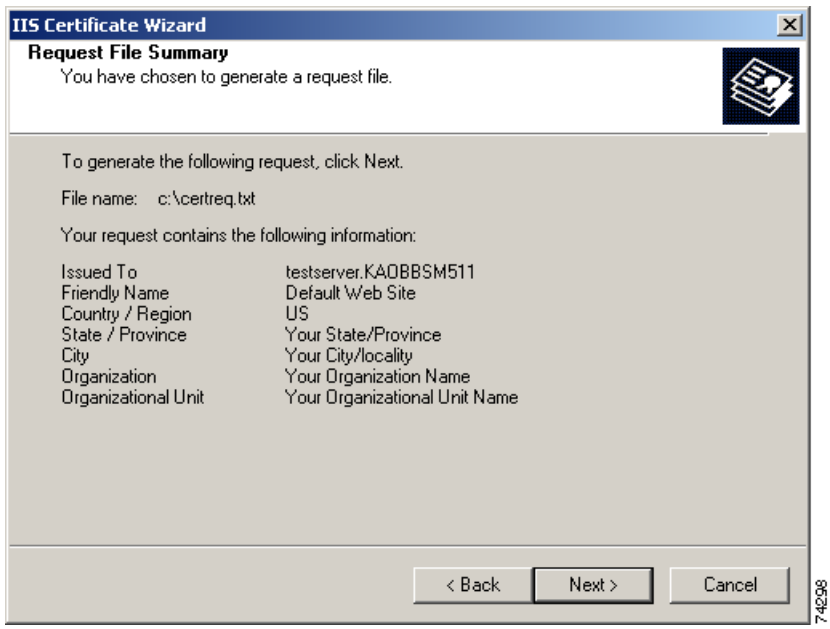


Step 18 Enter a file name for the certificate request.

Note Your certificate request is saved as a text file with the file name that you specify.

Step 19 Click **Next**. The wizard displays a summary. (See Figure C-12.)

Figure C-12 IIS Certificate Wizard, Certificate Request File Name Dialog Box



Step 20 Verify that information is correct, and click **Next**. The IIS Certificate Wizard, Completing the Web Server Certificate Wizard dialog box appears. (See Figure C-13.)

Figure C-13 IIS Certificate Wizard, Completing the Web Server Certificate Wizard Dialog Box

Step 21 Click **Finish** to close the dialog box.

Step 22 Click **OK** to close the Default Web Site Properties, Directory Security tab window.

Step 23 Close the Internet Information Services window.

You have completed the Web Server Certificate Wizard. A certificate is now installed on the BBSM server. If you need to renew, replace, or delete the certificate in the future, you can use the wizard again.

Purchasing a Secure Server ID from a Certificate Authority

After generating the CSR on your BBSM server, you must purchase a Secure Server Digital ID from a Certificate Authority (CA), such as VeriSign, Inc. This will authenticate your website and enable SSL encryption technology.

Note Cisco Systems does not endorse any particular company.

Use the following procedure to purchase a Secure Server Digital ID:

Step 1 Go to http://www.verisign.com, or the CA website of your choice, to access their online enrollment form to purchase a secure certificate.

Step 2 Follow the online instructions.

Note During the enrollment process, you must purchase 128-bit encryption. CA's need to verify that your organization is legitimate and registered with the proper government authorities. The easiest and fastest way to do this is by providing the CA with your company's Dun & Bradstreet DUNS number during the enrollment process. You are not required to have a DUNS number.

Step 3 At some point during enrollment, you will be asked to open the CSR text file (c:\certreq.txt) that you created in the previous section using a text editor, such as Windows Notepad.

Step 4 When asked, copy and paste the CSR into the appropriate text area of the CA's online enrollment form. A CSR looks like this:


```
-----BEGIN NEW CERTIFICATE REQUEST----
MIIBCTCBtAIBADBPMQswCQYDVQQGEwJVUzEQMA4GA1UECBMHRmxvcmlkYTEYMBYG
A1UEChMPRXllcyBvbiBUaGUgV2ViMRQwEgYDVQQDFAt3d3cuZXR3Lm5ldDBcMA0G
CSqGSIb3DQEBAQUAA0sAMEgCQQCeojtjnHqg0GTxp+XZ56RaSe1iZWpumXjU6Sx7
v1FdXzsY1oLOQa090Jtnu1WsQRHh0yDS+45oncjKm1zCG/IZAgMBAAGgADANBgkq
hkiG9w0BAQQFAANBAFBj9g+NiUh8YWPrFGntgf4miUd/wqUshptjJy4PjdsD3ugy
5avvuh3G//PpGh2aYXIjHpJXTUBQyzxSEIINYtc=
-----END NEW CERTIFICATE REQUEST-----
```


Note If any of the information is incorrect, generate a new CSR with the appropriate information.

Step 5 Complete the rest of the application, making sure that the information you enter is correct.

Waiting for the Digital ID to be Processed

After submitting your completed application, your domain's Technical and Organizational Contacts will receive an e-mail message confirming enrollment within 2 hours of submitting the order. It usually takes at least 3 to 5 working days to issue your Secure Server ID.

Installing the Granted Certificate

Use the following procedure to install the granted certificate received from a CA onto your BBSM server.

Step 1 **Choose Start > Programs > Administrative Tools > Internet Services Manager**. The Internet Information Services (IIS) window appears.

Step 2 In the tree in the left pane, click the server name.

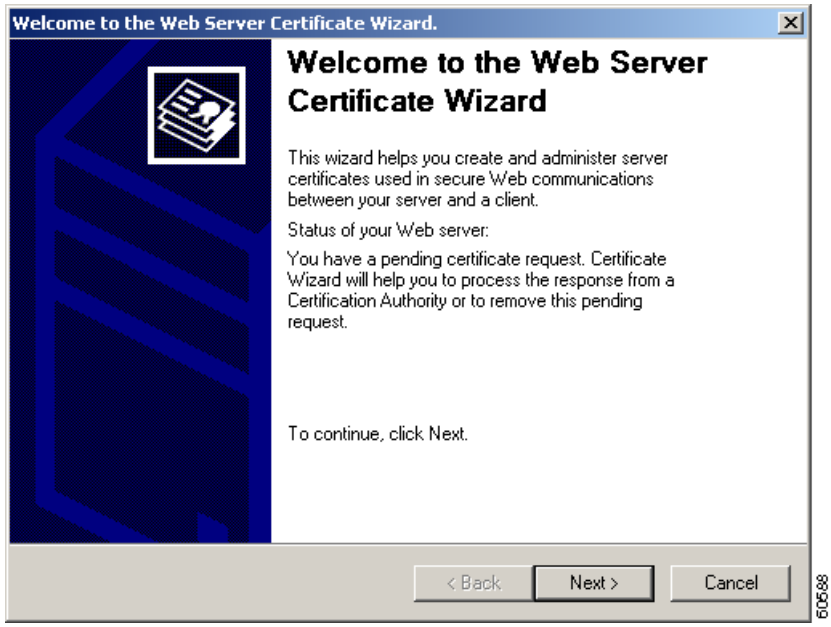
Step 3 In the right pane, right-click **Default Web Site**. The popup menu appears.

Step 4 Select **Properties**. The Default Web Site Properties window appears.

Step 5 Click the **Directory Security** tab. The Directory Security window appears.

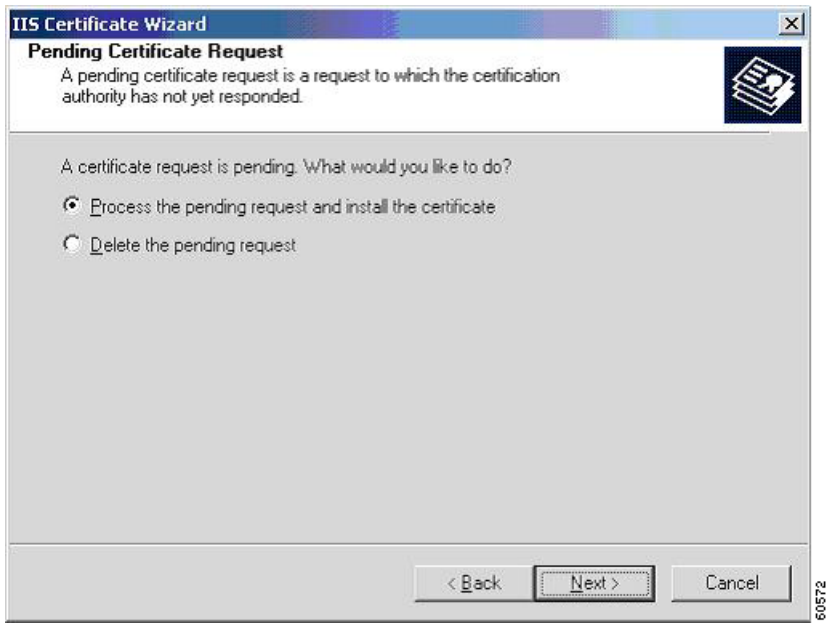
Step 6 In the Secure Communications pane, click **Server Certificate...** The Welcome to the Web Server Certificate Wizard window appears. (See Figure C-14.)

Figure C-14 Welcome to the Web Server Certificate Wizard Dialog Box



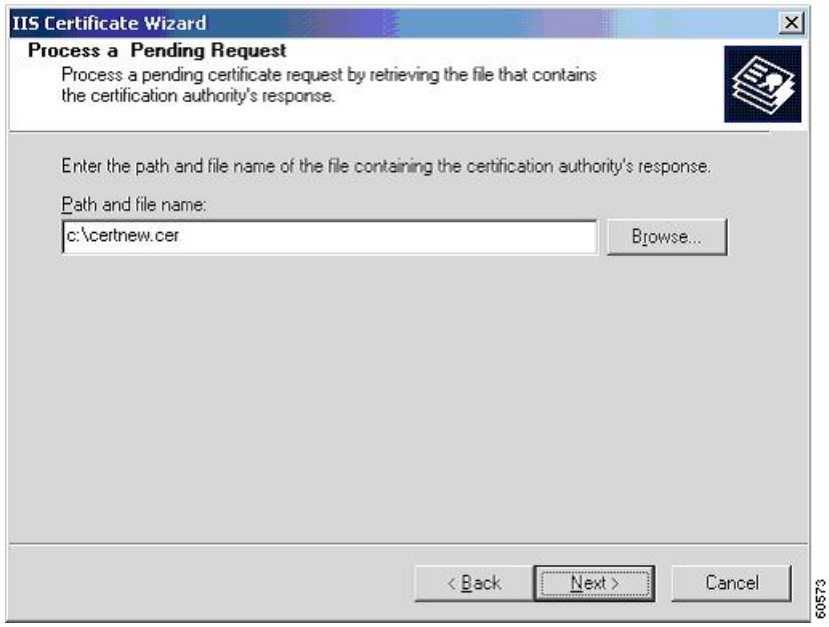
Step 7 Click **Next**. The IIS Certificate Wizard, Pending Certificate Request window appears. (See Figure C-15.)

Figure C-15 Pending Certificate Request Dialog Box



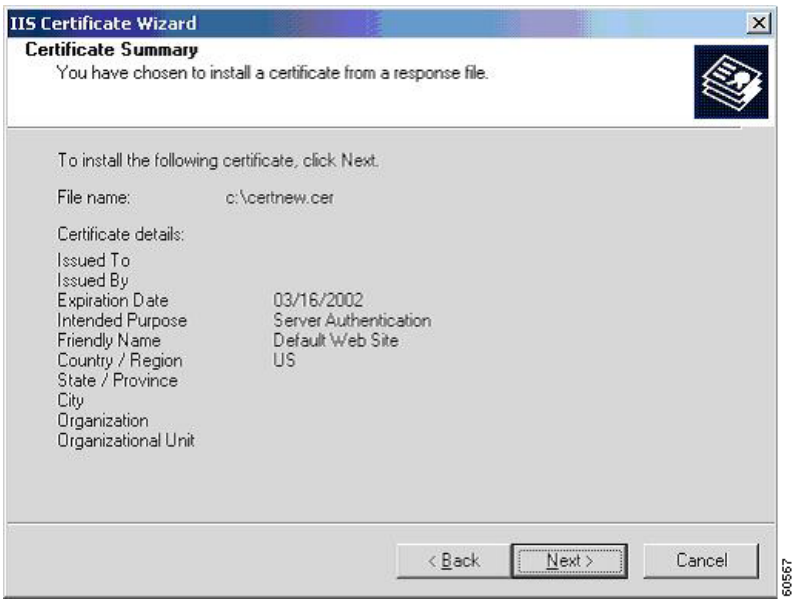
Step 8 Verify that the **Process the pending request and install the certificate** radio button is selected. If it is not, click it, and then click **Next**. The IIS Certificate Wizard, Process a Pending Request window appears. (See Figure C-16.)

Figure C-16 Process a Pending Request Dialog Box



Step 9 In the Path and file name field, type the path and file name of the signed certificate (such as c:\certnew.cer) or use the file received from your certificate authority. Then click **Next**. The IIS Certificate Wizard, Certificate Summary window appears. (See Figure C-17.)

Figure C-17 Certificate Summary Dialog Box



Step 10 Click **Next**. The Completing the Web Server Certificate Wizard window appears, indicating that the installation is complete. (See Figure C-18.)

Figure C-18 Completing the Web Server Certificate Wizard Dialog Box

Step 11 Click **Finish** to close the window. You return to the Default Web Site Properties window.

Step 12 Click **OK** to close the Default Web Site Properties window.

Step 13 Click **OK** to close the Internet Information Services window.

You now have a server certificate installed. You may want to test the Web site to ensure that everything is working correctly. Be sure to use https:// when you test connectivity to the site.

Backing Up the Server Certificate in IIS 5.0

The Microsoft Management Console (MMC) is an application that provides a graphical-user interface and a programming framework in which consoles (collections of administrative tools) can be created, saved, and opened.

Some overview text is needed here.

Creating MMC Snap-in for Managing Certificates

To perform the backup, you must first create a new MMC and add the Certificates snap-in. You can also add the snap-in to another MMC as long as it is opened in Author mode.

Use the following procedure to create a new MMC and add the Certificates snap-in:

Step 1 Choose **Start > Run**.

Step 2 Type **MMC.EXE** and then click **OK**.

Step 3 In the new MMC you created, click **Console**.

Step 4 Click **Add/Remove Snap-in**.

Step 5 In the new window that appears, click **Add**.

Step 6 Highlight **Certificates**, and click **Add**.

Step 7 Select the **Computer account** option, and click **Next**.

Step 8 Select **Local Computer**, and click **OK**.

Step 9 Click **Close**, and then click **OK**.

You have now added the Certificates snap-in, which will allow you to work with any certificates in your computer's certificate store. You may want to save this MMC for later use.

Exporting a Certificate

Now that you have added the Certificates snap-in, you can export the key pair that your Web server is using. To do so, follow this procedure:

Step 1 Open the Certificates (Local Computer) snap-in you added in the last section, navigate to **Personal**, and then to **Certificates**.

Note You will see your Web server certificate denoted by the Common Name (CN), which is found in the Subject field of the certificate.

Step 2 Right-click on the server certificate, select **All Tasks**, and click **Export**.

Step 3 After the wizard starts, click **Next**.

Step 4 Choose to export the private key, and click **Next**.

Caution Do not select Require Strong Encryption. This option causes a password prompt every time an application attempts to access the private key and causes IIS to fail.

Step 5 Choose the file format **Personal Information Exchange**. This will create a PFX file.

Step 6 Click **Next**.

Step 7 Choose a password to protect the PFX file, and click **Next**.

Step 8 Choose a file name that you want to save this as. Do not include an extension in your file name; the wizard adds it automatically.

Step 9 Click **Next**.

Step 10 Read the summary. Pay special attention to where the file is being saved to. If you are sure the information is correct, click **Finish**.

You now have a PFX file containing your server certificate and its corresponding private key. Be sure to move this file to a floppy disk and store it somewhere safe to protect this file.

Importing a Server Certificate in IIS 5.0

To complete this operation, you must have a backup of the server certificate contained in a PFX file.

Creating a MMC Snap-in for Managing Certificates

Use the following procedure to view the Certificates store on the local computer:

Step 1 Choose **Start > Run**.

Step 2 Type in **MMC.EXE**, and click **OK**.

Step 3 Click **Console** in the new MMC that you created.

Step 4 Click **Add/Remove Snap-in**.

Step 5 In the new window that appears, click **Add**.

Step 6 Highlight **Certificates**, and click **Add**.

Step 7 Choose the **Computer account** option, and then click **Next**.

Step 8 Select **Local Computer**, and click **OK**.

Step 9 Click **Close**, and then click **OK**.

You have now added the Certificates snap-in, which will allow you to work with any certificates in your computer's certificate store. You may want to save this MMC for later use.

Importing the Certificate

Now that you have added the Certificates snap-in, you can import the server certificate into your computer's certificate store by following these steps:

Step 1 Open the Certificates (Local Computer) snap-in, and navigate to **Personal**, and then to **Certificates**.

Note If no certificates are listed, it is because none were installed.

Step 2 Right-click **Certificates**, (or Personal, if that option does not exist) and select **All Tasks**.

Step 3 Click **Import**.

Step 4 When the wizard starts, click **Next**.

Step 5 Browse to the PFX file you created containing your server certificate, and click **Next**.

Step 6 Enter the password you gave the PFX file when you created it.

Note Verify that the **Mark the key as exportable** option is selected if you want to be able to export the key pair again from this computer.

Step 7 Click **Next**, and then choose the Certificate Store Personal to save the certificate to.

Step 8 Click **Next**. You should see a summary screen showing what the wizard is about to do. If this information is correct, click **Finish**.

You will now see the server certificate for your Web server in the list of Personal Certificates.

Enabling IIS 5.0 to Use the Imported Certificate

Now that you have the certificate backup imported into the certificate store, you can enable IIS 5.0 to use that certificate. To do this, perform the following steps:

Step 1 Choose **Start > Programs > Administrative Tools > Internet Services Manager**.

Step 2 Right-click **Default Web Site** (the website where you want to enable secure communications), and select **Properties**.

Step 3 Click the **Directory Security** tab.

Step 4 In the **Secure communications** section, click **Server Certificate**.

Step 5 When the Web Site Certificate Wizard starts, click **Next**.

Step 6 Choose the **Assign an existing certificate** option, and click **Next**.

Step 7 You will now see a screen showing that contents of your computer's personal certificate store. Highlight your web server certificate, and then click **Next**.

Step 8 You will now see a summary screen showing you all the details about the certificate you are installing. Be sure that this information is correct or you may have problems using SSL in HTTP communications. Click **Next**.

Step 9 Click **OK** to exit the wizard.

You should now have an SSL-enabled Web server. Be sure to protect your PFX files from any unwanted personnel.

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:

aaabbccddd

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.

Understanding Port Hopping

Cisco BBSM includes a feature known as *port hopping,* which allows the end user to seamlessly move from one wireless access point to another without having to re-authenticate.

Overview

The port hopping feature was designed to allow a user to move between network hardware such as switch ports, cable modems, or wireless access points in a BBSM network and maintain an active session in the BBSM server. This feature can be used in either a wireless or wired network layout. When using wireless network architecture, port hopping improves the user's experience by allowing mobility between wireless access points with uninterrupted service.

Note Port hopping from a wireless access point to a wired switch (or vice versa) is not supported. Also, mobility across subnets or cells operated by different service providers, is not supported.

If port hopping is enabled, BBSM keeps the session active when the user moves to another port or disassociates temporarily. For example, disassociation might occur when the signal is weak or an object comes between the wireless access point and the user, causing the user to suddenly associate with a secondary access point that might be configured to another aggregation switch port. BBSM continues to search for the user. If the user reappears back on the network within a configurable period of time, the session continues without interruption. If the user does not reappear on the network within the period, BBSM deactivates the session, and the user must re-authenticate to regain Internet access.

The BBSM Port Hopping feature is disabled by default. The Port Hopping feature is enabled and configured through BBSM WEBconfig by an administrator. Configuration of this feature can also be done through the Port Control and Subscription Port Control submenus of the BBSM Dashboard under Operations.

Functional Description

This section provides details on how BBSM Port Hopping interacts with the BBSM system. Additionally, any limitations or restrictions of using this feature are discussed. Transactions that occur while using this feature are logged into the BBSM Transaction History report. These specific port hop transactions are found in the "Transaction History Reporting for Port Hopping" section on page E-3.

Port Hopping Not Allowed Between BBSM Sites

The BBSM Port Hopping feature is configured per site and is *not* allowed across multiple BBSM sites. A user is limited to moving to and from ports within a specific BBSM site. If a user attempts an inter-site port hop, the user's session is deactivated and the user must re-authenticate to regain Internet access to the new BBSM site. If a user disappears from the network for a period of time less than the Port Hop Delay, the session remains active until the system finds the user again on a port on the same BBSM site. If BBSM finds the user on a port within a different BBSM site from where their active session originated, the session is deactivated.

Note The possibility exists that a user can move from the original site, authenticate to another site, and then move back to the original site within the duration of the Port Hop Delay parameter. In this case, BBSM deactivates the original active session even though the user eventually moved back to the original site. You should deploy your network to prevent overlap between cells on different sites.

Searching Network Elements for Port Hopping Users

When BBSM port hopping is enabled and a user disappears from the network, the BBSM system searches for the user. The BBSM software searches the configured network elements (Ethernet switches, access points, etc.) to locate the user. You configure the list of network elements using the BBSM WEBconfig Switches web page. BBSM system searches the last known network element that the user was connected to or associated with first. If the user is still not found, the system will begin to search all of the other configured network elements. BBSM performs this search every minute until the user is found or the BBSM Port Hop Delay time parameter expires.

Note While the system is searching for a user, the active session for the user remains active and appears in the Active Ports report.

BBSM Port Policy for Port Hopping Users

As the user hops from port to port, the port policy that BBSM associates with the user session follows the user to each new port.

The BBSM system applies the bandwidth limit (in kilobits per second) specified at session activation to the active session as the user moves from port to port. If a user has selected a dynamic bandwidth boost from a BBSM web page, when the user moves to another port, the bandwidth boost settings follow the session to the new destination port.

Port Hopping to a Restricted Port

The BBSM Port Hopping feature is enabled by applying a value of true or false to a configured port. If the user starts on or moves to a port where the Port Hopping value was configured as "false" (meaning port hopping is not allowed or enabled on this BBSM port), then BBSM ends the user session if the user attempts to move to a different port.

Session Duration for BBSM Port Hopping

The values for the duration of an active session reported in the system vary depending on how the session terminates. The BBSM system will report the time that it searched for the user in the session duration if the search succeeds. If the system searches for the user and fails to find the user before the port hop delay time expires, the BBSM system will not include the time spent searching in the reported length of time for that active session. In this way the user that terminates a session by turning off the computer is not charged for any system time that was spent looking for the user on other ports.

Hotel Billing Policy and BBSM Port Hopping

The BBSM Port Hopping feature works with any of the BBSM Page Set templates used to define an access service. However, when using this feature in a wireless network, some of the BBSM templates may not be applicable. For example, the page set templates that use the BBSM Port ID and Room Number for billing purposes, such as the DailyHotel policy, will not have meaning. A wireless network does not recognize the concept of a *room* because wireless access points can extend through walls. Most wireless access points (e.g. Cisco Aironet) map all users to the same port number and the concept of a room number which identifies the access point may not apply at all. Use of the Hotel Accounting Policy in this scenario would not provide useful billing information for a property management system to accurately charge users.

Alternatively, if the application uses a wired network, the port numbers and room numbers are much more meaningful to a hotel situation. The BBSM Port Hopping feature keeps track of the original port and original room numbers to ensure that the charges incurred during the session are billed correctly to the user. As a user moves from port to port, the system reports each new port and room, but the system bills only the original port and original room.

Transaction History Reporting for Port Hopping

The BBSM Port Hopping feature uses the existing Transaction History report to record transactions that occur while using the feature. Each time a port hop event occurs on the BBSM system, the system makes an entry into the Transaction History report to record the event. These transactions can be viewed in the BBSM Transaction History report, which is accessed through the Reporting Pages link on the BBSM Dashboard.

Entries are displayed in the Transaction History report when:

- A user starts a port hop by disappearing from the network.
- A user successfully moves from one port to another.
- A user moves to another port, but the port hop time expires before being located on the next port.
- A user moves to a port in another BBSM site, which terminates the active session. The transaction is recorded on both sites.

The following table provides a description of each column in the BBSM Transaction History report:

Table E-1 BBSM Transaction History Report Columns

Attribute	Description
Date / Time	The date and time when the port hop event occurred.
Type	The type of port hopping transactions that occurred. The possible types are: • Port Hop Started • Port Hop Completed • Port Hop Failed, attempt to hop to another site • Port Hop Time Expired, deactivating session
IP	The IP address of the user who moved ports.
Previous State	The value “Active” is used for port hop events.
New State	The value “Active” is used for port hop events.
Amount	Because BBSM did not bill for the port hop, the amount column has the value zero.
PortID	The PortID column displays the port to where the user moved.
MAC	The MAC column displays the MAC address of the user who moved ports.
Room	This column displays the room number or geographic location associated with the port to where the user moved.
Duration	This is zero for port hop everts.
Bandwidth Kbps	This column displays the bandwidth limit (in kilobits per second) applied to the session.

BBSD Feature

The Building Broadband Service Director (BBSD) is a standalone feature module included with the BBSM software package. The BBSD software enables a central system in the data center to manage remote BBSM systems. The primary functions include backing up key BBSM system data, performing centralized reporting across a group of BBSM servers, and pushing BBSM web content pages (ASP files sometimes called *BBSM page sets*) across a group of BBSM servers in the field. BBSD stores BBSM server configuration data, which enables you to restore a BBSM server and provides an interface for sending minor software patches to BBSM Servers.

Note The BBSD software should operate on a standalone server system in a secure central data center.

The Cisco BBSD package comes with a default database called Microsoft Data Engine (MSDE), which is adequate for evaluation purposes but is not intended for production BBSD environments. We recommend that you upgrade the BBSD system to use the full Microsoft SQL Server software prior to putting the system in a production mode.

Caution When BBSM is installed, the user is prompted for a BBSD username and password. BBSM creates a Windows user account and an SQL Server login using this username and password. Both logins are required for BBSD to function. BBSD stores a username and password for each BBSM server. For the BBSD to connect to each BBSM server, the stored username and password must match both the Windows BBSD login and the SQL Server login on the BBSM server.

For complete information on setting up and configuring BBSD, see the *Cisco Building Broadband Service Director Software Configuration Guide*.

Configuring a Laptop for Room Mapping

This section details the configuration of a laptop computer that is being used for room mapping.

Configuring a Laptop

To perform room mapping, you need a laptop that meets the following specifications:

- Windows 95, 98, Me, Windows 2000 Professional, or NT 4.0 Workstation
- A network interface card (NIC) that is configured to use TCP/IP with DHCP enabled and DNS disabled. (For Windows 2000 Professional, set it to obtain a DNS server address automatically.)
- One of these web browser releases: Internet Explorer 4.0 or higher, or Netscape 4.8 or higher

Caution If you use Netscape for your web browser, because of known compatibility issues with Netscape 4.7x and earlier, you must use Netscape 4.8 or higher for BBSM to work properly.

- All proxy server access to the Internet turned off

Note The laptop can remain turned on as you go from room to room.

Windows 95, 98, or Me

Use the following procedure for setting up a laptop using Windows 95, 98, or Me.

Step 1 From your desktop, right-click **Network Neighborhood**.

Step 2 Click **Local Area Connection**.

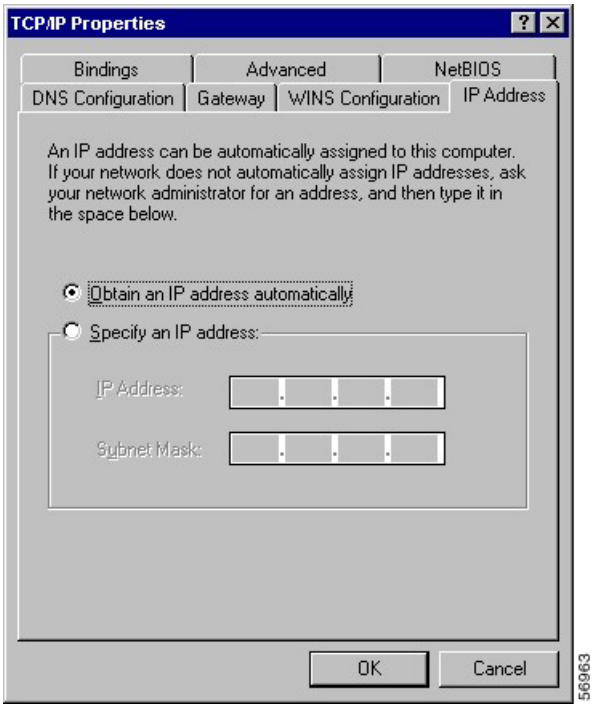
Step 3 Click **Properties**.

Step 4 Select the **Configuration** tab.

Step 5 Choose the TCP/IP protocol for your network interface card (Windows 95/98/NT4.0).

Step 6 Click **Properties**. (See Figure G-1.)

Figure G-1 TCP/IP Properties



Step 7 Select the **IP Address** tab.

Step 8 Click the **Obtain an IP address automatically** radio button.

Step 9 Select the **Gateway** tab.

Step 10 Remove all gateway addresses.

Step 11 Select the **DNS Configuration** tab.

Step 12 Select **Disable DNS**.

Step 13 Click **OK** to close the TCP/IP Properties window.

Step 14 Click **OK** to close the Network or General window.

Note If you receive a request to copy files from your Windows CD, follow the on-screen instructions.

Step 15 If a dialog box appears to restart, click **Yes**.

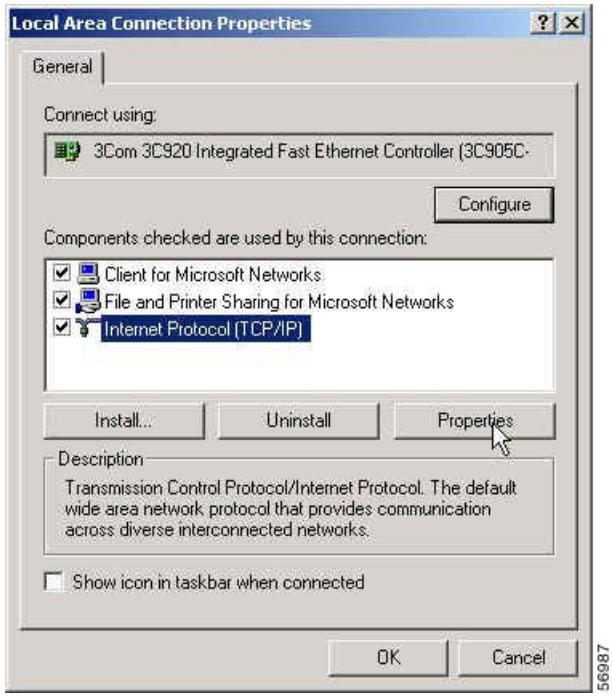
Windows 2000

Use the following procedure for setting up a laptop using Windows 2000.

Step 1 Choose **Start > Settings > Network and Dial-up Connections > Local Area Connection**.

Step 2 Click **Properties**. (See Figure G-2.)

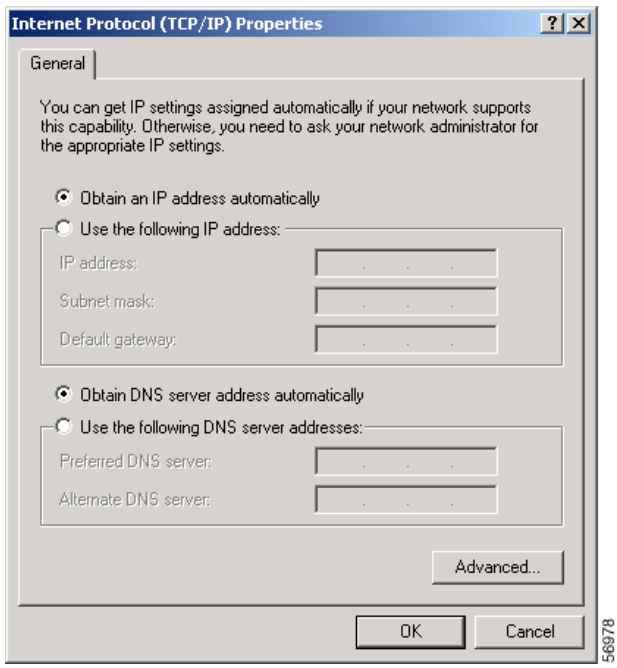
Figure G-2 Local Area Connection Properties Window



Step 3 Highlight **Internet Protocol (TCP/IP)**, and click **Properties**.

Step 4 Verify that Obtain an IP address automatically and Obtain a DNS server automatically are both selected, and click **OK**. (See Figure G-3.)

Figure G-3 Internet Protocol (TCP/IP) Properties Window



Step 5 Click **OK** to close the Internet Protocol (TCP/IP) Properties window.

Step 6 Click **OK** to close the Local Area Connections Properties window.

Step 7 Click **OK** to close the Local Area Connection Status window.

Note If you are using Windows 2000, no reboot is necessary.

Configuring the Browser

Regardless of the type of browser that you are using, it must be set to connect directly to the Internet with all proxy server options turned off.

Internet Explorer

Use the following procedure to configure Internet Explorer 4.0 or higher.

Step 1 Open Internet Explorer.

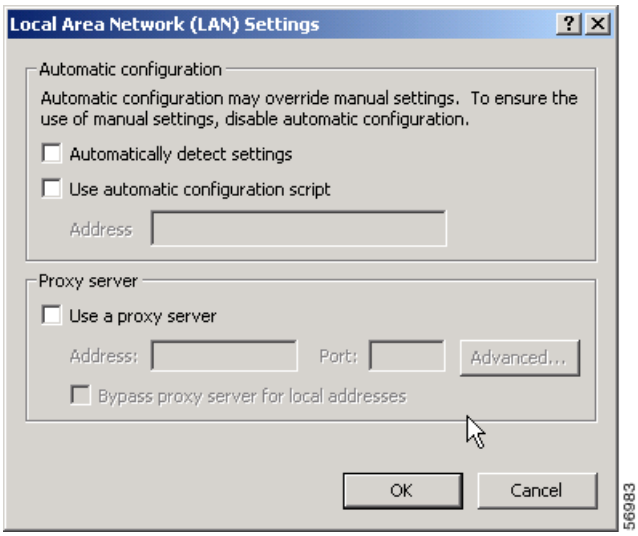
Step 2 Choose **Tools** > **Internet Options**.

Step 3 Select the **Connections** tab.

Step 4 Click **LAN Settings**.

Step 5 In the Local Area Network (LAN) Settings window, uncheck all check boxes. (See Figure G-4.)

Figure G-4 Local Area Network (LAN) Settings Window



Step 6 Click **OK**.

Step 7 Close Internet Explorer.

Netscape

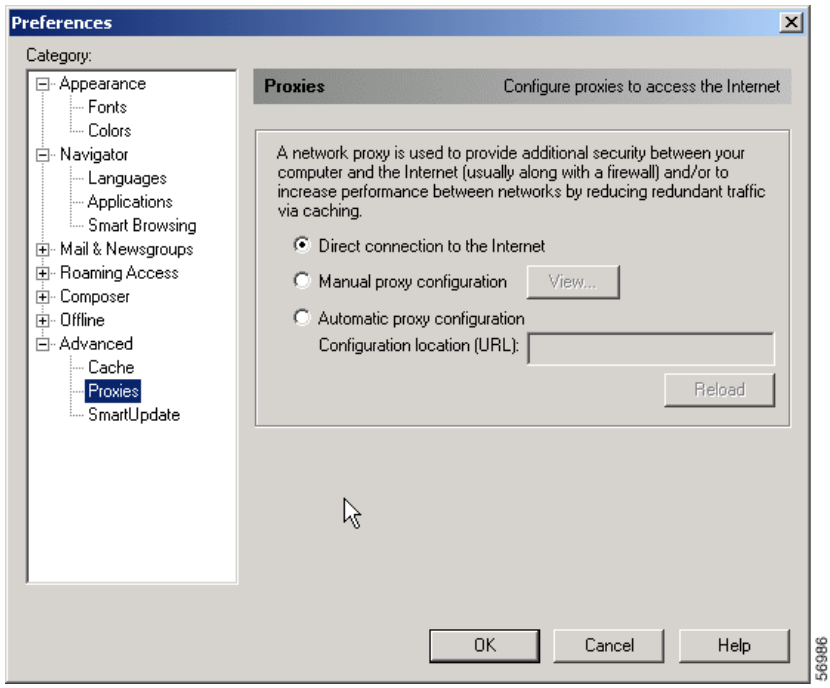
Use the following procedure to configure Netscape 4.x.

Step 1 Open the Netscape browser.

Step 2 Choose **Edit > Preferences**.

Step 3 Click **Advanced > Proxies**. The Proxies Preferences window appears. (See Figure G-5.)

Figure G-5 Network Proxy Setting



Step 4 Select the **Direct connection to the Internet** radio button.

Step 5 Click **OK**.

A

access code A five-digit number that the BBSM software generates for access to the Internet.

access policy An access policy defines how an end user gains access to the Internet through BBSM. The access policy is the BBSM logic that controls the duration of the Internet access for the end user.

access policy module BBSM ships with several access policy modules. An access policy controls the web user interface that an end user experiences before the session is active, and it also monitors the end user's session while it is active. An integrator can create a new access policy module by writing a DLL in C++.

accounting policy An accounting policy authorizes and posts charges for access to the Internet. An accounting policy is the BBSM logic that controls how the end user is charged for Internet access.

accounting policy module BBSM ships with several accounting policy modules. An accounting policy module charges for various services that the access policy module provides. An access policy decides when, or even if, it should invoke an accounting policy module. An integrator can create a new accounting policy module by writing a DLL in C++.

activate (session) Activating a session is the process by which BBSM grants Internet access to an authenticated end user.

Active Server Page *See ASP.*

Administrator A user who has authentication rights on the BBSM server as an Administrator. The administrator has full access to control and configure the system; that is, to add and edit sites and PMS systems and gain access to all other resources available on the BBSM system. Administrator access is on a global, not per-site, basis. *See also Operator and Reports user.*

API application program interface. An API is the language and message format by which an application program talks to communications software. Standardized APIs allow application programs to be developed independently of the underlying method of communication. It is a set of standard software interrupts, calls, and data formats that computer application programs use to initiate contact with other devices; for example, network services, mainframe communications programs, or other program-to-program communications. Typically, APIs make it easier for software developers to create the links that an application needs to communicate with the operating system or with the network.

ARP address resolution protocol. ARP is a protocol for mapping IP addresses to physical addresses in the local network.

AS answer status.

ASP Active Server Page. An ASP file is a web page implemented using Microsoft IIS ASP technology. ASP files can contain logic that runs on the web server before the page is served to the client browser. Typically, the server side logic looks up information from a database and generates specific content for the client based on the information looked up.

AtDial 1. Running as a Windows 2000 service, the component of BBSM configuration and logging data.

2. The BBSM SQL server database that contains BBSM configuration and logging data.

Athdmn Adaptive Translation Deamon (UNIX).

authentication The process by which BBSM identifies the user by verifying the user's credentials, using an external system, such as a RADIUS server or a credit card server.

authorization The process by which BBSM allows the client access to the Internet by obtaining user credentials for authentication (such as username, password, and credit card number) and other policy preferences, such as bandwidth selection.

B

BAN building area network.

barred In the hospitality industry, the term "barred" is used to describe a guest room that is cash only and not allowed to make charges.

BBSD (Cisco) Building Broadband Service Director. BBSD is a feature of BBSM that provides backup/restore capabilities for BBSM servers. It also provides centralized usage reporting.

BBSM (Cisco) Building Broadband Service Manager. BBSM is an authentication, authorization, and accounting router, built on Windows 2000 technology, that controls access to and charging for Internet access in building-centric applications, such as hotels, apartments, and multi-tenant offices.

bridged network In bridged networks, a repeater or transparent bridge connects two or more network elements and forwards packets between them. It allows clients to communicate directly with each other as if they are attached to the same network. In this configuration, the packet appears to come directly from the sending clients, even if a bridge or repeater is in the path.

C

cable modem A device that enables you to hook up your PC to a local cable TV line and receive high-speed data.

CAS call accounting system.

certificate An electronic credential used to establish identity when conducting web transactions for the purpose of securing communications between the web server and the web browser. The certificate contains sufficient information that the recipient can verify that the certificate is real. *See certificate authority.*

certificate authority A company that issues and manages security credentials; that is, certificates. The CA verifies the information provided by the requestor of the certificate. If the CA successfully verifies the requestor's information, the CA then issues a certificate to the requestor. *See certificate*.

certificate request A file generated by following the certificate request generation procedure. An administrator generates a certificate request, sends the request to a certificate authority, and receives from the certificate authority a signed certificate for installation on the Microsoft Internet Information Server (IIS).

client The hardware device, such as a laptop or PC, that the end user uses to access the Internet through BBSM. *See end user.*

client search The process used to search network elements in a BBSM network to locate the stack, switch, and port to which a client is physically connected.

CMS Conversational Monitor System. CMS is software that provides interactive communications for IBM's VM operating system. It allows a user or programmer to launch an application from a terminal and interactively work with it.

CMTS Cable Modem Termination Systems. A CMTS is a component that exchanges digital signals with cable modems on a cable network. When a CMTS sends signals to a cable modem, it converts them into Internet Protocol (IP) and sends the signal to a router for transmission over the Internet.

CNR Cisco Network Registrar. CNR is a Cisco DHCP server that runs on Windows or Solaris and can be extended with C++ DLLs.

COM common object model. COM is a platform-independent, distributed, object-oriented system for creating binary software components that can interact. It requires a formal separation of interface and implementation; that is, it requires that clients communicate with objects exclusively through interface references.

COS class of service.

CPE customer premise equipment.

CSR certificate signing request.

customer An individual or organization who purchased BBSM.

D

dashboard A central location for similar features or links related to a specific feature or feature set. The BBSM dashboard is the BBSM-hosted web page that contains links to all BBSM management and reporting web applications.

deactivate (session) Deactivating a session is the process by which BBSM denies access to the Internet to a formerly authorized end user.

deprecated parameter An API feature that is still supported but not recommended for use, because it may be removed in the future. Usually a newer feature has superseded a deprecated parameter.

DHCP Dynamic Host Configuration Protocol. DHCP is a protocol that allows TCP/IP settings of a networked computer, called a DHCP client, to be configured automatically from a central DHCP server. In the BBSM network, the BBSM server is a DHCP server, and a guest computer may be a DHCP client.

DHCP Option 82 The Relay Agent Information Option, as described in RFC 3046. Option 82 is a DHCP option that contains information to be sent from a DHCP relay agent to a DHCP server. This is normally used to convey information that is known by the relay agent, but is not accessible by the server.

DLL dynamic link library. A DLL is a library of executable functions or data that can be used by a Windows application. The DLL feature allows executable code modules to be loaded on demand and linked at run time, which enables the library code to be updated automatically (transparent to applications) and then unloaded when they are no longer needed.

DNS Domain Name System. DNS is name resolution software that lets users locate computers on a UNIX network or on the Internet (TCP/IP network) by domain name. The DNS server maintains a database of domain names (host names) and their corresponding IP addresses.

DOCSIS Data-Over-Cable Service Interface Specification. DOCSIS is a standard for cable products to facilitate the interoperability of the hardware from different vendors.

DSL digital subscriber line

DSLAM digital subscriber line access multiplexer. A DSLAM is a device that connects many digital subscriber lines (DSLs) to a network by multiplexing the DSL traffic onto one or more network trunk lines.

E

end user In regard to BBSM, an end user is a user who accesses the Internet through the BBSM server. The term is used interchangeably with user. *See user.*

external network BBSM acts as a router connecting two networks: the external network and the internal network. The external network is “closer” to the Internet. BBSM does not allow an end user to transmit packets to the external network until the end user has an active session. *See internal network*.

F

folio An itemized list of charges accrued by an end user.

forced redirect A forced redirect occurs when an end user attempts to view one URL and BBSM forces the user to a different URL. BBSM performs a forced redirect when it detects an unauthenticated client, or a client that needs to reauthenticate.

FQDN fully qualified domain name. An FQDN is that portion of the URL that defines the server addressed by the URL. For example, the FQDN of http://www.microsoft.com/default.asp is www.microsoft.com.

FSIA full-speed Internet access.

G

gateway address The address of the gateway used to reach a specified destination; for example, on a network or the Internet. Gateways are devices that route packets between the different physical networks.

GUI graphical user interface.

H

Handheld PC A Handheld PC is a class of PC devices that has a half VGA screen (640 by 240 pixels) or a full-size screen (640 by 480 or 800 by 600 pixels) with or without an integrated keyboard, or roughly, a device that fits into the palm of your hand.

HMRIAM Hotel Meeting Room Internet Access Management. HMRIAM is an application that is accessible through the BBSM dashboard.

host byte order The order of bytes in a binary representation of a number on a host computer. On Intel computers, the least significant byte is the first; for example, a 16-bit word representation of “256” is 0x0010.

HTTP Hyper-Text Transmission Protocol. HTTP is a TCP protocol used to request and deliver web pages.

I

ICMP Internet Control Message Protocol. ICMP is a TCP/IP protocol used to send error and control messages. For example, a router uses ICMP to notify the sender that its destination mode is not available. A ping utility sends ICMP echo requests to verify the existence of an IP address.

IETF Internet Engineering Task Force. The IETF is the main standards organization for the Internet. It is a large, open, international community of network designers, operators, vendors, and researchers concerned with identifying problems and opportunities in IP data networks and proposing technical solutions to the Internet community.

IIS (Microsoft) Internet Information Server. IIS is Microsoft’s web server that runs under Windows NT. You can install a certificate on the server to enable it to serve pages using Netscape’s SSL security protocol.

Inetinfo Inetinfo is the process in the Microsoft IIS in which the BBSM Access Policy ActiveX server components run.

integrator A software developer that uses the BBSM SDK to extend the functionality of the BBSM.

internal adapter The internal adapter communicates with the local area network; that is, the internal network.

internal network The network that the end user connects to. The internal network consists of a collection of network elements, end-user computers, and the BBSM internal interface. *See external network*.

IP address Internet Protocol address. The 32-bit (IPv4) address of a network interface on a computer. A computer with multiple network interfaces typically has a different address for each interface.

iPass Smart Client The iPass Smart Client is a piece of software on an end-user PC that controls the user experience for gaining access to the Internet in a visitor-based network.

ISA (Microsoft) Internet Security and Acceleration. ISA is the name of the Microsoft’s server that replaces Microsoft Proxy Server 2.0. It provides caching, proxy server, and firewall features.

ISAPI Internet server application program interface. ISAPI is a programming interface on IIS, Microsoft's web server. It allows third parties (and Microsoft) to add functionality to web servers running Microsoft IIS.

ISAPI filter A DLL that uses the Internet Server API (ISAPI) to register for web server events and edit the data stream going to and coming from the Microsoft IIS web server.

J

JavaScript An interpreted programming script language that is used in HTML programs and ASP files.

external network BBSM acts as a router connecting two networks: the external network and the internal network. The external network is “closer” to the Internet. BBSM does not allow an end user to transmit packets to the external network until the end user has an active session. *See internal network*.

K

kbps kilobits per second (thousands of bits per second). kbps is a measure of bandwidth on a data transmission medium.

key manager The part of Microsoft IIS that allows the BBSM administrator to generate a certificate request and install a signed certificate.

KeyView Pro A desktop utility that provides instant access to virtually all the popular file formats for viewing, printing, or converting files to Rich Text Format (RTF).

L

L2TP Layer 2 Tunneling Protocol.

LA link alive.

LAN local area network.

LD link description.

LR link record.

LRE long-reach Ethernet

LS link start.

M

MAC address Media Access Control address. The MAC address is the client’s unique hardware number. BBSM uses the MAC address to identify the location (or port) of a client. Once BBSM knows the port that a client is using, BBSM applies the per-port policy to the client’s session.

mapped port The port has an entry in the port_map table. The values in the Room_number and Time_of_last_configure fields may be either default values or updated values.

mapped room Because enterroom.asp has been run successfully from the port, the port's port_map table entry has a correct room number value in the Room_number field and a time/date value in the Time_of_last_configure field.

Mbps Megabits per second (millions of bits per second). Mbps is a measure of bandwidth on a data transmission medium.

MDU multiple dwelling unit.

META tag A special HTML tag that provides information about a web page. Unlike normal HTML tags, meta tags do not affect how the page is displayed. Instead, they provide information such as who created the page, how often it is updated, what the page is about, and which keywords represent the page's content. Many search engines use this information when building their indices.

MFC Microsoft Foundation Classes. MFC is a library of C++ classes that Microsoft developed.

MIB management information base

mixed network BBSM supports networks that contain a mixture of bridged and routed networks by combining bridged and fully routed network associations. Some switches reside on the BBSM server's internal network, and others are accessible through routers on the internal network.

MMC Microsoft management console.

module A software component that implements the functionality of the BBSM system. BBSM supports access policy modules, accounting policy modules, property management system (PMS) modules, and network element modules.

MSDE Microsoft SQL Server Desktop Engine. MSDE is a freely distributable, fully SQL server-compatible database engine without the graphical management tools that accompany an SQL server.

MSSQLServer The MSSQLServer service is the service for the Microsoft SQL Server and MSDE.

MTU multiple tenant unit

multinet A physical network upon which two or more logical networks operate.

N

NAT network address translation. NAT is an Internet standard that enables a LAN to use one set of IP adddresses for internal traffic and a second set of addresses for external traffic. This allows a company to shield internal addresses from the public Internet.

NE network element. An NE is a device connected to the internal network. An end user connects his or her computer to an NE, then BBSM queries the NE to determine the end user's location. You may also see "switch" or "switch stack" used in place of network element. Although, initially, BBSM only supported Ethernet switches, as the product evolved, BBSM added support for cable modem head ends, DSLAMs, and other types of network equipment. For this reason, you may see the word switch used to refer to a device that is not a switch.

NetBIOS Network Basic Input Output System. NetBIOS is a LAN protocol used by Windows computers.

network A network connects all buildings, sites, and ports together with the BBSM server. The network is configured with routers, switches, and other network hardware. BBSM supports bridged networks, fully routed networks, and mixed networks that are combination of bridged and fully routed networks. *See bridged networks, fully routed networks, and mixed networks.*

network byte order The order of bytes in a binary representation of a number as transmitted on the Internet. The most significant byte is first; for example, a 16-bit word representation of "256" would be 0x0100.

network element *See NE.*

network element module BBSM ships with support for several types of network equipment, such as a variety of Ethernet switches, DSL access multiplexers, and cable modem head ends. An integrator can add support for new equipment by writing a network element DLL in C++.

NIC network interface card. The NIC is an adapter card inserted into a computer to provide network communication capabilities. It connects the server to the network. It is also referred to as an Ethernet adapter.

O

Operator A BBSM user who can perform some administrative functions on the BBSM server but does not have access to the full administrative interface. An Operator is allowed to change entries in the port map and access code tables. Operator access is on a per-site basis. *See also Administrator and Reports user.*

outage The duration that the client cannot fully use the BBSM server. The outage can be caused either by an AtDial service restart or by a server reboot. *See service restart* and *server reboot*.

P

PA posting answer.

package file Some page sets define configuration information in a package file, such as DailyHotelPackage.asp. Not all page sets have an associated package file. The package file contains settings to control session behavior, pricing, and bandwidth settings. Other pages within a page set include the package file to gain access to the configuration values. Putting the configuration information in an "include" file eliminates duplication of the configuration information in multiple pages.

page set A set of active server page (ASP) files that the end user is allowed to view and that the administrator specifies on a per-port basis. BBSM restricts the end user from viewing pages that are part of any page set other than the port's allowed page set. BBSM uses Microsoft's ASP technology to implement the page set and ships with several page sets that implement various end user interfaces. Integrators can modify existing page sets (for example, the colors, graphics, and behavior) or create new page sets to create new services.

PAT port address translation. PAT is a form of dynamic NAT that lets you number a LAN with inside local addresses and filter them through one globally routable IPS address.

PDA personal digital assistant. A PDA is a hand-held computer that allows you to store, access, and organize information. Most PDAs work on either a Windows-based or a Palm operating system. PDAs can be screen based or keyboard based, or both.

plug and play A set of features that allows a client to access the Internet without reconfiguring network and browser settings.

PMS property management system. A PMS is a software system used in the hospitality industry to implement customer accounting and billing.

PNF patch information file. A PNF is a text file that contains sections and keys that include all the information that WEBpatch needs to install a patch.

Pocket PC A class of PC devices that has a quarter VGA screen (320 by 240 pixels), or roughly, a device that can fit in your pocket. Pocket PC also refers to one of the Microsoft platforms that are based on the Windows CE operating system and used to develop mobile devices.

policy Any rule that determines the use of resources within the network. A policy can be based on the user, the port, the device, the subnetwork, the network, or the application.

port The jack into which an end user connects a PC to access the Internet. In the case of a wireless network element, such as an Aironet access point, the port is a virtual jack. BBSM allows the administrator to configure the page set and start page on a per-port basis.

port hopping A feature that allows an end user to maintain an active session when moving from port to port.

port ID An identifier that uniquely identifies a network element port within a site. *See port.*

post page A page that processes the information that the end user submits. This page usually makes calls to a SendActivateSession method to activate an end user's session.

PPTP Point-to-Point Tunneling Protocol. Because the Internet is essentially an open network, PPTP is used to ensure that messages are transmitted from one VPN to another. With PPTP, users can dial in to their corporate network through the Internet.

Property Management System *See PMS.*

pre-connect page A web page that implements logic to determine the physical location of the client requesting the page. Used by the policy server to determine the access and accounting policies that apply to a client session.

pseudo-debug A Microsoft Visual C++ project build configuration that generates executables and DLLs that contain symbolic debug information but invoke the release version of the Microsoft memory management library. Release executables and DLLs can invoke pseudo-debug DLLs so developers of pseudo-debug DLLs can debug their DLLs in a release environment.

Q

QoS quality of service. QoS usually refers to the prioritization of packets over a network.

R

RADIUS Remote Authentication Dial-In User Service. RADIUS is a client/server protocol and software that enables network access servers to communicate with a central server to authenticate dial-in users, authorize their access to the requested system or service, and send accounting information about their use of the requested system or service.

redirect The procedure by which a web server tells a web browser to obtain a certain requested page from a different location.

remote client A hardware device, such as a laptop or PC, used by an end user to access a BBSM server from the external network.

Reports A BBSM web application used to display BBSM configuration and logged data.

Reports user A BBSM user who has read-only access to the Reports web applications. This user has more access permissions than an end user but fewer access permissions than an Operator. A Reports user has access to the information for only one site. *See also Operator and Administrator.*

RFC Request for Comments. An RFC is a series of notes on topics concerning the Internet. RFCs can be purely informational, or they can specify a proposed, draft, or approved Internet standard. Online versions of RFCs are available at the following URL: http://www.ietf.org/rfc.html

rogue user An end user who attempts to access the BBSM server fraudulently or maliciously.

routed network In routed networks, some computers cannot communicate with each other directly. Instead, they must send packets through one or more relays, or routers. In a routed network, the only plug-and-play feature that works is redirection of the initial web page request.

RTF Rich Text Format. A Microsoft standard for encoding formatted text and graphics.

RX receive.

S

SDK software developer's kit. An SDK is a set of routines and utilities used to help programmers write an application. The BBSM SDK is used to customize and extend the functionality of the BBSM server.

server reboot In the BBSM system, the situation in which the BBSM server is powered off or shut down for any reason (such as from a power outage, a tripped cord, or installing a patch that requires the server to be rebooted) and the server restarts. When the BBSM server is shut down, clients lose access to the Internet and BBSM services, and active sessions are disrupted. End users are not able to connect to the BBSM server or terminate active sessions. Once the server restarts, clients still may not be able to resume active sessions, because session states are not preserved across server reboots. Even if the session is resumed across a server reboot, the end user may be charged an excessive amount (if the user is charged on a per-minute basis), or the user may not receive fair access to the Internet (if the user is being charged for a block of time), because the duration of the server downtime is not captured.

server-side script A series of statements that a web server executes when a client's browser requests a page.

service restart In the BBSM system, the situation in which AtDial service has stopped for any reason (for example, through WEBconfig) and AtDial service is being restarted and re-initialized. When service stops, clients can still access the Internet. Although active sessions are not disrupted, end users cannot activate new sessions or terminate existing sessions until AtDial is restarted. Session termination can be active (such as the end user's clicking the Disconnect button) or passive (such as the end user's shutting the client down, unplugging the Ethernet connection, or the client's moving out of range). If a client terminates a session when AtDial service is unavailable, the end user may be charged an excessive amount if the user is being charged on a per-minute basis, because the duration of service disruption is not captured.

session In the BBSM system, a set of interactions between an end user and BBSM. The session starts when BBSM serves the start page. At this point, the session is inactive, which means that the user does not have access to the Internet. The session becomes active when BBSM authorizes the user to access the Internet according to the access policy and accounting policy that are specified by the page set. The session ends when AtDial deactivates service for the end user. Note that transactions pertaining to the session can still exist after the session deactivates. These transactions are still associated with that session.

site As used in BBSM documentation, a site is a collection of clients behind switches connected to the Internet through a single network element. It is a subset of the BBSM internal network. Each network element and all its ports are associated with exactly one site. There are always one or more mutually exclusive sites in the BBSM internal network. A site is often at a single geographic location, such as a single hotel or at a large building.

Site Controller Software that runs on a separate machine from the BBSM server. The Site Controller acts as an interface between one or more multiple BBSM servers and a PMS system. This software is used when the PMS system is remote from the BBSM server.

SNMP Simple Network Management Protocol. SNMP is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP allows network administrators to manage network performance, find and solve network problems, and plan for network growth.

SOAP Simple Object Access Protocol. SOAP is an XML-based protocol that enables web services based on a shared and open web infrastructure. It can be used in combination with various Internet protocols and formats, including HTTP, SMTP, and MIME and can support applications such as messaging systems and RPC. *See XML.*

SSL secure sockets layer. SSL is a web encryption protocol for providing secure transactions between a web server and a web browser, such as the transmission of credit card numbers for e-commerce.

start page When an end user's session is inactive, BBSM directs all web access attempts to the start page. It is the first page displayed to the end user when the end user attempts to connect to the Internet. This page usually collects information from the end user using an HTML form. The start page prompts the user to authenticate to become authorized to access the Internet.

subscription A subscription is a period during which BBSM allows the end users to create sessions. If a user attempts to create a session outside any subscription period, BBSM denies the session.

switch A switch is a network device that learns which clients are connected to which ports.

T

tagged format Syntax used to denote the beginning or end of a particular message string, parameter string, or data element.

TCP/IP Transmission Control Protocol/Internet Protocol. TCP/IP is a communications protocol that is the standard protocol of the Internet and the global standard for communications. TCP provides transport functions, which ensures that the total amount of bytes sent is received correctly at the other end. TCP/IP is a routable protocol, and the IP part of TCP/IP provides the routing capability.

TCP port transmission control protocol port. An Internet host can support multiple networking applications, each of which needs a unique identity. An IP address is analogous to a street address with a port number that is like a room number at a specific address.

testing session A set of interactions that a remote user has with a Remote Page Set Test feature on a BBSM server. The testing session starts when the external user begins a remote page set test through the GUI and ends when the user ends a remote page set test through a GUI.

TX transmit.

U

URL uniform resource locator. The address that defines the route to a file on the web or any other Internet facility.

USB universal serial bus.

user A person who uses a hardware device, such as a PC, at a site to access services on the Internet. The term is used interchangeably with end user. *See end user.*

V

VPN virtual private network. VPN is a private network that uses the public Internet to connect some nodes. It maintains privacy by using a tunneling protocol and security procedures.

W

Walled Garden A subset of the Internet accessible to unauthenticated BBSM clients. It allows BBSM users to “try before they buy.” It can include brand recognition or services to the user each time they connect to the Internet.

WEBpatch The web-based utility included with BBSM that allows remote updates to the BBSM server.

web service A programmable entity that provides a particular element of functionality, such as application logic, and is accessible to any number of potentially disparate systems through the use of Internet standards, such as XML and HTTP.

Windows CE A modular, real-time, embedded version of the Windows operating system designed to support small, mobile, 32-bit intelligent devices such as PDAs or, to use the Microsoft term, Handheld PCs.

WISPr Wi-Fi service provider roaming.

WMF Windows Metafile

X

XML extensible markup language. XML is a standard format for data on the web. It allows developers to describe and deliver structured data to and from any application.

XML document An XML element that can, but might not, include nested XML elements. *See XML element.*

XML element An XML element is made up of a start tag, an end tag, and data in between the tags. The start and end tags describe the data within the tags, which is the value of the element. For example, <IP>10.10.10.27<IP> is an XML element. *See XML.*

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W