Cisco BBSM Hotspot 1.0 User Guide

Software Release 1.0
January 2003

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

Customer Order Number: DOC-7815293=
Text Part Number: 78-15293-01

Cisco BBSM Hotspot 1.0 User Guide

Preface

This guide is written for the personnel responsible for configuring and maintaining the Building Broadband Service Manager (BBSM) Hotspot server. After BBSM Hotspot has been configured, it is ready to be used. During daily operation, BBSM Hotspot uses the information provided during configuration to recognize ports, switches, and other related network equipment. The result allows service providers to offer Internet services on a port-by-port basis.

Note The term *customer* refers to the individual or organization that purchased BBSM Hotspot. The term *end user* refers to the customer that is accessing the Internet through the BBSM Hotspot system.

This guide is organized into the following chapters and appendixes.

Chapter/Appendix		
No.	**Title**	**Description**
1	Introduction	Provides an overview of the BBSM Hotspot system.
2	Setting Up BBSM Hotspot	Describes how to configure the BBSM Hotspot software for operation.
3	Advanced Configuration Options	Provides procedures for using the Hotspot Configuration features, configuring individual ports, and using the Custom Web Page Wizard.
4	System Operation	Describes how to perform operational procedures for reporting, creating access codes, and maintenance.
A	Advanced Wizards	Provides step-by-step procedures for running the Address Change Wizard and the Switch Discovery Wizard.
B	Installing an SSL Certificate	Describes how to acquire and install an SSL certificate to provide Internet security through the BBSM Hotspot server.
C	Changing Server Bandwidth Parameter Settings	Provides the procedure for changing the default server bandwidth parameter settings in the registry.

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 ([ ]).

Related Publications

For additional information about BBSM Hotspot, refer to the following documents. Both documents are available online through Cisco.com:

- For assembling BBSM Hotspot, refer to the *Cisco BBSM Hotspot 1.0 Hardware Assembly Guide.*
- For manually creating custom web pages, refer to the *Cisco BBSM 5.2 SDK Developer Guide.*

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

Obtaining Documentation

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

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

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).

You can submit comments to Cisco electronically, by e-mail, or by mail. To submit them electronically, 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. Or submit your comments 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.

Introduction

Cisco BBSM Hotspot is a software-based platform that enables service providers and property owners to offer broadband access services, such as high-speed Internet access, to end users.

BBSM Hotspot was developed to offer a simplified BBSM so that more customers can provide Internet access to consumers and corporate employees who need improved access away from the home or office.

Note SDK software is provided with Cisco's BBSM software product so customers can create custom web page sets and web page policies. Although the guide for the SDK, the *Cisco BBSM 5.2 SDK Developer Guide*, was written to be used with the BBSM software, the appropriate sections of the guide can be used to manually create custom web page sets for BBSM Hotspot, if you choose not to use BBSM Hotspot's Custom Web Page Wizard. The SDK software, however, cannot be used with BBSM Hotspot. Using this software will corrupt the BBSM Hotspot server.

BBSM Hotspot Features

Hotspots are public venues, such as airports, libraries, and coffee shops, where end users can access the Internet at any time. These hotspots must support many end users with a variety of devices, configurations, and security with little or no technical support. To meet these needs and ensure optimal usage and revenue, hotspots need to have the full range of public access features that BBSM Hotspot provides:

- Provides plug-and-play access to public networks so end users can access the Internet without configuring their network devices, such as laptops and handheld devices
- Supports both wired and wireless environments
- Supports multiple authentication and billing options, including credit cards, access codes, and pre- and post-paid accounting through RADIUS
- Supports foreign roaming subscribers from services such as iPass
- Offers multiple bandwidth options
- Supports all VPN clients with simultaneous private and public IP address functionality
- Provides secure local authentication through the Secure Sockets Layer (SSL) protocol

BBSM Hotspot offers three types of deployment options:

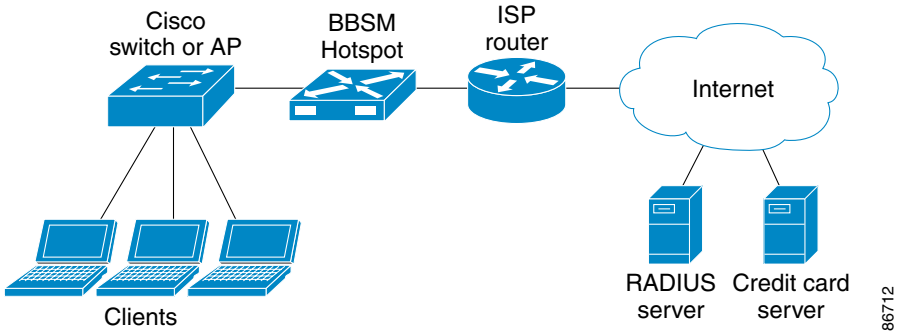
- LRE—Cisco long-reach Ethernet (LRE) switches deliver 5- to 15-Mbps performance over existing Category 1, 2, and 3 wiring. These switches support two types of LRE customer premise equipment (CPE) devices: Cisco 575 and 585 LRE CPEs. The following LRE switches are supported: Catalyst 2912 LRE, 2924 LRE, 2950-24 LRE, and 2950-8 LRE.
- Wireless LAN—BBSM Hotspot supports the Cisco Aironet 340, 350, 1100, and 1200 wireless LAN (WLAN) products.
- Ethernet—Cisco's Ethernet switches include the Catalyst 2950, 3500 XL, 3550, 4000, and 6500 series switches.

The BBSM Hotspot system supports the following types of networks:

- Bridged networks—A centrally located BBSM Hotspot server on a bridged network provides DHCP and static (plug-and-play) support.
- Routed networks—Only DHCP is supported.
- Mixed (integrated routed and bridged) networks

Figure 1-1 shows an example of a simple BBSM Hotspot network.

Figure 1-1 Basic BBSM Hotspot Network



For detailed information about using BBSM Hotspot 1.0 with Cisco networks, refer to the *Cisco BBSM 5.2 User Guide*. The implementation is the same for BBSM Hotspot. For information on obtaining this guide and other Cisco documentation, refer to the Obtaining Documentation section in the preface of this user guide.

BBSM Hotspot Functionality

BBSM Hotspot integrates and manages several key functions:

- Connection—Enables end-user Internet access regardless of the client's network interface configurations. Network deployment options include Ethernet, LRE, and wireless.
- Authentication—Supports multiple authentication methods, such as port-based, RADIUS, and access codes.
- Accounting—Supports accounting and payment methods that include the following:
  - Credit cards—Charge processing by a remote credit card processing service; this enables payment from any location on a property

  - RADIUS—Subscribers or prepaid users can authenticate through RADIUS and pay through offline methods
  - Access codes—End users can use broadband access paid for through access codes
- Portal—Includes a forced portal, walled garden free access, and Start pages that can be customized. BBSM Hotspot redirects end users through two steps during connection:
  - First, they are directed to the Start page, which explains available services, including multiple bandwidth, public and private IP, and price options; walled garden free access areas, such as local sites, advertising, or weather; and a link to the home page of the hotel or property owner.
  - After the end users select and purchase service, they are directed to a portal page as their first Internet site. This page provides you with a second marketing opportunity.
- Bandwidth options—Supports multiple options, including bandwidth throttling.
- Network buildout and configuration—Includes multiple features to support network installation, configuration, and testing.

Setting Up BBSM Hotspot

This chapter provides step-by-step procedures for setting up BBSM Hotspot. After you complete the procedures in this chapter, your BBSM Hotspot server should be fully operational.

The following two chapters, Chapter 3, "Advanced Configuration Options," and Chapter 4, "System Operation,", provide more detailed information and advanced options for configuring and using BBSM Hotspot.

Read the Before You Start section, then follow the step-by-step procedures to set up your BBSM Hotspot.

Before You Start

This section describes the prerequisites that you need to complete or check before setting up the software. After running the Setup Wizard in this chapter, you perform all operations from the Dashboard.

Before you configure BBSM, make sure that you complete the following tasks:

- First, read the ReadMeFirst web page, which launches the first time you start your BBSM Hotspot server.
- Then, read the first chapter to this guide, and the cautions below to avoid costly problems.
- From your BBSM Hotspot server desktop, open the BBSM Hotspot Configuration Requirements Checklist and complete it to make sure that you have all of the networking information you need to configure your server.
- Assemble the BBSM Hotspot server using the instructions in the *Cisco BBSM Hotspot Hardware Assembly Guide*. For information on obtaining this guide and other Cisco documentation, refer to the Obtaining Documentation section in the preface to this user guide.
- If you will be using secured (https) pages, obtain and install a Certificate Authority (third-party SSL). (Refer to Appendix B, "Installing an SSL Certificate.")

- Before beginning the basic configuration of your BBSM Hotspot 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 Hotspot server. For instructions on performing these installations, refer to Chapter 4, "System Operation."

Caution Do not change the Windows 2000 computer name of your BBSM Hotspot server, because the BBSM Hotspot MSDE database has the name embedded in the application. Changing the name breaks MSDE functionality, and you will see SQL server errors reported on your BBSM Hotspot server. This problem is a Microsoft issue and not one that the Cisco software team can change.

Caution We recommend using the latest version of Internet Explorer to perform functions accessed through the BBSM Hotspot Dashboard.

Caution When running the wizards, making any changes to BBSM Hotspot, or rebooting the BBSM Hotspot server, make sure that there are no active sessions. The Client Deactivation tool, located on the Dashboard, can be used to deactivate any active sessions.

Running the Setup Wizard

This section explains how to configure the BBSM Hotspot server by using the Setup Wizard. This wizard prompts you for your server's basic configuration parameters and then configures the server with these settings.

It also prompts you to decide if you would like to create a custom web page at this time:

- If you decide to use a custom web page, the Custom Web Page Wizard launches after the Setup Wizard completes.
- If you decide not to create a custom web page, the first time you run the Setup Wizard, it applies the FreeAccess web page to all ports. If you run the Setup Wizard again at a later time, it will not change the port settings.

Note the following configuration and custom web page options that you can use:

- To configure your server using the Address Change Wizard and Switch Discovery Wizard, refer to Appendix A, "Advanced Wizards."
- To configure your server manually on a per-port basis or change your configurations after the initial setup, refer to Configuring Your Server (Hotspot Configuration), page 3-1.
- To change your port settings after the initial setup, refer to Configuring Ports (Port Configuration), page 3-27.
- To create a custom web page after the initial setup, refer to Adding Custom Web Pages to BBSM Hotspot, page 3-24.

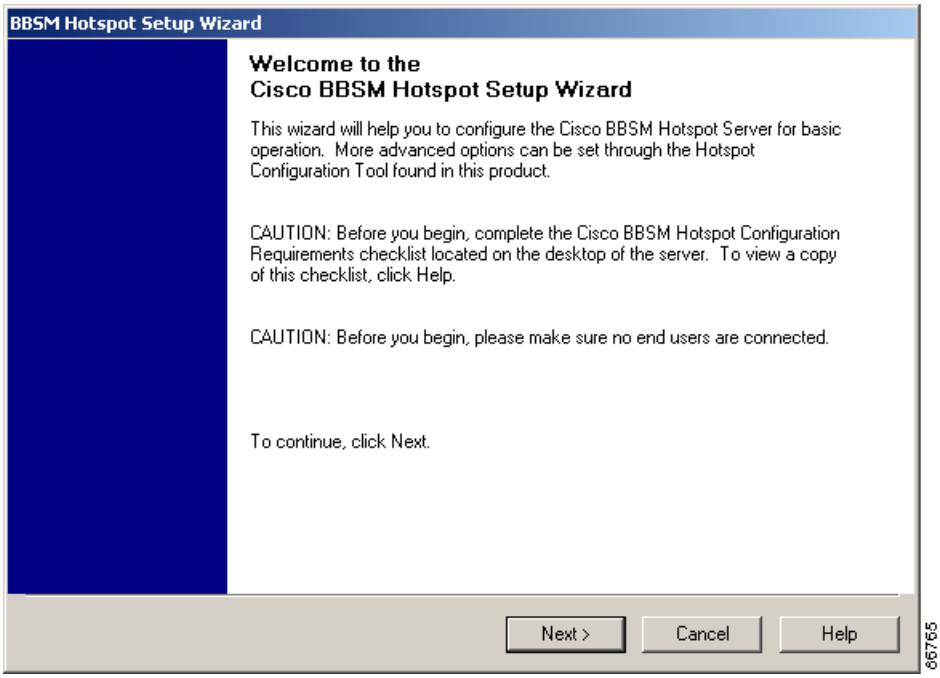
Note Be sure to complete the BBSM Hotspot Configuration Requirements Checklist before running the Setup Wizard.

Caution Be sure to disconnect all active end-user sessions before running any BBSM Hotspot wizard, including the Setup Wizard. Refer to the "Deactivating Client Sessions" section on page 4-21.

Follow these steps to run the wizard.

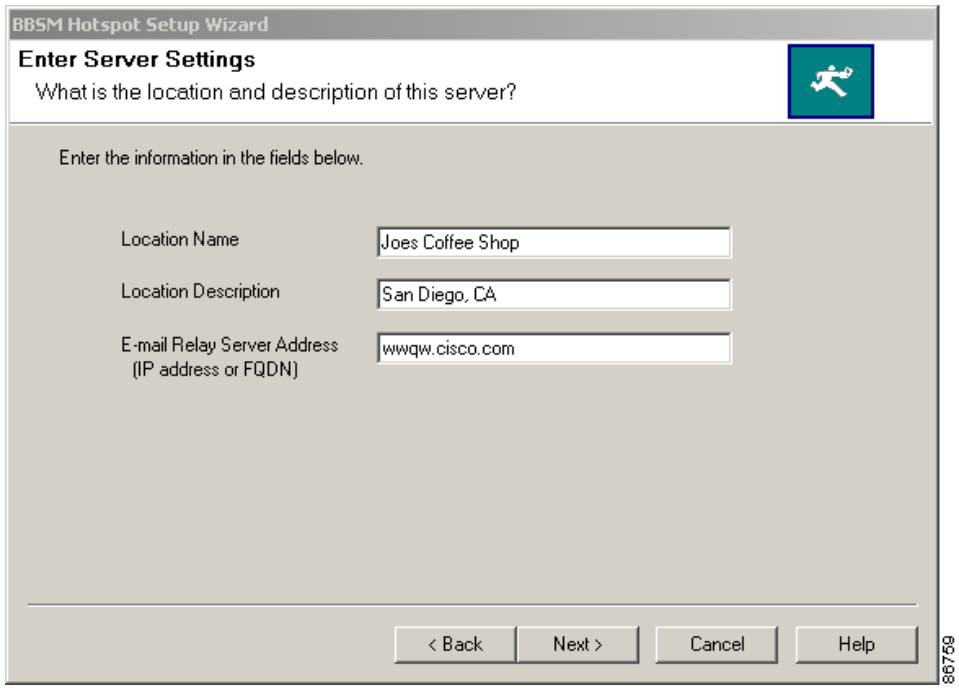
Step 1 From the Windows desktop, double-click the **BBSM Hotspot Setup Wizard** icon. (From the Windows desktop, you can also choose **Start > BBSM Hotspot Wizards > BBSM Hotspot Setup Wizard**.) The BBSM Hotspot Setup Wizard Welcome window appears. (See Figure 2-1.)

Figure 2-1 BBSM Hotspot Setup Wizard Welcome Window



Step 2 Click **Next.** The Enter Server Settings window appears. This window lets you enter location information and the server address for relaying e-mail messages sent out through BBSM Hotspot. (See Figure 2-2.)

Figure 2-2 Enter Server Settings Window



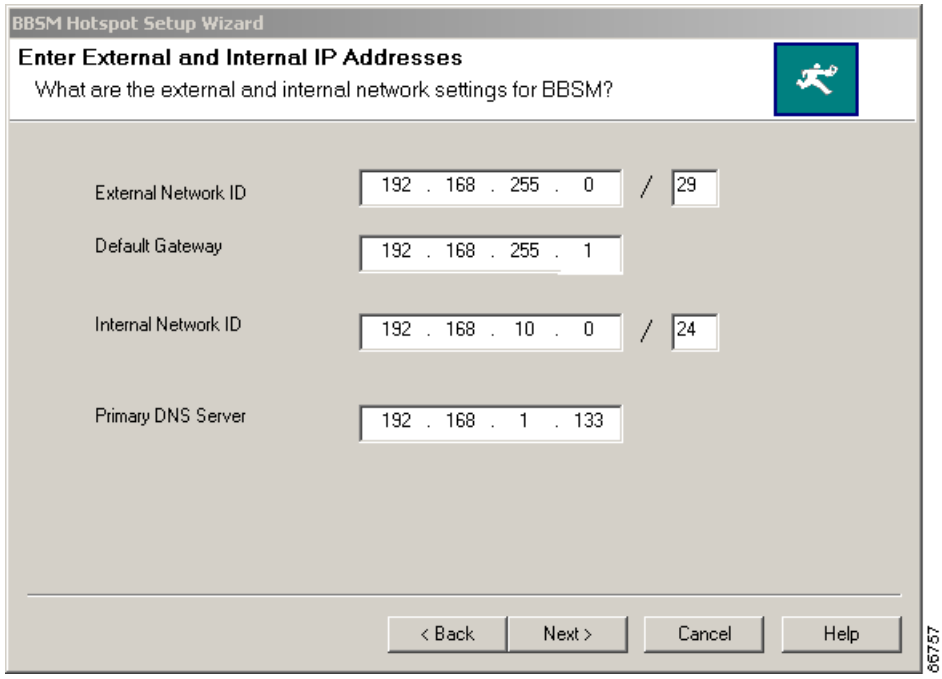
Step 3 Enter the field data, as described in Table 2-1. This location data is used globally by BBSM Hotspot.

Table 2-1 Enter Server Settings Field Descriptions

Field	Description
Location Name	Enter a specific property name. Use up to 50 alphanumeric characters, such as “Joes Coffee Shop” or “2nd Level Conference Rooms.” This field is required.
Location Description	Enter descriptive text for the location, such as the city or address. You can use any alphanumeric word or phrase to a maximum of 100 characters, such as “San Diego, CA,” or “Guest cubicles in the northeast annex.” This field is optional.
E-mail Relay Server Address (IP address or FQDN)	Enter the IP address or the fully qualified domain name (FQDN) for the e-mail relay server that is used by your Internet service provider (ISP) to forward non–web-based e-mail, such as Microsoft Outlook or Eudora mail programs, from public locations. An example FQDN is www.ispemail.com. The FQDN can contain a maximum of 100 characters. This field is optional. Use it only if you want to provide your end users with e-mail support. Typical e-mail servers block traffic from unknown sources for security purposes. The BBSM Hotspot server, as with any public location, is considered an unknown source that requires an e-mail relay server to forward end-user mail.

Step 4 Click **Next**. The Enter External and Internal IP Addresses window appears. (See Figure 2-3.)

Figure 2-3 Enter External and Internal IP Addresses Window



Step 5 Enter the IP addresses, as described in Table 2-2. The wizard uses this data to determine BBSM Hotspot external and internal NIC addresses, the router address, and allocation of the network device, static, and DHCP client address pools. Note that the wizard requests the external and internal network IDs and subnet masks and then calculates the external and internal IP addresses automatically. Obtain the network IDs from your ISP. (An internal network of size Class C or smaller is supported.)

Table 2-3 shows the number of IP addresses available to you based on the subnet code number you enter after the slash. The table shows the subnet codes that you would most likely use.

Table 2-2 Enter External and Internal IP Addresses Field Descriptions

Field	Description
External Network ID	Enter the external network IP address block assigned by your ISP. The number after the slash is the subnet code for the number of IP addresses available in the block.
Default Gateway	*This IP address is automatically generated based on the external network ID that you entered. You cannot change the first three sets of numbers in this address.* This IP address is the address of the gateway (router) assigned by the ISP and used to access the Internet. Here's what can and cannot be changed in this field: • You cannot change the first three sets of numbers in the IP address. • The fourth set defaults to the number 1. You can change this fourth octet after the Setup Wizard populates the Default Gateway based on the External Network ID. Your router needs to be configured for the internal network to point to the external NIC of the BBSM Hotspot server. If you are using a private IP address, you will also need to create a network address translation (NAT) pool for end users and one-to-one NAT statements for remote access to internal network devices.
Internal Network ID	This is the Network ID for the subnet that end users use to connect to the BBSM Hotspot network and, through it, the Internet. The internal subnet consists of the network devices, end-user clients (such as laptops and PDAs), and the BBSM Hotspot internal NIC. The number after the slash is the subnet code for the number of IP addresses available in the block. You can enter your own private network ID, or you can input a public network ID.
Primary DNS Server	Enter the IP address for the primary domain name system (DNS) server provided by your ISP. Because BBSM Hotspot is not configured as a DNS server, DNS forwarding is enabled to forward all DNS requests to a remote DNS server. BBSM Hotspot acts as a DNS forwarder for end-user DNS requests as well as its own DNS requests. These requests, such as www.cisco.com, are resolved into IP addresses so the Internet routers can locate the web server with the content.

Table 2-3 Subnet Code Conversions

Subnet Code	Number of IP Addresses
/29	6
/28	14
/27	30
/26	62
/25	126
/24	254

Step 6 Click **Next**. The Calculating TCP/IP Addresses window appears. BBSM Hotspot uses the information provided in the Enter External and Internal IP Addresses window to calculate TCP/IP addresses for the server.

Note If you need to change the IP addresses of the NICs from the defaults generated by the Setup Wizard, you must use the Address Change Wizard to make these changes. Continue with and complete the Setup Wizard, then use the Address Change Wizard to change the NIC addresses to the desired settings. Refer to the "Running the Address Change Wizard" section on page A-1.

(See Figure 2-4 and Table 2-4 for field descriptions.)

Figure 2-4 Calculating TCP/IP Addresses Window

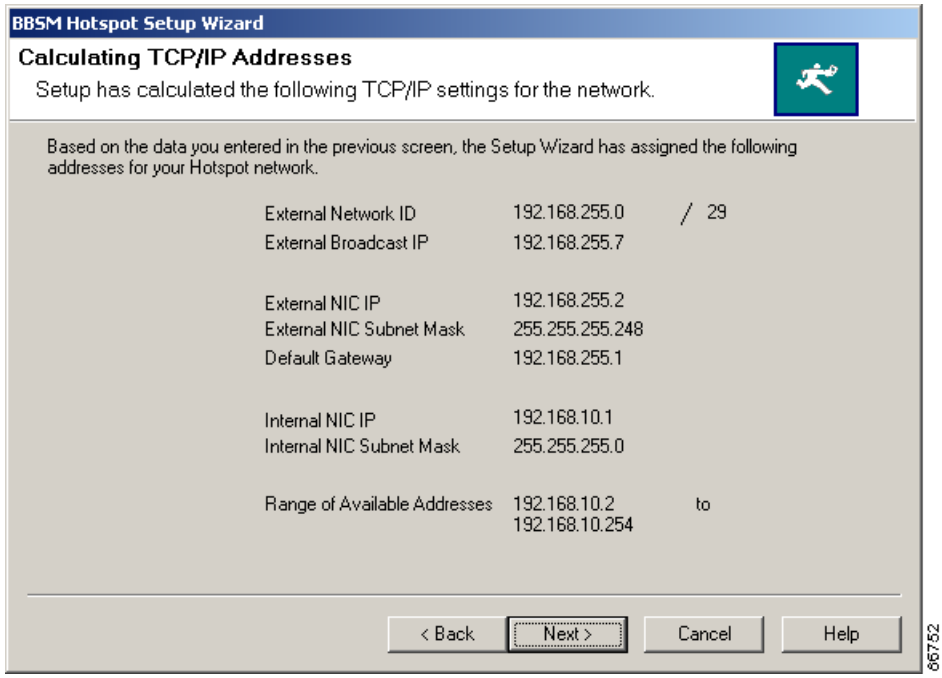


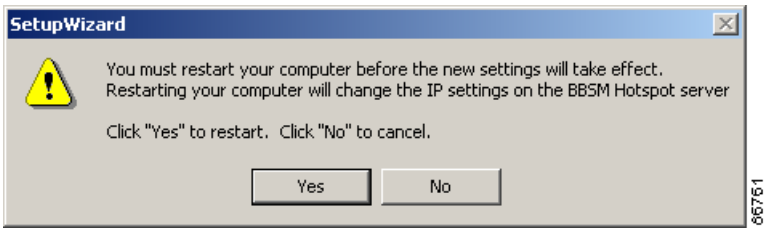
Table 2-4 BBSM Hotspot Setup Wizard, Calculating TCP/IP Addresses Field Descriptions

Field	Description
External Network ID	The network ID used for your BBSM external network.
External Broadcast IP	The IP address used to broadcast data within the external network.
External NIC IP	The IP address of the external NIC on BBSM Hotspot. BBSM Hotspot assigns the first host address that is not the default gateway, as calculated from the External Network ID field in Step 5.
External NIC Subnet Mask	The subnet mask calculated from the External Network ID subnet code (after the slash) in Step 5.
Default Gateway	The default gateway address entered in the Default Gateway field in Step 5.
Internal NIC IP	The IP address on the internal NIC on BBSM Hotspot, as calculated from the Internal Network ID in Step 5. It is set to the first host address calculated from the Internal Network ID.
Internal NIC Subnet Mask	The subnet mask on the internal NIC, as calculated from the Internal Network ID subnet code (after the slash) in Step 5.
Range of Available Addresses	The range of IP addresses available for internal network devices and end-user connections on the internal network. The range is from the second host ID through the last host ID calculated.

Step 7 Click **Next**. The Restart Computer dialog box appears on top of the Setup Wizard. This dialog box gives you the option to restart BBSM now or cancel. (See Figure 2-5.) You must restart or reboot for the IP address settings to take place. If you do not restart, you cannot continue with the setup.

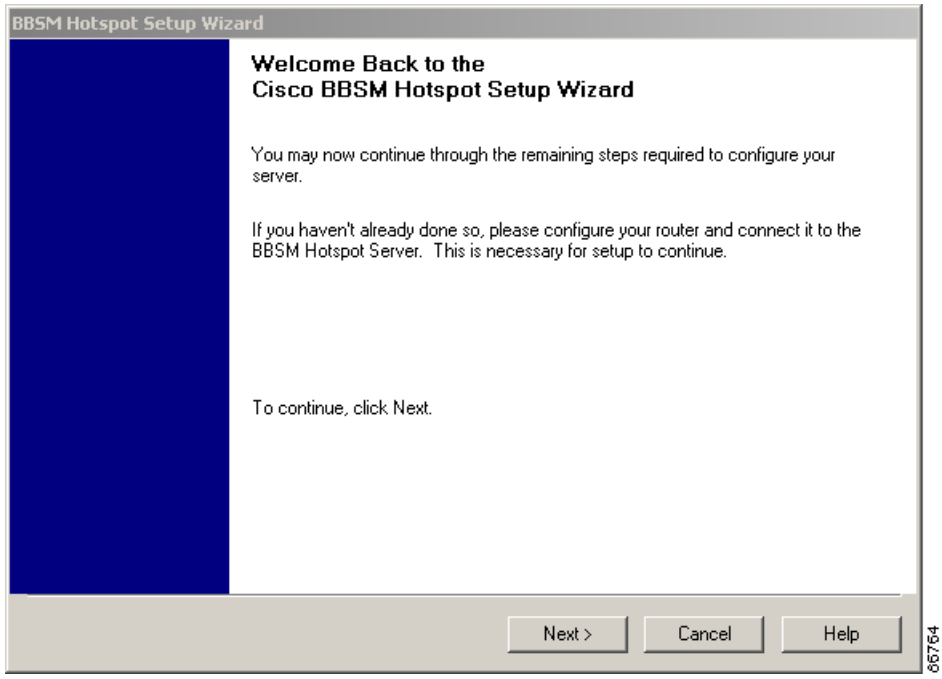
Caution Restarting the BBSM Hotspot server at this point will save all of the settings entered for your server up to this point. Click **No** to close the dialog box, which returns you to the Calculating TCP/IP Addresses window. If you click Cancel at any point after the restart, the server settings and IP addresses that you have entered at this time will be retained, while settings entered after the restart will be cancelled. If you run the Setup Wizard a second time and do not change the IP address settings (a reboot is unnecessary), if you click Cancel, all settings entered at that time, including the server settings, will be cancelled.

Figure 2-5 Restart Computer Dialog Box



Step 8 For the IP address configuration settings to take effect, click **Yes**. The BBSM Hotspot server configures the new settings, then restarts. After you log in to BBSM Hotspot as Administrator, the Welcome Back window appears. (See Figure 2-6.)

Figure 2-6 Welcome Back Window

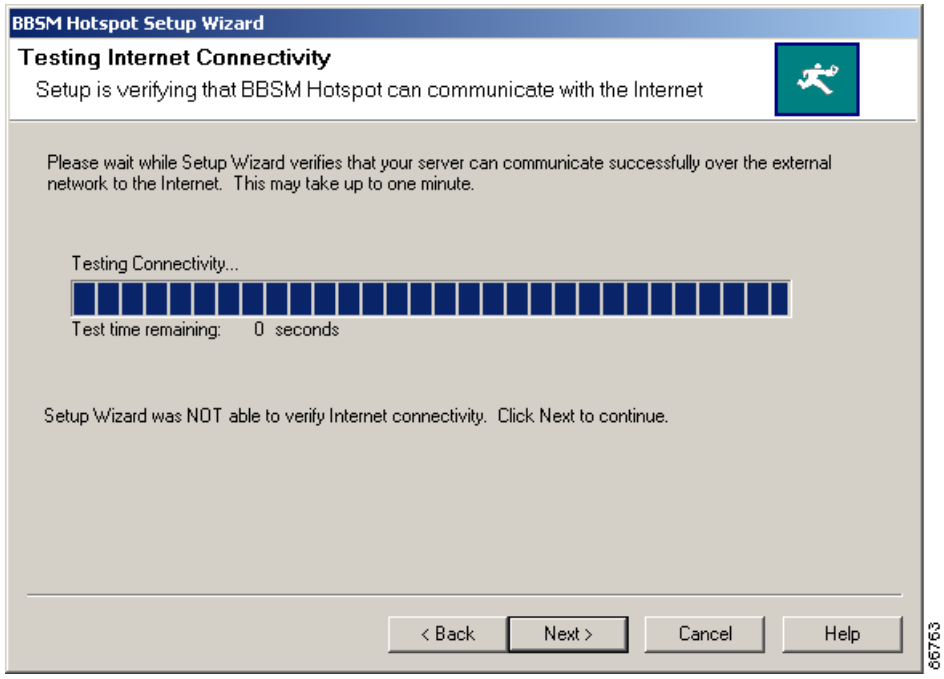


Caution Before continuing, make sure that your router is configured and connected to the Internet.

Step 9 Click **Next**. The Testing Internet Connectivity window appears and begins testing the connection from BBSM Hotspot through the router to the Internet. A progress bar shows the test time remaining. The test should take less than a minute. The Back and Next buttons are disabled until the test is complete. (See Figure 2-7.)

- If the test is successful, a Test Success window pops up with a message telling you that the connection test was successful. Click **OK** to close the window, then go to Step 11.
- If the test was unsuccessful, this message appears on the Testing Internet Connectivity web page: "Setup Wizard was NOT able to verify Internet connectivity. Click Next to continue." Go to Step 10.

Figure 2-7 BBSM Hotspot Setup Wizard, Testing Internet Connectivity Window



Step 10 Click Next. The Test Failure window appears (Figure 2-8) and provides you with options. Note the following reasons that the test may have failed and the options for correcting errors:

- Failure to communicate with the default gateway IP address:
  - Verify the physical connection from BBSM Hotspot to the router.
  - Make sure that a cross-over cable has been used.
  - Verify that the link status light is on for both the internal connection of the router and the BBSM Hotspot external NIC.
  - Verify that the router IP address was configured correctly. You may need to contact your ISP so they can verify this setting.
- Failure to communicate with the DNS server IP address:
  - Verify the physical connection from the router to the Internet.
  - Verify that the link status light is on for the external connection of the router.
  - Verify that the ISP provided the correct DNS address and that it was entered correctly.
  - Contact the ISP to verify this address.
- Failure to resolve the DNS name: www.yahoo.com—Contact the ISP to verify that the DNS is operational.

The following are the options available to you from the Test Failure window:

- Check your physical connections. Then click **Back** to rerun the test.
- After the question asking if you want to change your IP addresses, click **Yes**. Then click **Next** to continue. You are returned to the Enter External and Internal IP Addresses window where you can enter new IP addresses. Then continue with the setup.

- After the question asking if you want to change your IP addresses, click **No** to ignore the connectivity issues and continue with the setup. A warning message pops up to tell you that you must resolve the IP address issue for BBSM Hotspot to work properly. (See Figure 2-9.) You are then taken to the Enter Network Device Configuration Parameters window. (See Figure 2-10.)
- Click **Cancel** to stop the setup.

Figure 2-8 Test Failure Window

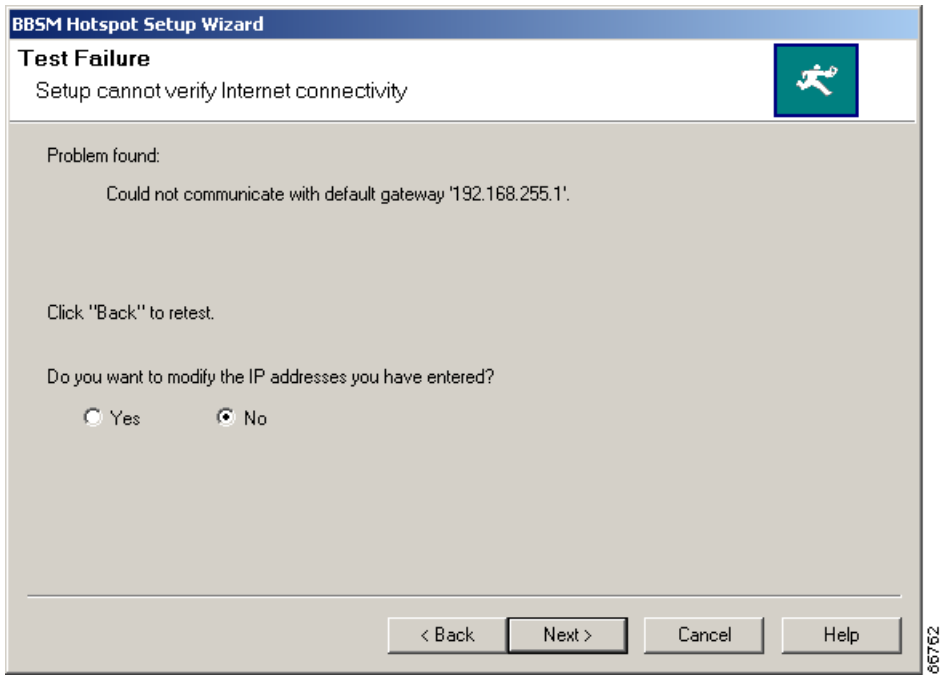
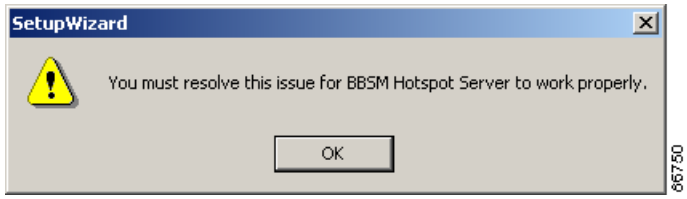
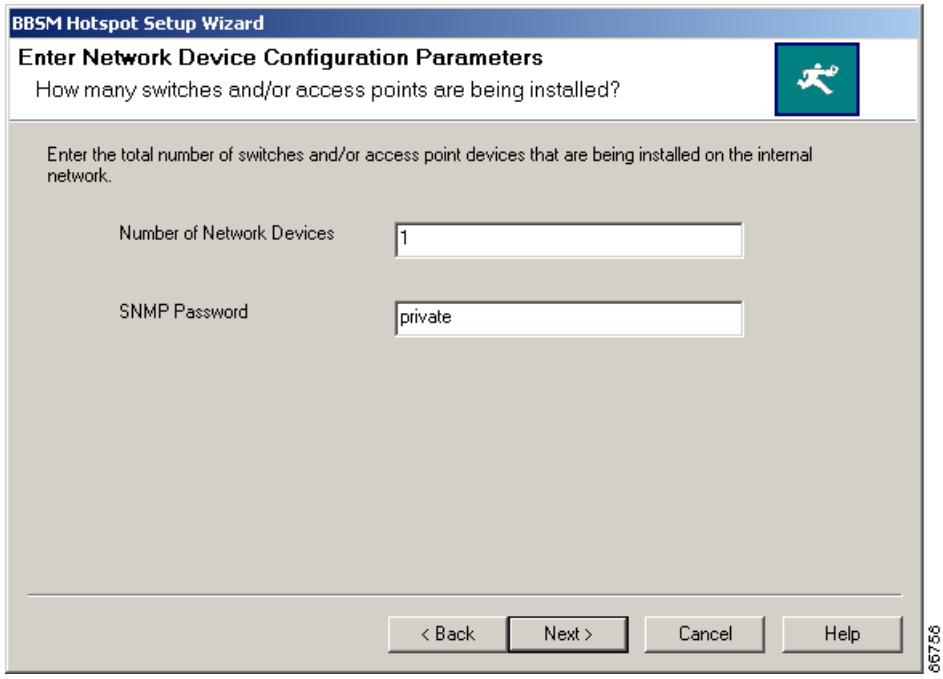


Figure 2-9 You Must Resolve This Issue Dialog Box



Step 11 Click **Next**. The Enter Network Device Configuration Parameters window appears. (See Figure 2-10.)

Figure 2-10 Enter Network Device Configuration Parameters Window



Step 12 Enter the network device parameters, as described in Table 2-5. The wizard uses this data to determine the number of IP addresses to allocate to the network device range. (This may have been familiar to current BBSM customers as the "Management Range.") This information will also be used in the switch discovery part of the wizard.

Table 2-5 Enter Network Device Configuration Descriptions

Field	Description
Number of Network Devices	Enter the total number of switches and wireless access points that will be installed on the BBSM internal network. You can also enter a larger number than the current amount of network devices in anticipation of additional devices in the future.
SNMP Password	Enter the SNMP password that is used to access network devices. BBSM Hotspot needs this information to run switch discovery. Note that on Cisco Catalyst switches, the SNMP password is also known as the SNMP community read/write string.

Step 13 Click **Next**. The Calculating Internal Network Address Ranges window appears, providing you with a list of the internal IP address ranges that have been calculated and assigned by the BBSM Hotspot server. These include the following:

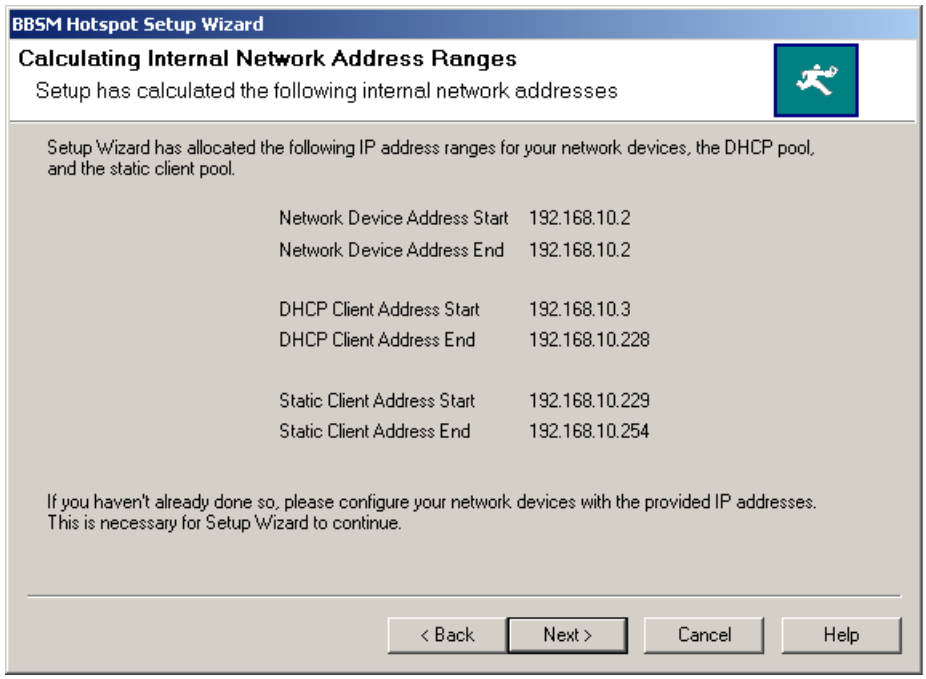
- Network Device Addresses—These addresses are allocated to the network devices. This address range is allocated from the "Number of Network Devices" number entered in Step 12.

Caution The IP addresses of your switches and access points must be set to addresses that are within this Network Devices Address range. To increase performance, we recommend using the numbers in this range consecutively so that any unused IP addresses are at the end of the range.

- DHCP Client Addresses—These addresses are allocated to the DHCP client address pool. Because most network devices are configured as DHCP, after the BBSM NIC and the network device addresses have been allocated, BBSM Hotspot allocates 90 percent of the available end-user addresses to the DHCP pool. You can modify this address range in the Hotspot Configuration tool on the Dashboard or by using the Address Change Wizard.
- Static Client Addresses—These addresses are allocated to the statically configured client address pool. Because static configurations are not common, this range is allocated by BBSM Hotspot to 10 percent of the total remaining pool after the BBSM NIC and the Network Device addresses have been allocated.

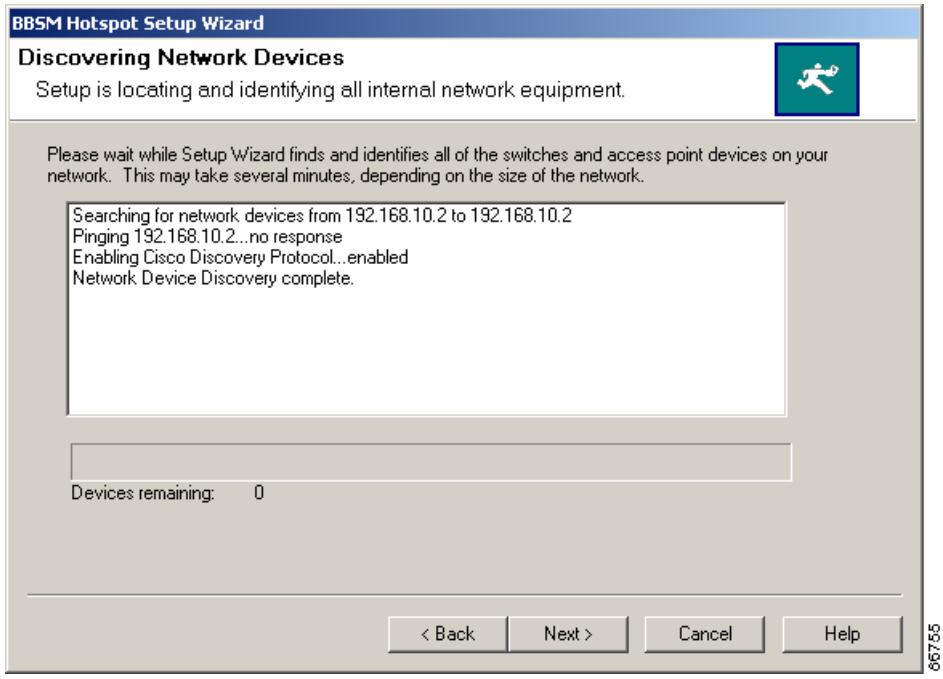
(See Figure 2-11.)

Figure 2-11 Calculating Internal Network Address Ranges Window



Step 14 Click **Next**. The Discovering Network Devices window appears, showing that BBSM Hotspot is running switch discovery to find network devices connected to the BBSM Hotspot internal network. (See Figure 2-12.) As each device is discovered, BBSM Hotspot is automatically configured to work with the device. The progress bar shows the number of devices found based on the number entered in Step 12. The Back and Next buttons are disabled until the process is complete.

Figure 2-12 Discovering Network Devices Window



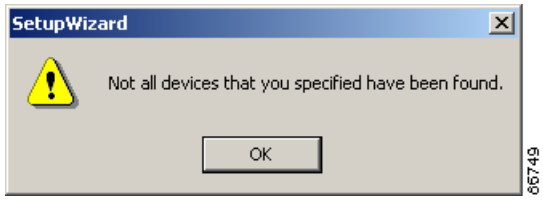
When discovery is complete, two scenarios are possible:

- If all of the network devices were found, a dialog box appears, telling you that network discovery is complete. (See Figure 2-13.) Go to Step 16.

Figure 2-13 Network Discovery Complete Window

- If some of the network devices were not found, a dialog box appears, telling you that not all of the devices could be found. (See Figure 2-14.) Go to Step 15.

Figure 2-14 Devices Not Found Window



Step 15 Click **OK**. The Discovering Network Devices Results window appears, listing discovery results and a summary of devices found. If the wizard located less devices than you entered in the "Number of Network Devices" field in Step 12, BBSM Hotspot shows the reduced number that were found. The reasons for the discrepancy can include the following:

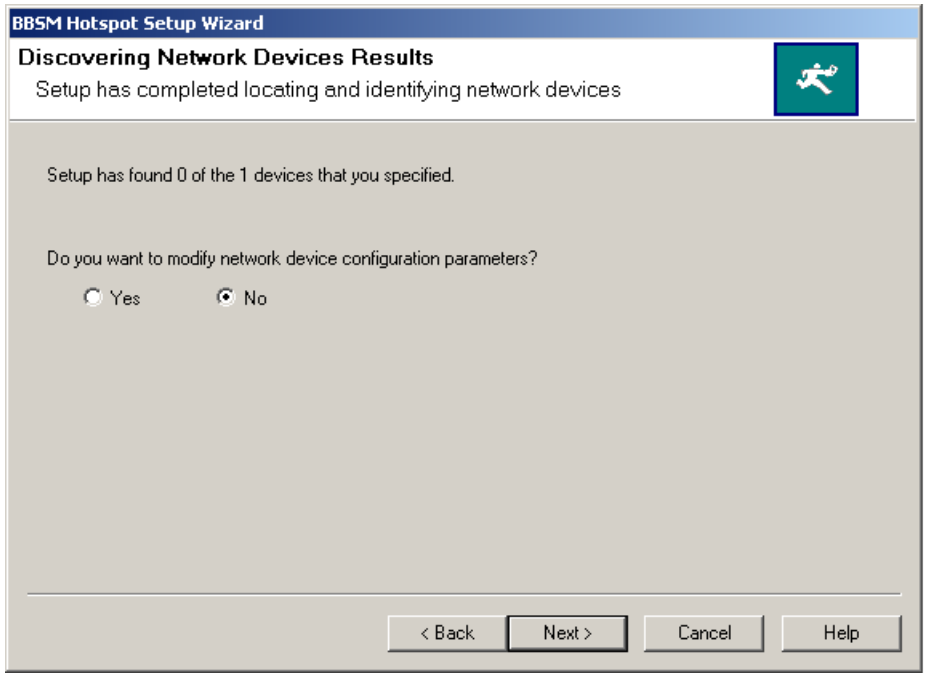
- Intentional discrepancies may exist, because addresses were included for future system growth.
- The physical connections may be faulty.
- The IP address and SNMP password may not be configured correctly.
- The correct network device cannot be found for each IP address.

You are asked if you want to change the network device configuration parameters:

- Click **Back** to make corrections, such as reconnecting a cable, then retest the server. Then continue with the setup.
- To change your network device data, click **Yes**. Then click **Next** to continue. You are returned to the Enter Network Device Configuration Parameters window where you can change the network device data. Then continue with the setup.
- If you choose not to change your network device data; for example, if you assigned additional addresses for future system growth, click **No** to ignore the discrepancy and continue with the setup.
- Click **Cancel** to stop the setup.

(See Figure 2-15.)

Figure 2-15 Discovering Network Devices Results Window



Step 16 Click **Next**. The Create Custom Web Page window appears. The wizard prompts you to decide if you want to create a custom web page now or use the default web pages that ship with BBSM Hotspot:

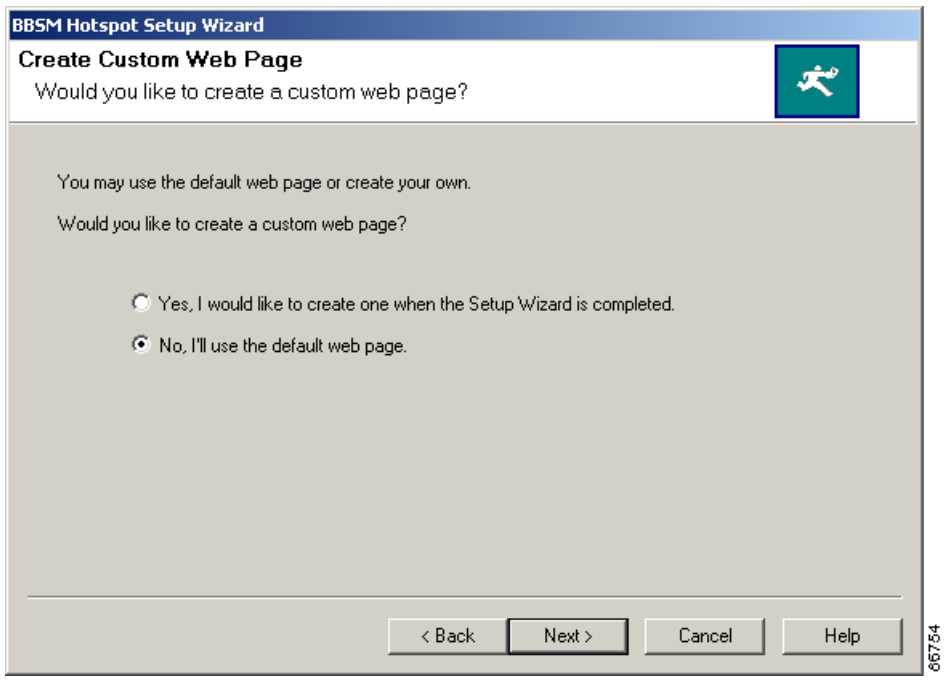
- Click **No** to use the BBSM Hotspot default web pages. The Setup Wizard generates a generic FreeAccess web page to all ports. If you do not want to create a custom web page at this time, you can create one later by using the Custom Web Page Wizard. The custom web page can then be enabled on a per-port basis by using the Port Configuration tool on the Dashboard.

  Note The first time you run Setup Wizard, it sets all ports to free Internet access. If you run the Setup Wizard again at a later time, it will not change the port settings.

- Click **Yes** to complete the Setup Wizard, then launch the Custom Web Page Wizard to create a custom web page at this time. Creating a custom web page allows you to provide a welcome message, instructions, and branding information to your end users.

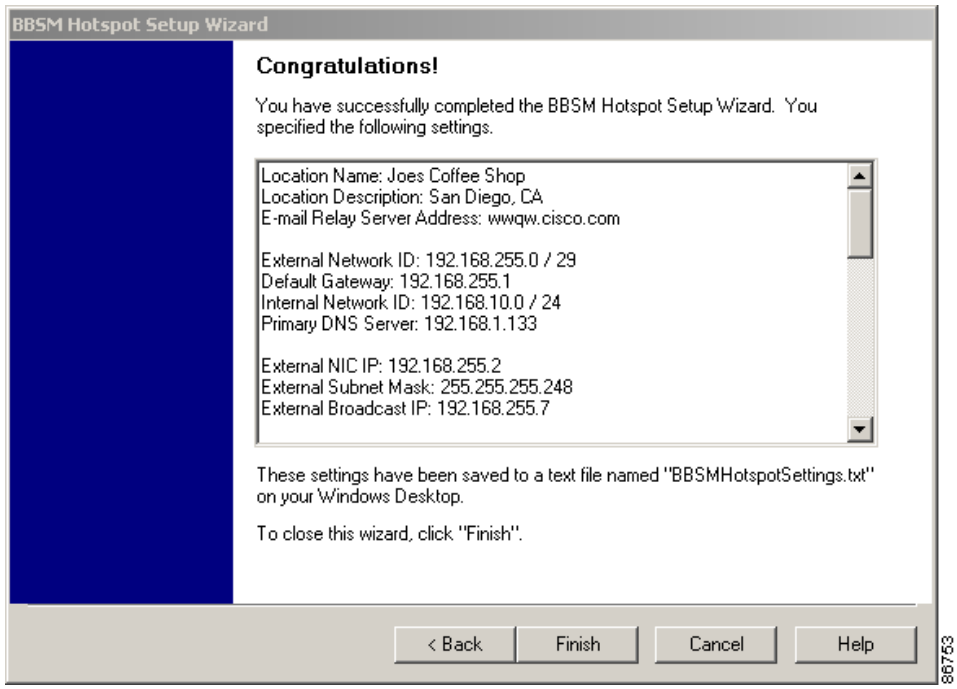
(See Figure 2-16.)

Figure 2-16 Create Custom Web Page Window



Step 17 Click **Next**. The Congratulations window appears, showing the configurations that you set. The Setup Wizard saves these settings to a text file named "BBSMHotspotSettings.txt on the Windows desktop. (See Figure 2-17.)

Figure 2-17 Congratulations! Window



Step 18 Click **Finish**:

- If you chose to create a custom web page, the Setup Wizard launches the Custom Web Page Wizard.
- If you chose to use the default web page that the Setup Wizard creates, the Setup Wizard closes.

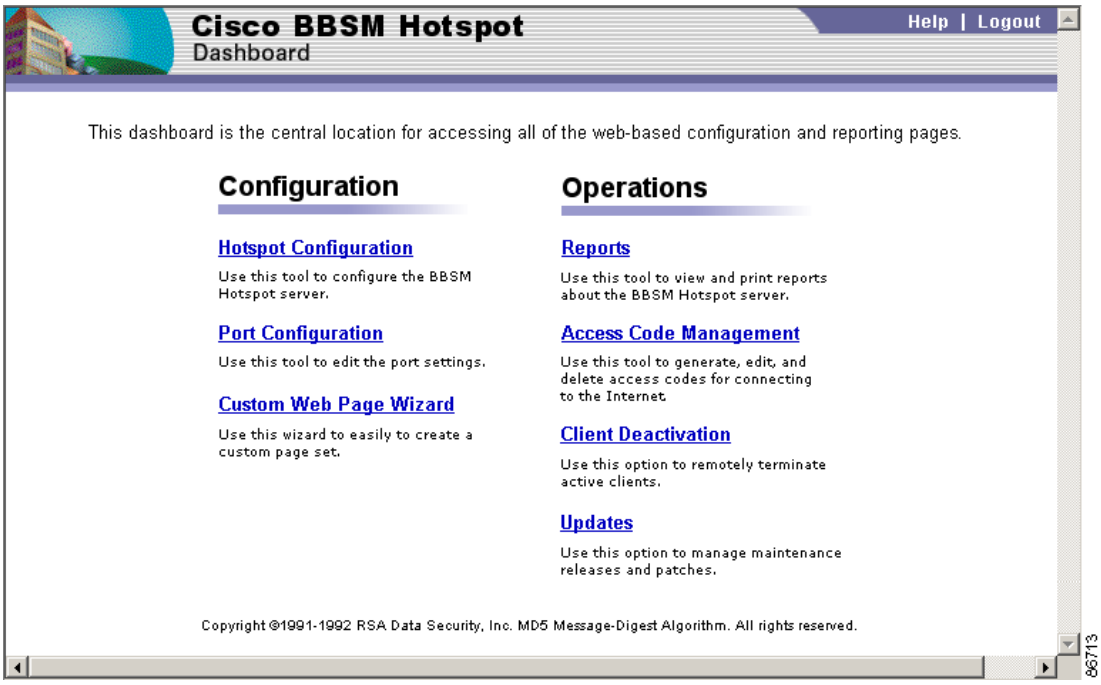
Understanding the BBSM Hotspot Dashboard

The BBSM Hotspot Dashboard comprises two primary components—Configuration and Operations, from which an administrator can perform all system functions. These functions include configuring the system, performing all system operations, managing and updating the system, and reporting. The Dashboard and the two components are described in the sections that follow.

Dashboard Access

The Dashboard is the BBSM Hotspot home page for accessing BBSM Hotspot options. (See Figure 2-18.)

Figure 2-18 Dashboard

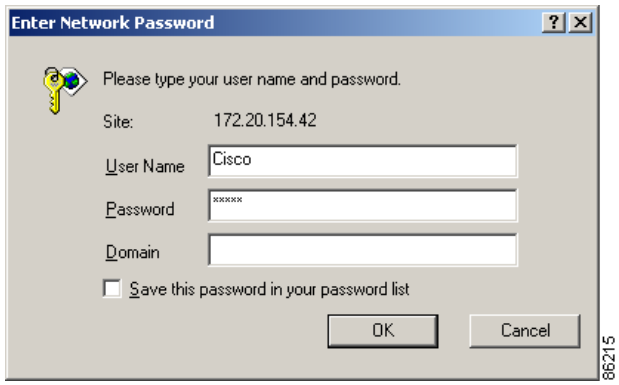


You can access the Dashboard locally or remotely:

- To access the Dashboard locally, at the BBSM Hotspot console, double-click the Dashboard icon on the desktop. The Dashboard appears. You can also choose **Start > BBSM Hotspot Dashboard**.
- To access the Dashboard remotely, launch Internet Explorer to access the BBSM Hotspot server on port 9488 instead of through the default web server port 80, as shown below. Use one of the following IP addresses:
  - If you are accessing BBSM Hotspot from a remote location, enter BBSM Hotspot's external IP address: **http://<external_NIC_address>:9488/www**, where <external_NIC_address> is the external NIC address of the BBSM Hotspot server you want to access; for example, type **http://192.168.38.1:9488/www**, and press **Enter**. The Enter Network Password dialog box appears. (See Figure 2-19.)
  - If you are accessing the BBSM Hotspot server within BBSM Hotspot's subnet, enter the BBSM Hotspot server's internal IP address: **http://<internal_IP_address>:9488/www**, where <internal_IP_address> is the internal IP address of the BBSM Hotspot server you want to access; for example, type **http://192.168.10.1:9488/www**, and press **Enter**. The Enter Network Password dialog box appears. (See Figure 2-19.)

    Note To access the Dashboard from BBSM Hotspot's internal subnet, the end user's client must have either an IP address in the Network Devices address range or an active BBSM Hotspot session. If neither of these is true, the end user will be redirected to the Start page for the port that they are connected to.

Figure 2-19 Enter Network Password Dialog Box



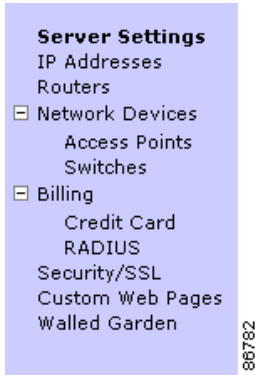
– When you access the Dashboard remotely, you are prompted for a username and password. (Leave the domain name blank.)

Configuration

The following three Administration options allow an administrator to perform all configuration tasks:

- Hotspot Configuration—Use this tool to configure the BBSM Hotspot server. Figure 2-20 shows the functionality accessed through the Hotspot Configuration navigation bar (NavBar).

Figure 2-20 Hotspot Configuration NavBar



- Port Configuration—Use this tool to change port settings.
- Custom Web Page Wizard—Use this wizard to create a customized end-user web pages.

The Hotspot Configuration web page options are described in Table 2-6.

Table 2-6 Hotspot Configuration Web Page Options

Web Page	Description
Server Settings	Configures server-wide settings such as bandwidth throttling and the e-mail server IP address.
IP Addresses	Configures the IP address ranges for the BBSM Hotspot server and the network devices.
Routers	Sets router interface parameters. Configures routes to the switches and to the clients attached to these switches. (This feature is for routed networks and is not related to WAN activities.)
Network Devices	Expands to the Access Points and Switches web pages: • Access Points—Sets the access point parameters, such as access point IP address and access point type. • Switches—For a particular cluster and switch number, sets the switch parameters, such as number of client ports, cluster IP address, router IP address, and Cisco switch type. Note that each cluster can support up to 16 cluster-capable switches.
Billing	Expands to the RADIUS and Credit Card web pages, which define the billing features: • Credit Card—Configures the credit card server parameters and the merchant ID number. • RADIUS—Configures the RADIUS server parameters and the ability to have multiple concurrent RADIUS sessions.
Security/SSL	Configures the domain name for SSL web pages and enables changes to the MSDE ‘sa’ password.
Custom Web Pages	Adds your new custom web pages and sets the associated Start page. The web page then appears in the Web Page drop-down menu when configuring port settings from the Access Points or Switches web page.
Walled Garden	Configures the desired walled garden web sites, which let the end user view the web sites that you specify free of charge.

Operations

The following are the options available under the Operations section of the Dashboard:

- Reports—Use this tool to view and print reports about the BBSM Hotspot server.
- Access Code Management—Use this tool to generate, edit, and delete access codes for connecting to the Internet.
- Client Deactivation—Use this option to remotely terminate active client sessions.
- Updates—Use this option to install maintenance releases (service packs) and patches.

Using Navigation Buttons

BBSM Hotspot web pages use navigation buttons to help you locate information. Use the navigation buttons to locate the correct record before making changes. (See Table 2-7.)

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

Table 2-7 Navigation Button Descriptions

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

Connecting a Client to BBSM Hotspot

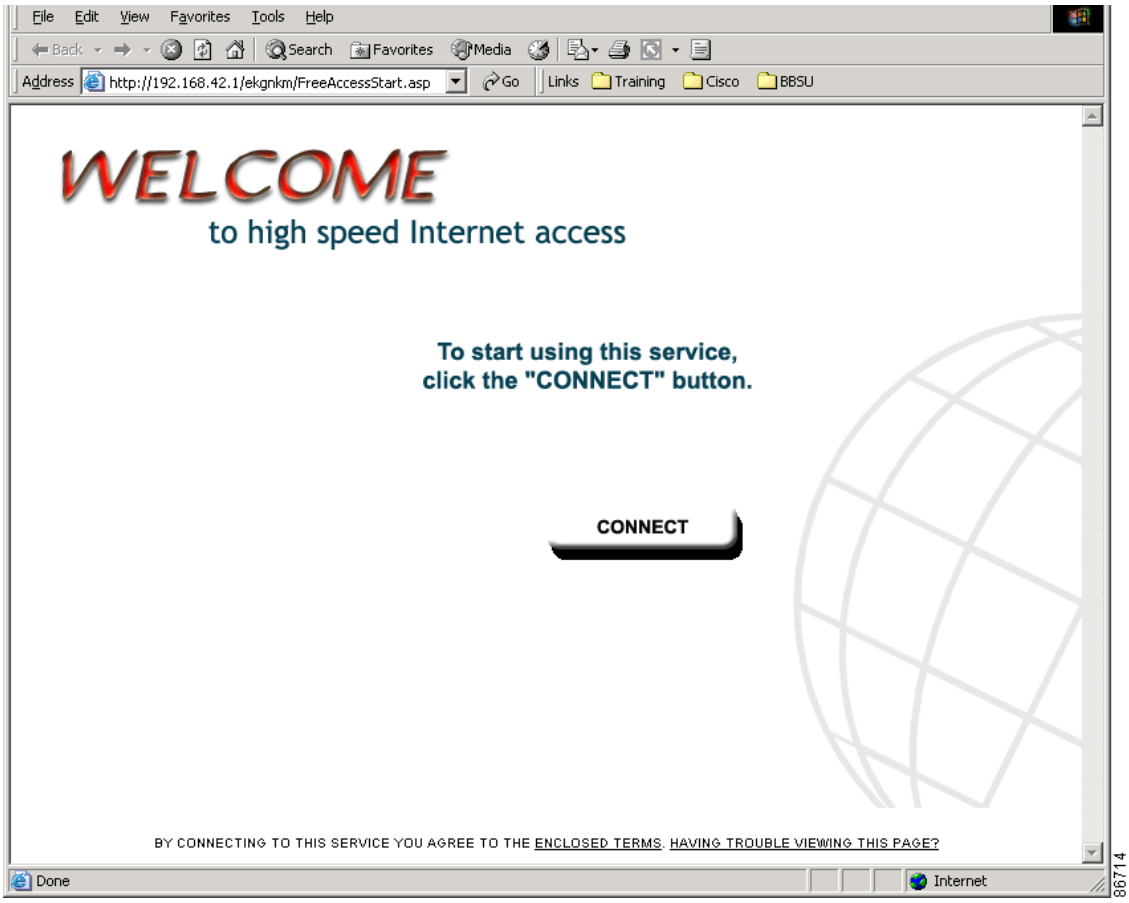
To connect a client to BBSM Hotspot, the client should meet minimum requirements. This section provides those requirements and tells how an end user connects to the BBSM Hotspot server. Table 2-8 shows the operating system and browser versions that have been tested and are supported for the BBSM Hotspot software release 1.0.

Table 2-8 Minimum End-User Client Connection Requirements

Component	Tested and Supported for BBSM Hotspot 1.0
Operating system	Windows 98, 2000 Professional, and XP Professional Linux Red Hat 7.1 Macintosh OS9.0 and OS10.0
Browser	Internet Explorer 5.0 or higher Netscape Navigator 4.7x or higher
Colors, depth	256 (65,000 recommended)
Screen Area, pixels	800 by 600—For Compaq H3635 and H3760 iPAQ pocket PCs: 240 by 320 limitation.

Note that the Setup Wizard sets all ports to the FreeAccess web page the first time the wizard is run. You can change the Start page by using the Custom Web Page Wizard or the Port Settings option in Hotspot Configuration. Figure 2-21 shows the FreeAccess Start page. (For instructions on how to use the Setup Wizard, refer to the "Running the Setup Wizard" section on page 2-2.)

Figure 2-21 FreeAccess Start Page



The following example shows how an end user using a wireless NIC connects to the Internet using BBSM Hotspot. In the example, a coffee shop has purchased a BBSM Hotspot server, set it up, and selected the FreeAccess web page. The end user does the following:

Step 1 Turn on your laptop and open your web browser. The FreeAccess web page should appear.

Step 2 If the Start page does not appear, contact property staff for information on configuring your wireless NIC.

Step 3 After verifying the configuration of the wireless NIC, open the web browser. The FreeAccess Start page appears.

Note If the Start page does not appear, refer to the troubleshooting section, "No Start Page Received by End User" section on page 4-31, for probable causes and corrective action.

Step 4 The end user is then redirected to a "Connecting..." window and then to the end user's configured initial page.

Changing the Default Security Passwords

This section describes how to change the default security passwords that come with your BBSM Hotspot server. Table 2-9 lists these passwords.

Caution For security reasons, we strongly recommend that you change these default passwords immediately. Failing to change them could compromise network security. Do not use any blank passwords.

Table 2-9 BBSM Hotspot Default Passwords

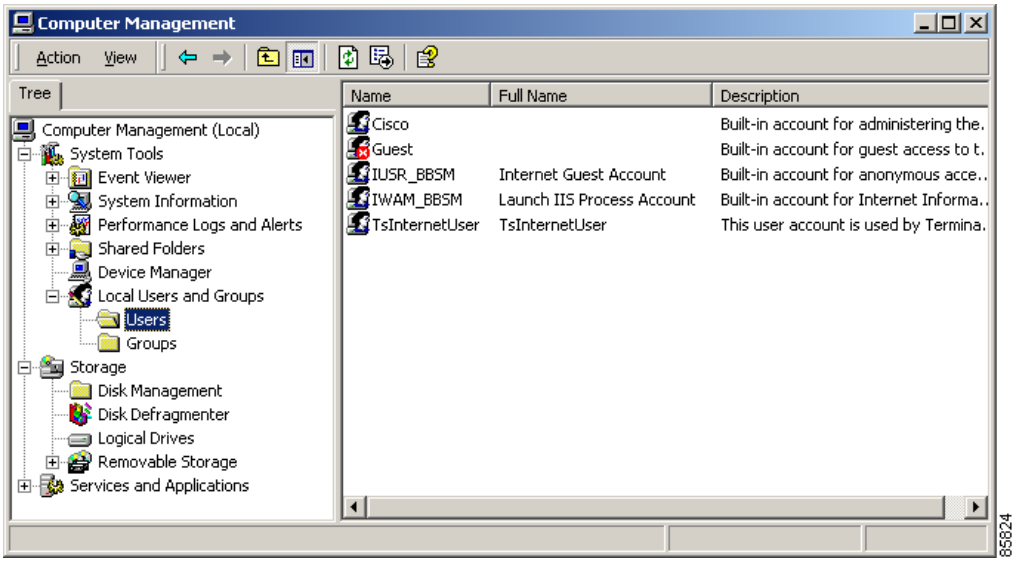
Account	Username	Default Password	Description
Windows 2000 Administrator	Cisco	cisco	The Windows 2000 Administrator has full system permissions and rights, can alter any BBSM Hotspot configuration setting, and has access to any Dashboard option.
MSDE System Administrator	sa	cisco	The MSDE system administrator ('sa') login is a default system administrator login that is included with every MSDE installation.

Changing the Windows 2000 Administrator Password

Use the following procedure to change the Windows 2000 Administrator default password.

Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **Computer Management**. The Computer Management window appears. (See Figure 2-22.)

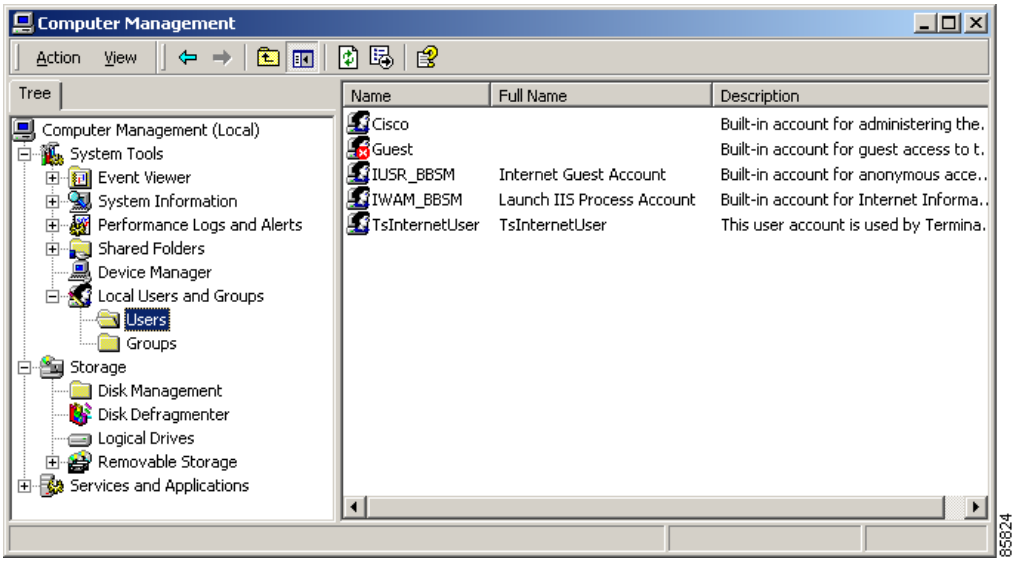
Figure 2-22 Computer Management Window



Step 2 In the left pane, double-click **Local Users and Groups**. The folder opens, showing the Users and Groups folders.

Step 3 Double-click **Users**. The folder opens, showing the user accounts. (See Figure 2-23.)

Figure 2-23 Computer Management Window, showing User Accounts



Step 4 In the right pane, right-click **Cisco**, and from the drop-down menu, choose **Set Password**.

Step 5 In the New password field, enter the new password.

Step 6 In the Confirm password field, enter the new password again.

Step 7 Click **OK**. A confirmation dialog box appears, notifying you that the password has been changed. (See Figure 2-24.)

Figure 2-24 Password Changed Confirmation Dialog Box

Step 8 Click **OK** to close the dialog box. The Computer Management window reappears.

Step 9 Close the Computer Management window.

Changing the MSDE 'sa' Password

The system administrator ('sa') login is a default system administrator login that is included with every MSDE installation. Use the following procedure to change the default MSDE 'sa' password.

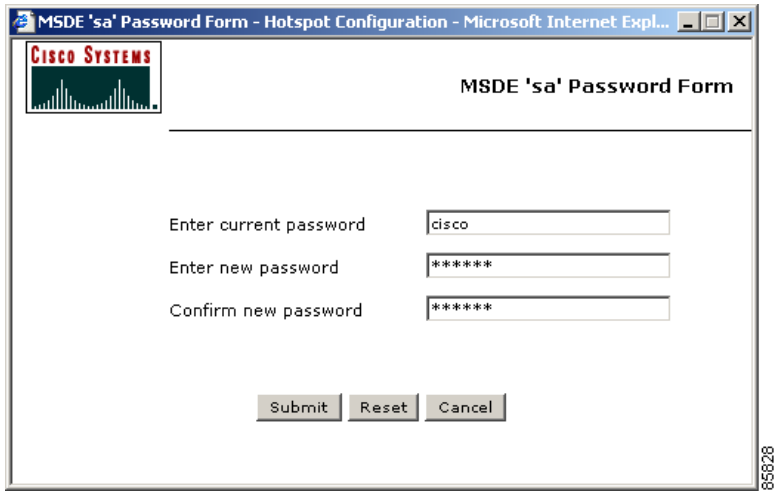
Step 1 From the Dashboard, click **Hotspot Configuration**. The Server Settings web page appears.

Step 2 In the NavBar, click **Security/SSL**. The Security/SSL web page appears.

Step 3 Next to Change MSDE 'sa' Password, click **Change**. The MSDE 'sa' Password Form appears. (See Figure 2-25.)

Note You cannot change this password without knowing the current password. Save this password in a secure location.

Figure 2-25 MSDE 'sa' Password Form



Step 4 In the Enter current password field, enter the current 'sa' password.

Step 5 In the Enter new password field, enter the new password.

Step 6 In the Confirm new password field, reenter the new password again.

Step 7 Click **Submit**. A confirmation window appears.

Step 8 Click **Close**.

Configuring Windows for Multinet

This section describes how to configure the Windows operating system to support multiple networks (multinets), on the BBSM Hotspot server. You only need to perform this procedure if you are using a multinet. BBSM Hotspot servers are initially configured as single networks, or singlenets.

Note For more information on multinets, refer to the "Private and Public IP Addresses (Multinet)" section on page 2-40.

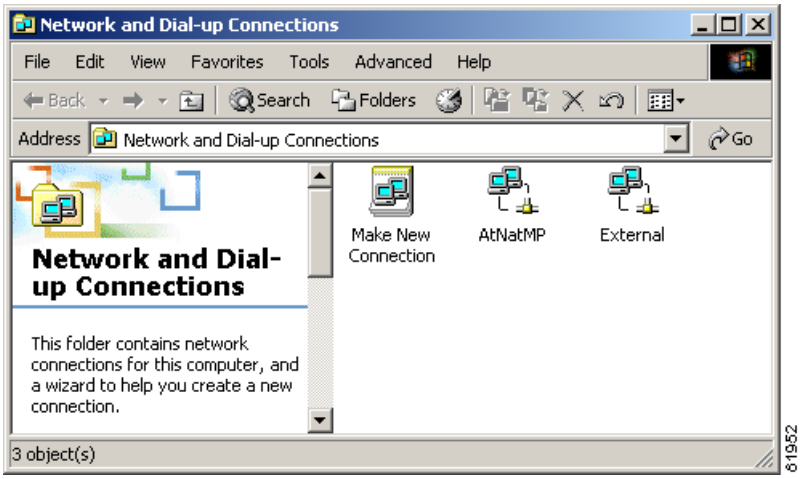
Caution Although you use the Network and Dial-up Connections window to add multinet 2, do not delete multinet 2 through this window, because although it is deleted from the GUI, it does not actually get removed from the BBSM Hotspot databases. Use the Address Change Wizard to remove multinet 2. Refer to the "Running the Address Change Wizard" section on page A-1.

Use the following procedure to reconfigure the internal NIC on your BBSM Hotspot server.

Step 1 Right-click **My Network Places**.

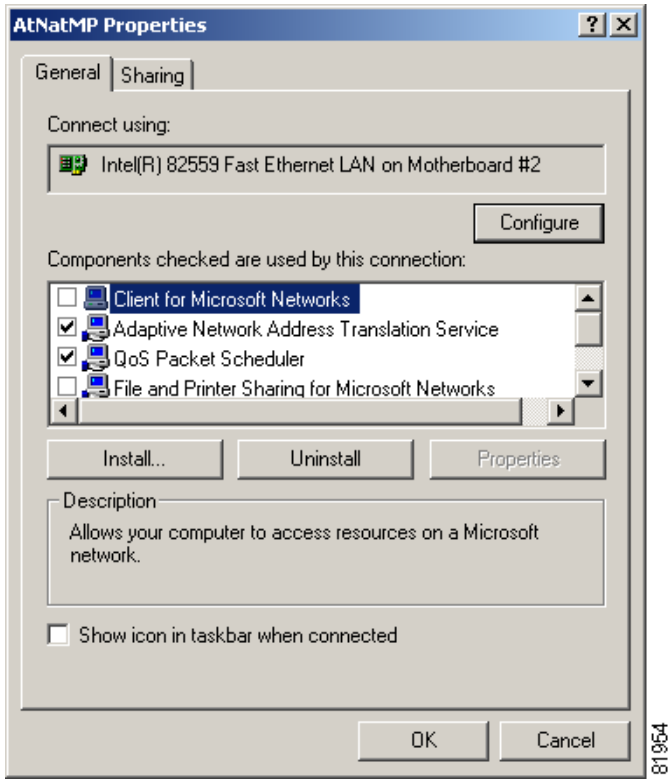
Step 2 From the pop-up menu, select **Properties**. The Network and Dial-up Connections window appears. (See Figure 2-26.)

Figure 2-26 Network and Dial-up Connections Window



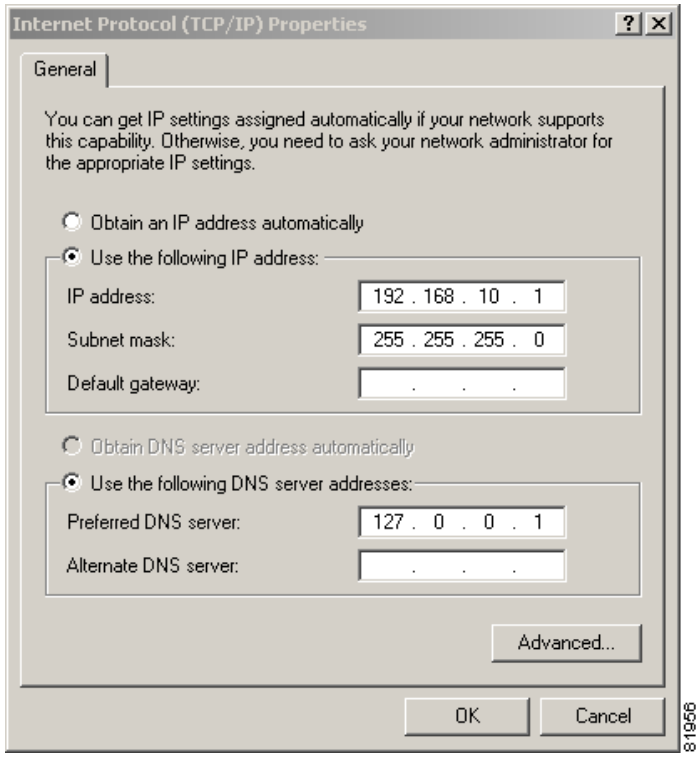
Step 3 Right-click **AtNatMP**, and select **Properties**. The AtNatMP Properties window appears. (See Figure 2-27.)

Figure 2-27 AtNatMP Properties Window



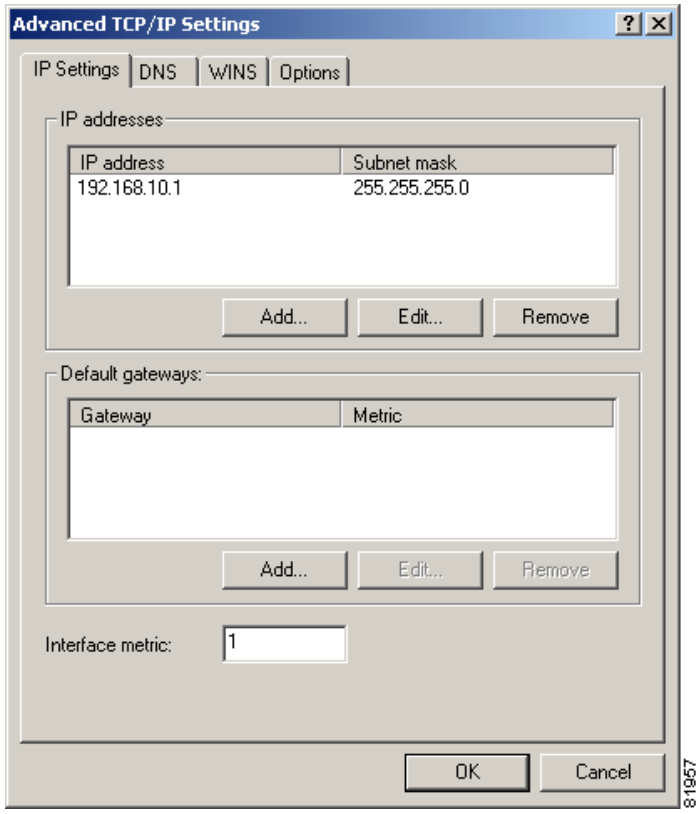
Step 4 Highlight **Internet Protocol (TCP/IP)**, and select **Properties**. The Internet Protocol (TCP/IP) Properties window appears. (See Figure 2-28.)

Figure 2-28 Internet Protocol (TCP/IP) Properties Window



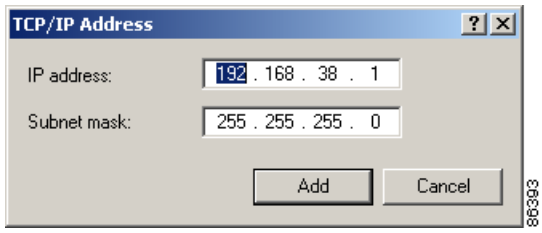
Step 5 Click **Advanced**. The Advanced TCP/IP Settings window appears, showing the IP addresses tab. (See Figure 2-29.)

Figure 2-29 Advanced TCP/IP Settings Window



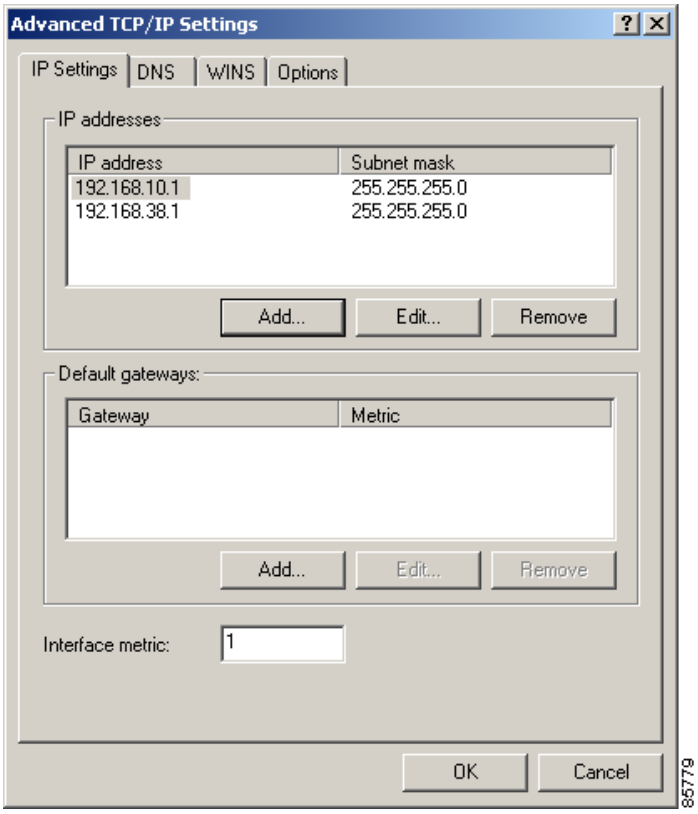
Step 6 From the IP addresses area, click **Add**. The TCP/IP Address window appears. (See Figure 2-30.)

Figure 2-30 Advanced TCP/IP Settings Window



Step 7 In the IP address and Subnet mask fields, enter the second IP address and subnet mask, and then click **Add**. You are returned to the Advanced TCP/IP Settings window, which now shows the added TCP/IP address, and you are finished with the configuration. (See Figure 2-31.) No gateways are configured for the internal NIC.

Figure 2-31 Advanced TCP/IP Settings Window with Added TCP/IP Address



Step 8 To close the Advanced TCP/IP Settings window, click **OK**.

Step 9 To close the Internet Protocol (TCP/IP) Properties window, click **OK**.

Step 10 To close the AtNatMP Properties window, click **OK**.

Step 11 Close the Network and Dialup Connections window.

Configuring DNS Forwarding

This section describes how to configure DNS forwarding if you did not configure your server by using the Setup Wizard. If you used the Setup Wizard, it configured DNS forwarding automatically.

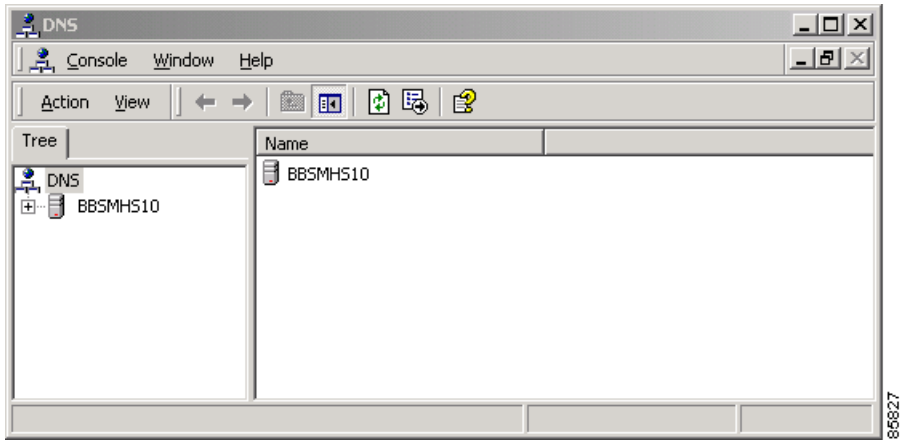
The Domain Name System (DNS) forwarding feature is enabled on BBSM Hotspot to allow DNS requests to be relayed to a remote DNS server. BBSM Hotspot is not configured as a DNS server; it acts as a DNS forwarder for its clients and its own DNS requests. These DNS requests, such as www.cisco.com, are resolved into IP addresses so the Internet routers can locate the web server with the content.

Note You must obtain the IP address for your DNS servers from your ISP before you can perform the following procedure. Refer to the BBSM Hotspot Configuration Requirements Checklist.

Use the following procedure to configure DNS forwarding for each IP address.

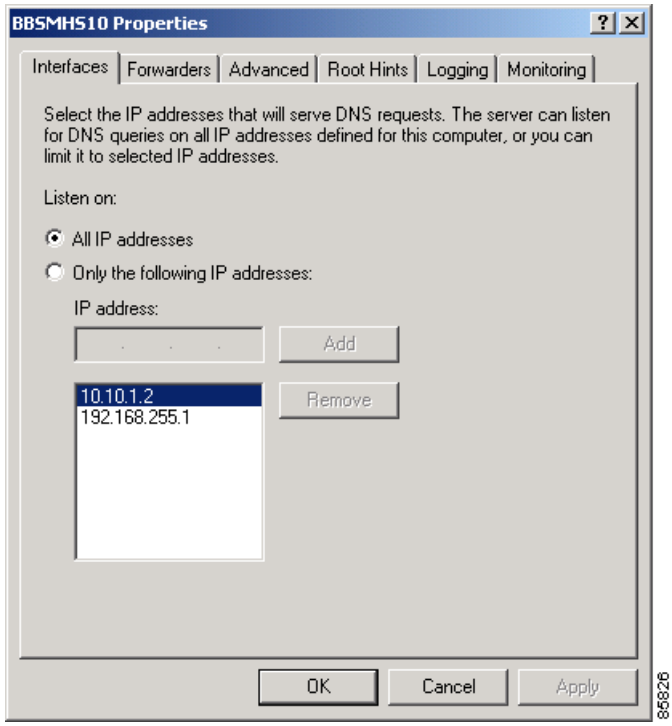
Step 1 Choose **Start** > **Programs** > **Administrative Tools** > **DNS**. The DNS window appears. (See Figure 2-32.)

Figure 2-32 DNS Window



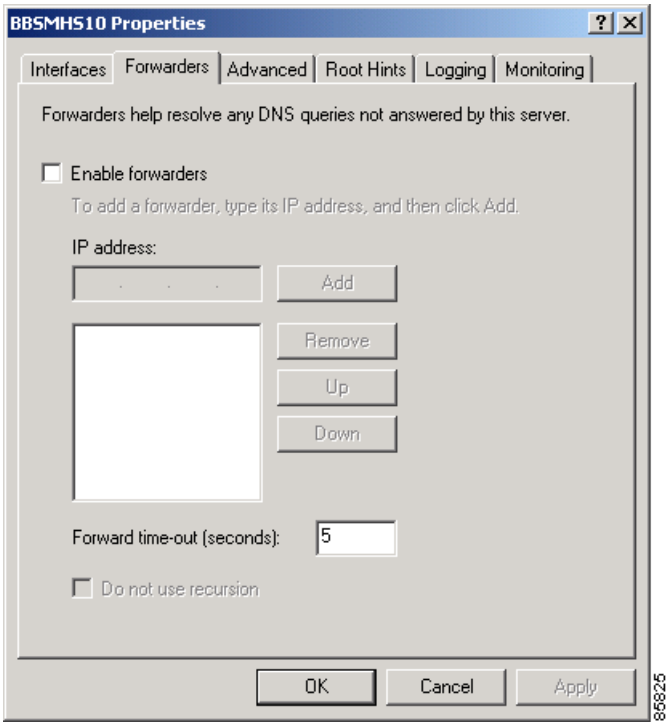
Step 2 From the left pane, right-click BBSMHS10 and choose **Properties**. The BBSMHS10 Properties window appears, showing the Interfaces tab. (See Figure 2-33.)

Figure 2-33 BBSM Hotspot Properties Window, Interfaces Tab



Step 3 Click the **Forwarders** tab. (See Figure 2-34.)

Figure 2-34 BBSMHS10 Properties Window, Forwarders Tab



Step 4 Check the **Enable forwarders** check box.

Step 5 In the IP address field, enter your DNS server IP address that is provided by your ISP, and click **Add**.

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

Step 7 Close the DNS window.

Feature Considerations

The following sections describe BBSM Hotspot features that may need some background and explanation. For information on configuring these features, refer to the "Running the Setup Wizard" section on page 2-2.

Using Web Pages

A web page set is a set of active server page (ASP) files written in Microsoft JScript, JavaScript, and HTML. They are executed on both the BBSM Hotspot server and the end user's browser when the end user starts the browser. BBSM Hotspot ships with a set of default web page sets shown in Table 2-10. You can use these default web pages without making changes.

If you want to create custom web page sets, the simplest way to create a custom web page set is to use the Custom Web Page Wizard. Refer to the "Using the Custom Web Page Wizard" section on page 3-32.

If you want to customize your web page beyond what is offered by the Custom Web Page Wizard, refer to the *Cisco BBSM 5.2 SDK Developer Guide* for instructions on manually customizing web page sets. This guide can also be used to create a custom web page for pocket PCs.

Note SDK software is provided with Cisco's BBSM software product so customers can create custom web page sets and web page policies. Although the *Cisco BBSM 5.2 SDK Developer Guide* was written to be used with the BBSM software, the appropriate sections of the guide can be used to manually create custom web page sets for BBSM Hotspot, if you choose not to use BBSM Hotspot's Custom Web Page Wizard. The SDK software, however, cannot be used with BBSM Hotspot. Using this software will corrupt the BBSM Hotspot server.

You add the new custom web page to the list of web pages on the BBSM Hotspot server by using the Custom Web Pages option in the Hotspot Configuration tool. Refer to the Adding Custom Web Pages to BBSM Hotspot, page 3-24.

If a web page requires the end user to enter sensitive information, such as credit card information, an SSL certificate should be used. When using the SSL web pages, you must buy and install an SSL certificate. For complete details on installing the certificate, refer to Appendix B, "Installing an SSL Certificate."

Caution Because web page sets whose name ends in "Clear" do not use SSL security to transmit data to the BBSM Hotspot server, Cisco does not recommend using them in production. Without SSL, the end user's browser transmits RADIUS and credit card information to BBSM Hotspot in clear text. BBSM Hotspot provides these web pages for demonstration and testing situations in which installing a server certificate is not feasible.

Table 2-10 BBSM Hotspot Default Web Page Descriptions

Web Page Set	Uses SSL?	Description
AccessCode	No	Prompts the end user to enter an access code to access the Internet for the time period configured by the BBSM Hotspot administrator. Only one user at a time is able to access the Internet using the access code.
BlockICS BlockICSClear	Yes No	Prompts the end user to enter credit card information to access the Internet for a block of minutes. When the end user disconnects, they forfeit any unused time. The time does not carry over to their next session.
DailyICS DailyICSClear	Yes No	Prompts the end user to enter credit card information to access the Internet for a 24-hour period.
FreeAccess	No	Allows the end user to connect to the Internet for an indefinite time period without charges.
Hotspot HotspotClear	Yes No	Allows the end user to select the desired access option—RADIUS, access codes, or a specified time period.
MinuteICS MinuteICSClear	Yes No	Prompts the end user to enter credit card information to access the Internet per minute.
RADIUS RADIUSClear	Yes No	Prompts the end user to enter a RADIUS username and password to access the Internet.
RADIUSUBand RADIUSUBandClear	Yes No	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 web page, 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.

Using RADIUS with BBSM Hotspot

RADIUS is the industry-standard client/server protocol for user authentication, authorization, and accounting, which enables users to access the Internet. It is designed to enable a RADIUS client to communicate with a RADIUS server by using secure communication methods. You can implement one or more RADIUS servers and a distributed network of RADIUS clients to manage security and retrieve accounting information across various broadband building sites. This strategy benefits you by providing greater security, a more scalable architecture, the ability to implement an open standards protocol, and the ability to leverage future RADIUS enhancements.

The BBSM Hotspot system has a built-in RADIUS client that supports RADIUS and is compliant with RFCs 2865 and 2866, which are the standards for RADIUS and RADIUS authentication.

Note Because this section explains only the BBSM Hotspot implementation and configuration of a RADIUS server, the customer is expected to be familiar with RADIUS protocols, as documented in RFC 2865 and RFC 2866, and how to configure their specific RADIUS server. Configuration of RADIUS servers is outside the scope of this text.

For detailed information on configuring BBSM Hotspot for RADIUS, refer to the "Configuring RADIUS Billing" section on page 3-19.

Although BBSM Hotspot officially supports the Cisco ACS, Microsoft IAS, and Navis RADIUS server protocols, it is compatible with any RADIUS server that complies with RFCs 2865 and 2866 and allows configuration of vendor-specific attributes.

BBSM Hotspot stores accounting and activation/deactivation information in the RADIUS_SessionHistory table in the BBSM Hotspot database. This table provides independent auditing of end-user sessions. Session data can be viewed in the RADIUS Session History report or by direct SQL query.

The RADIUS Session History report shows session activation and deactivation entries:

- Session activation entries—When the end user authenticates through the RADIUS authentication server and gains Internet access
- Session deactivation entries—When the end user's Internet access is terminated

The report shows Start and Stop accounting requests and whether or not an accounting response was received. If BBSM Hotspot is configured to send Interim-Update packets, the report displays the first Interim-Update accounting request made for each session. Subsequent Interim-Update requests are reported only if an error occurs during the packet transmission.

RADIUS Authentication, Authorization, and Accounting

Each time the end user connects to the BBSM Hotspot service, BBSM Hotspot prompts the user for a username and password. These values are sent in the Access-Request packet to the RADIUS authentication server. These authentication servers can be configured by administrators by order of rank using the RADIUS Server web page in Hotspot Configuration. (Servers are ranked in ascending order, so the primary RADIUS server is rank = 1, secondary server is rank = 2, and so on.) When sending the Access-Request packets, BBSM Hotspot begins authenticating servers in ascending order by using all configured RADIUS authentication servers until an Access-Accept packet is received:

- If a server does not respond within the specified time, BBSM Hotspot 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 Hotspot immediately attempts to authenticate using the next highest ranked server. (A RADIUS user can have a session active on more than one computer on the BBSM Hotspot network at the same time if this option is configured.)

When a RADIUS server sends a vendor-specific attribute that contains a bandwidth kbps value, BBSM Hotspot throttles the bandwidth of the end-user session to the specified kbps value (if bandwidth throttle is configured on BBSM Hotspot). To use this feature, administrators need to configure their RADIUS server to send the vendor-specific attribute to transmit the following:

- A vendor ID of 5263
- A vendor type of 1
- The integer value of the bandwidth kbps desired for the user account

RADIUS accounting provides administrators with end-user session information when Internet access is granted and terminated. This end-user information can then be retrieved from RADIUS accounting servers, and independent billing can be performed. Administrators can choose flat-rate or per-minute billing by using the information that BBSM Hotspot sends to the RADIUS accounting server in Start and Stop Accounting-Request packets. If configured, BBSM Hotspot also sends Interim-Update packets to the RADIUS accounting server at intervals set by the administrator.

Administrators can configure multiple RADIUS accounting servers, which provides redundancy in case the primary RADIUS server is not responding. As with RADIUS authentication servers, each server is configured with a ranking. BBSM Hotspot attempts to send accounting packets to accounting servers until an accounting response packet is successfully received. For each server, BBSM Hotspot attempts to send accounting request packets up to three times if the server fails to respond.

Table 2-11 shows the RADIUS attributes and the packets in which they are sent from the BBSM Hotspot server to the RADIUS server. Table 2-12 describes these attributes.

Table 2-11 RADIUS Access-Request and Accounting-Request Packets

Attribute	No.	Access-Request	Accounting-Request		
			Start	Interim-Update	Stop
User-Name	1	X	X	X	X
User-Password	2	X			
NAS-IP-Address	4	X	X	X	X
NAS-Port	5	X	X	X	X
Service-Type	6	X	X	X	X
Framed-Protocol	7	X	X	X	X
Framed-IP-Address	8	X	X	X	X
Vendor-Specific	26		X	X	X
Called-Station-ID	30	X	X	X	X
Calling-Station-ID	31	X	X	X	X
NAS-Identifier	32	X	X	X	X
Acct-Status-Type	40		X	X	X
Acct-Input-Octets	42				X
Acct-Output-Octets	43				X
Acct-Session-ID	44	X	X	X	X
Acct-Session-Time	46				X
Acct-Input-Packets	47				X
Acct-Output-Packets	48				X
Acct-Terminate-Cause	49				X
NAS-Port-Type	61	X	X	X	X

Table 2-12 RADIUS Attribute Descriptions

Attribute	Description
User-Name	The end user enters this name to authenticate against the RADIUS server and access the Internet through BBSM Hotspot.
User-Password	The end user enters this password to authenticate against the RADIUS server and access the Internet through BBSM Hotspot.
NAS-IP-Address	Contains either the IP address of the BBSM Hotspot external NIC or the IP address entered in the WEBconfig RADIUS Server web page as the NAT IP address.
NAS-Port	The NAS-Port value is a numeric value (therefore the leading zeros of the site number are dropped). BBSM Hotspot maps the NAS-Port attribute as the following: aaabbccddd, where aaa = site number, bb = cluster, cc = switch, and ddd = port. For example, if the site number = 1, the cluster number = 2, the switch number = 3, and the port number = 5, the NAS-Port number = 10203005.
Service-Type	2 indicates Framed.
Framed-Protocol	1 indicates PPP.
Framed-IP-Address	IP address of client computer (PC) connecting to the Internet through BBSM Hotspot.
Called-Station-Id	Contains the MAC address of the BBSM Hotspot internal NIC.
Calling-Station-Id	Contains the MAC address of the client (end-user) NIC.
Vendor-Specific	Contains the bandwidth kbps value that the end user selects when requesting Internet access. This attribute is only sent to RADIUS accounting servers if the UBand feature is enabled. See Table 2-13 for the vendor-specific attribute formatting.
NAS-Identifier	Contains the NAS Identifier value entered in the WEBconfig RADIUS Server web page. If no value is entered in this field, BBSM Hotspot will not include this attribute in the RADIUS Access-Request packet.
Acct-Status-Type	1: Start Accounting-Request packet—Requests that a message be sent when the user gains access. 2: Interim-Update Accounting-Request packet—Requests that a message be sent at regular intervals, as configured. 3: Stop Accounting-Request packet—Requests that a message be sent when the user disconnects.
Acct-Input-Octets	The number of octets (bytes) that BBSM Hotspot received from the end user during their session.
Acct-Output-Octets	The number of octets (bytes) that BBSM Hotspot transmitted to the end user during their session.
Acct-Session-Id	The unique Session ID assigned to each BBSM Hotspot end-user session used to identify all authentication and accounting messages generated for a single user session.
Acct-Session-Time	Indicates how many seconds the user has received service for and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
Acct-Input-Packets	The number of packets that BBSM Hotspot received from the end user during the user's session.
Acct-Output-Packets	The number of packets that BBSM Hotspot transmitted to the end user during the user's session.
Acct-Terminate-Cause	Indicates how the session was terminated and can only be present in Accounting-Request records where the Acct- Status-Type is set to Stop.
NAS-Port-Type	5 = Virtual.

Table 2-13 RADIUS Cisco BBSM Hotspot-Bandwidth Vendor-Specific Attribute Format

Byte	Value	Description
1	26	Vendor-specific attribute type in accordance with RFC 2865
2	(4 * sizeof (BYTE)) + (2 * sizeof (DWORD))	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	The vendor-ID value.
7	1	The vendor data type; 1 indicates bandwidth kbps value.
8	(2 * sizeof (BYTE)) + sizeof (DWORD)	The length in bytes of the vendor-specific portion of the attribute specification starting with vendor-specific attribute data type. If each byte size = 1, should come out to 6.
9–12	A bandwidth specified in kbps; such as 256	Actual bandwidth kbps value (ulong).

User-Selected Bandwidth (UBand) Web Pages

User-selected bandwidth (UBand) web pages support a user-specified bandwidth. This feature allows the administrator to define the service offerings and allows the end user to select from the tiered services offered directly from the Start page, such as the following:

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

When a UBand web page is used, BBSM Hotspot throttles the session bandwidth at the kbps value that the end user selects. This bandwidth value is transmitted to the RADIUS accounting servers in the Start, Stop, and Interim-Update Accounting-Request packets and BBSM Hotspot ignores any bandwidth value that the RADIUS authentication servers return in the Access-Accept packets.

The two BBSM Hotspot-provided sample web pages that implement this feature are RADIUSUBand and RADIUSUBandClear. These web pages can be used as templates to customize the tiered services that you want to offer.

Note Note that the administrators must make sure that the RADIUS accounting servers are configured to accept the bandwidth that BBSM passes in the vendor-specific attribute and to record this attribute value so the data can be retrieved for billing. The RADIUS provider is responsible for charging the end user for the selected bandwidth.

When the user disconnects from the session, the Disconnect web page appears and displays the session summary information: username, session duration (in minutes), and estimated session charge.

Port Hopping

The port hopping feature allows users to move from port to port without interrupting BBSM Hotspot service. Within a BBSM Hotspot network, users can move between like types of hardware, such as wireless access points or switch ports. Users cannot hop between wireless access points and wired switches. Also, mobility across subnets or cells operated by different customers is not allowed.

Port hopping is disabled by default and can only be enabled on a per-port basis by an administrator. For procedures on different ways to configure port hopping, refer to the following sections:

- "Configuring Your Server (Hotspot Configuration)" section on page 3-1
- "Configuring Ports (Port Configuration)" section on page 3-27

When port hopping is enabled, BBSM Hotspot keeps the session active when the user moves to another port or temporarily disassociates. For example, disassociation might occur when the signal is weak or an object comes between the wireless access point and the end user, which causes the user to associate suddenly with a secondary access point that might be configured to another aggregation switch port.

When a user dissociates from the BBSM Hotspot network, BBSM Hotspot searches for the user until one of the following occurs:

- The user's MAC address reappears back on the network within the configured port hop delay time period. The session then continues without interruption.
- The port hop delay time period expires. BBSM Hotspot then deactivates the session, and the user must reauthenticate to regain Internet access.

Note the following about port hopping:

- Searching for end user—When port hopping is enabled and an end user disappears from the network, BBSM Hotspot begins searching for the end user. BBSM Hotspot searches all configured network elements. It first searches the last known network element that the end user was connected to or associated with. If the user is not found, BBSM Hotspot then searches all other configured network elements until the end user is found or the port hop delay time period expires.
- Session duration—The reported duration of an active session varies depending on how the session terminates:
  - If the search succeeds, BBSM Hotspot includes the time that it searched for the user in the session duration.
  - If the search fails to find the user before the port hop delay time period expires, BBSM Hotspot does not include the search time in the session duration. In this way, the user that terminates a session by turning off the computer is not charged for the time that BBSM Hotspot spends searching for the user on other ports.
- Port hopping from a port hop disabled port—Port hopping is enabled on a per-port basis. The end user is allowed to hop from a port hop enabled port to any port on the same site and continue the session even if the port hop status of the destination port is disabled. However, the user is not allowed to hop from a port hop disabled port at all. If this is attempted, BBSM Hotspot deactivates the session.
- Port policy—As the user hops from port to port, the port policy that BBSM Hotspot associates with the user session follows the user to each new port:
  - BBSM Hotspot applies the bandwidth limit (in kbps) specified at session activation to the session as the user moves from port to port.
  - If a user has selected a dynamic bandwidth boost from a BBSM Hotspot web page, when the user moves to another port, the bandwidth boost settings follow the session to the new port.
- Active Ports report—While the system is searching for a user, the user session remains active and appears in the Active Ports report as associated with the last used port.

Private and Public IP Addresses (Multinet)

You can offer end users the choice of using individually assigned private or public DHCP IP addresses:

- Public IP addresses can be accessed by other devices on the Internet.
- Private IP addresses cannot be accessed by other Internet devices.

To explain the difference between private and public IP addresses, we can compare the IP address to a phone number. A public IP address is equivalent to a full 10-digit telephone number (619-555-1234), and a private address is equivalent to an office extension number.

The advantage of using one type of IP address over the other depends on the end user's needs:

- The advantage of using public IP addresses is that some virtual private network (VPN) systems require their clients to have public IP addresses to operate correctly.
- The advantage of using private IP addresses is many security threats are eliminated, because other Internet devices cannot access private IP addresses. Because the local network automatically maps each private IP address to a different public IP address for data going to and from the Internet, a private IP address is never visible on the Internet. In addition, because private IP addresses are free, they of course cost less than public IP addresses.

BBSM Hotspot servers are configured initially as singlenet. If you want to use a multinet configuration, you must reconfigure the server for multinet. Singlenet and multinet BBSM Hotspot servers are defined as follows:

- Singlenet—A singlenet BBSM Hotspot server is configured as a single logical subnet and only supports one logical subnet of IP address.
- Multinet—A multinet BBSM Hotspot server is configured with two distinct logical subnets and supports both public and private IP addresses.

To change your BBSM Hotspot server to a multinet configuration, you must configure Windows for multinet. Refer to the "Configuring Windows for Multinet" section on page 2-26.

To configure public or private IP addresses, refer to the "Running the Address Change Wizard" section on page A-1. To add, change, or delete public-private IP addresses after the initial configuration, refer to the "Configuring IP Addresses" section on page 3-3.

The per-port default IP type, which can be overridden by web page sets, can only be changed by the BBSM Hotspot administrator. To add this functionality to your custom web page sets, refer to the *Cisco BBSM 5.2 SDK Developer Guide*.

Cisco Switch Clustering

The BBSM Hotspot software supports the Cisco switch clustering technology that allows up to 16 switches (Catalyst 2950, 3500, and 3550 XL switches) to be clustered together and managed using just one IP address for the entire cluster. It allows the administrator to update the Network Devices page in the Hotspot Configuration tool, by using only the master switch IP address and a unique SNMP password for each switch in the cluster.

The switch clustering feature also continues to support cluster configurations in which each cluster/switch has a unique IP address.

Note Before running the Setup Wizard, the administrator must enable the switch clustering capability for all cluster-capable switches. For detailed information, refer to your switch documentation.

CHAPTER 3

Advanced Configuration Options

Cisco recommends that you use the Setup Wizard for the initial configuration before using the advanced options in this chapter. This chapter covers the tools that enable you to change option settings to better tailor your operation.

Again, by performing the procedures in Chapter 2, "Setting Up BBSM Hotspot," you should be fully operational. This chapter is divided into the following sections:

- Configuring Your Server (Hotspot Configuration), page 3-1—How to configure your server using the Hotspot Configuration tool
- Configuring Ports (Port Configuration), page 3-27—How to configure ports using the Port Configuration tool
- Using the Custom Web Page Wizard, page 3-32—How to create custom web pages using the Custom Web Page Wizard

Configuring Your Server (Hotspot Configuration)

After using the Setup Wizard, you can make server changes using the Hotspot Configuration tool. When you click on the Hotspot Configuration tool on the Dashboard, it displays the Server Settings web page and the navigation bar (NavBar) that is used for selecting all of the configuration web pages. To close the Hotspot Configuration tool and return to the Dashboard, click the Dashboard link in the upper right-hand corner of the web page.

In conjunction with the options available to you on the NavBar, the Hotspot Configuration tool and this section are divided into the following functionality:

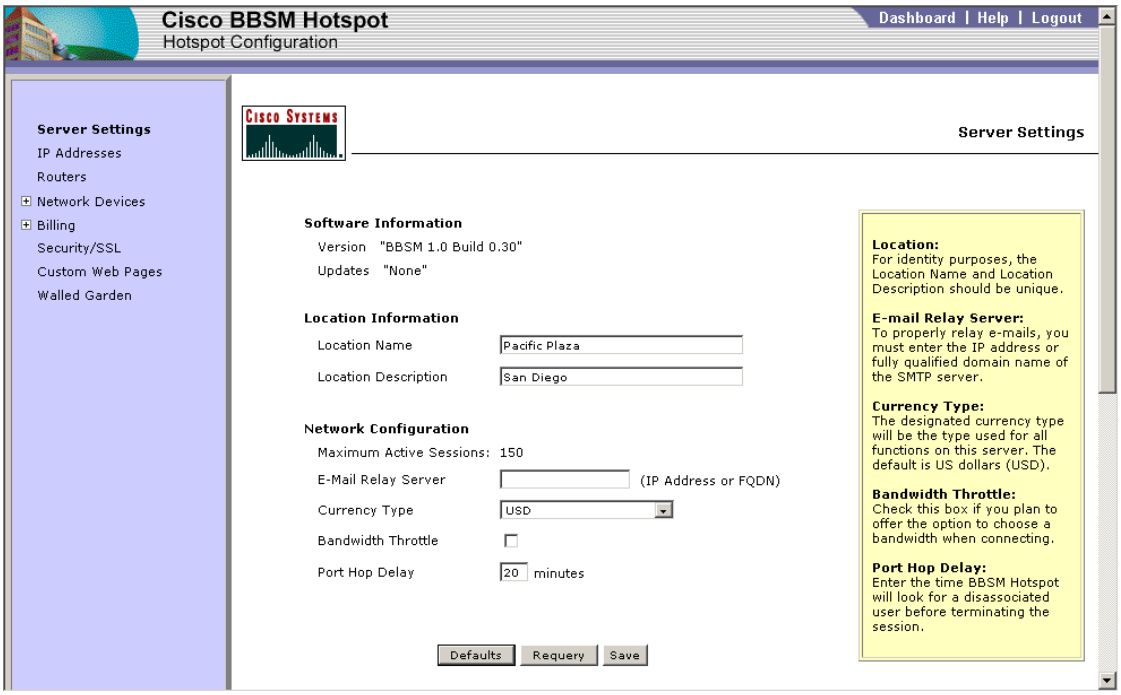
- Configuring Server Settings, page 3-2
- Configuring IP Addresses, page 3-3
- Configuring Routers, page 3-6
- Configuring Network Devices, page 3-10
- Configuring Billing Options, page 3-16
- Configuring Security/SSL, page 3-22
- Configuring Walled Gardens, page 3-25

Configuring Server Settings

To configure the basic network and bandwidth management settings, use the Server Settings web page. Use the following procedure to configure these settings.

Step 1 From the Dashboard, click **Hotspot Configuration**. The Server Settings web page appears. (See Figure 3-1.)

Figure 3-1 Server Settings Web Page



Step 2 Configure the network configuration and bandwidth management options, based on the information shown in Table 3-1.

Step 3 To save the changes made on the web page, click **Save**.

Table 3-1 Server Settings Web Page Options

Field	Description
Location Information	
Location Name	Enter a specific property name. You can use up to 50 alphanumeric characters, such as "Joes Coffee Shop" or "2nd Level Conference Rooms."
Location Description	Enter optional descriptive text for the location, such as the city or address. You can use any alphanumeric word or phrase up to a maximum of 100 characters, such as "San Diego, CA," or "Guest cubicles in the northeast annex." This field is optional.
Network Configuration	
Maximum Active Sessions	Displays the maximum number of allowable active sessions, which is the maximum number of simultaneous users. BBSM Hotspot supports up to 150 simultaneous users.
E-Mail Relay Server	Enter the IP address or fully qualified domain name (FQDN) for the e-mail relay server that is used by your ISP to forward non-web based e-mail, such as Microsoft Outlook or Eudora e-mail programs, from public locations. An example FQDN is www.ispemail.com. The FQDN can contain a maximum of 100 characters. This field is optional. Use it only if you want to provide your end users with e-mail support.
Currency Type	From the drop-down menu, select the local currency type for BBSM Hotspot transactions. Note that this currency type will be the designated currency type for the entire BBSM Hotspot server. The default type is USD (for U.S. dollars).
Bandwidth Throttle	Check this box if you plan to offer end users the option to choose a particular bandwidth when they connect. Bandwidth throttling allows the administrator to control the maximum bandwidth allocated to end users per port.
Port Hop Delay	Enter the number of minutes between 1 and 60 that BBSM Hotspot will search for the end user after disassociating from the original port. If the end user is not found within this time frame, the BBSM Hotspot session is terminated. The default number of minutes is 20. **Note** Port hopping is configured for each port. For an overview of the port hopping feature, refer to the "Port Hopping" section on page 2-38.
Buttons	
Defaults	Displays the default parameter settings.
Requery	Before you have saved any changes, click to return the web page to the previously saved settings.
Save	Saves the changes made to the web page.

Configuring IP Addresses

You must configure the following IP address ranges that BBSM Hotspot uses. This configuration applies to the entire BBSM Hotspot server.

- Network device IP address range
- End-user client IP address ranges (DHCP and Static)

During the initial configuration, you use the Setup Wizard or the Address Change Wizard to configure these fields. You can also use this Hotspot Configuration tool to configure or change these IP addresses. If you are using a multinet, you must also configure the Temp DHCP Client address range.

Refer to the following sections for additional information:

- For additional information about public and private IP addresses, refer to Private and Public IP Addresses (Multinet), page 2-40.

- For the step-by-step instructions on running the Setup Wizard, refer to Running the Setup Wizard, page 2-2.
- For the step-by-step instructions on running the Address Change Wizard, refer to Running the Address Change Wizard, page A-1.

Use the following procedure to add, change, or delete IP addresses using the Hotspot Configuration tool.

Step 1 From the Dashboard, click **Hotspot Configuration**. The Server Settings web page appears.

Step 2 In the NavBar, click **IP Addresses**. The IP Addresses web page appears. Note that the Multinet 2 and Temp DHCP Lease Duration fields only apply to a server configured for multinets. (Figures 3-2 and 3-3 show the web pages for singlenet and multinet.)

Figure 3-2 IP Addresses Web Page for a Singlenet

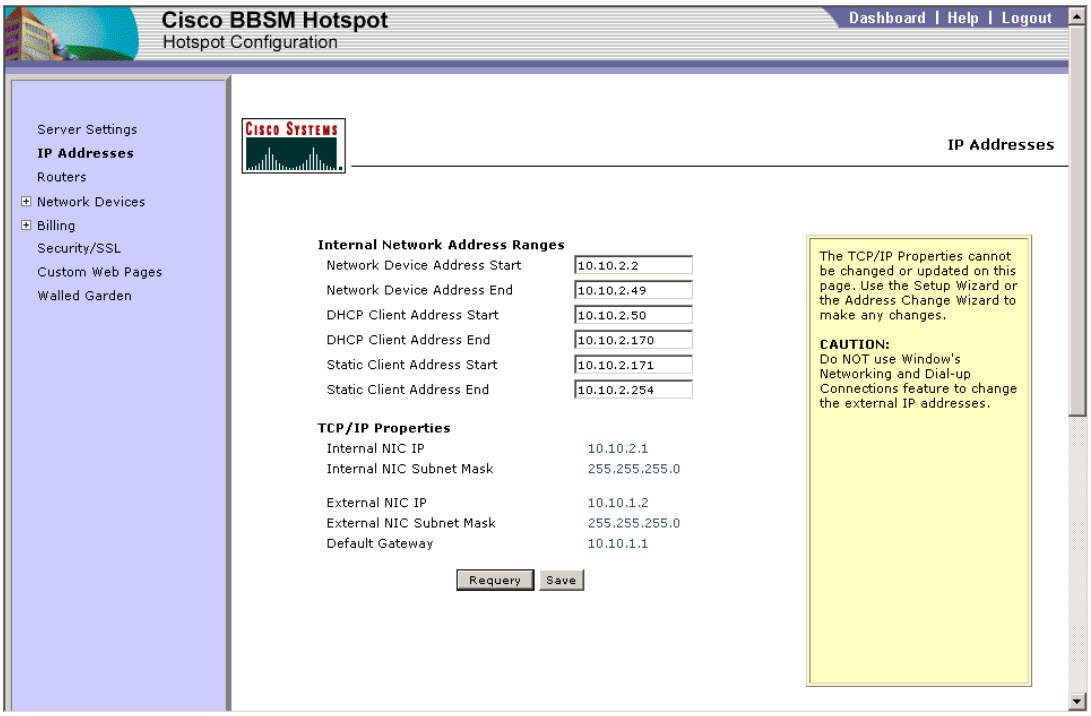
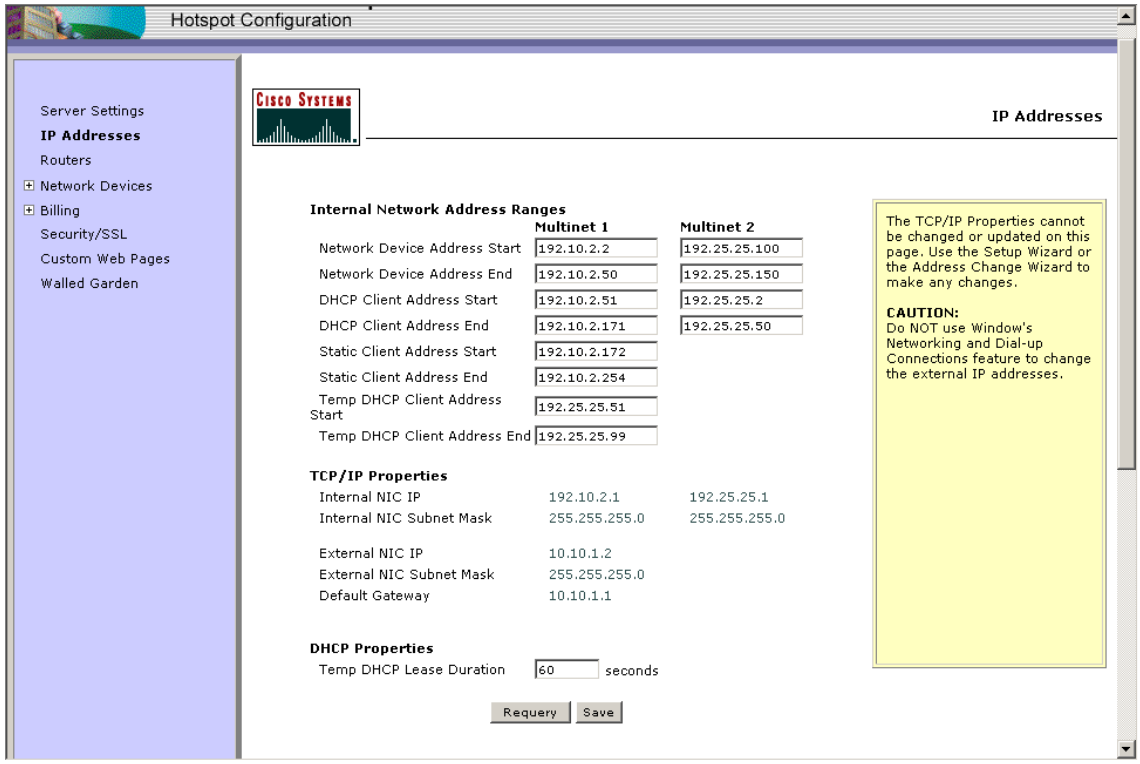


Figure 3-3 IP Addresses Web Page for Multinets



Step 3 Enter the IP configuration data, based on the information shown in Tables 3-2 and 3-3.

Table 3-2 IP Addresses Configuration

	Network Type		
		Multinet	
Parameter	**Single**	**1**	**2**
DHCP client IP address ranges	X	X	X
Static client IP address ranges	X	X	—
Temp DHCP IP address ranges	—	Multinet 1 or 2, whichever address range is higher	

Step 4 Verify that the TCP/IP IP properties are correct, which is necessary for BBSM Hotspot to function properly. If they are incorrect, refer to the "Running the Address Change Wizard" section on page A-1 to change them.

Step 5 To save the changes, click **Save**.

Table 3-3 IP Addresses Web Page Options

Field	Description
BBSM Hotspot Internal Network Address Ranges	
Network Device Address Start Network Device Address End	Enter the starting and ending IP addresses to be assigned to switches and access points. To access equipment remotely over the Internet, put network equipment in this range.
DHCP Client Address Start DHCP Client Address End	Enter the starting and ending IP addresses to be assigned to end-user clients configured as DHCP clients. This address range must be on the same subnet as your internal network interface card (NIC).
Static Client Address Start Static Client Address End	Enter the starting and ending IP addresses for end-user clients that are configured with static IP addresses. This address range enables BBSM Hotspot to perform adaptive network address translation (NAT) for statically configured clients in a bridged environment. **Note** All other NAT and PAT functionality is handled by the external router.
Temp DHCP Client Address Start Temp DHCP Client Address End *(multinets only)*	Enter the starting and ending IP addresses for the DHCP leases received by clients when they initially connect to the network in a multinet environment. This address range can be on either Multinet 1 or Multinet 2.
BBSM Hotspot TCP/IP Properties *(These fields are read only.)*	
Internal NIC IP Internal NIC Subnet Mask	The IP address and subnet mask of the internal NIC that connects to the base switch.
External NIC IP External NIC Subnet Mask	The IP address and subnet mask of the external NIC that connects to the external router.
Default Gateway	The default gateway to the Internet.
BBSM Hotspot DHCP Properties	
Temp DHCP Lease Duration (in seconds) *(multinets only)*	Enter the lease time for the temporary DHCP leases received by clients when they initially connect to the network. This time should be set low so that when the client chooses their IP preference, they will receive their final IP address in a short amount of time. The longer it takes for the client to receive their final IP address, the more likely it is that the Temp DHCP range will fill up, thereby preventing additional clients from connecting. The default is 60 seconds.
Buttons	
Requery	Before you have saved any changes, click to return the web page to the previously saved settings.
Save	Saves the changes made to the web page.

Configuring Routers

In BBSM Hotspot, all network devices are associated with a router. This association tells BBSM Hotspot how to build routes to the networks internal to itself. When you add routers, make sure you physically install them before attempting to configure them. (Refer to your network configuration information to configure the router fields.)

Note In a bridged BBSM Hotspot internal network, all network devices are associated with router 0, the BBSM Hotspot server. If your internal network is bridged, you do not need to configure a router on BBSM Hotspot.

Use the following procedure to configure a router on the BBSM Hotspot internal network.

Step 1 From the Dashboard, click **Hotspot Configuration**. The Server Settings web page appears.

Step 2 In the NavBar, click **Routers**. The Routers web page appears. (Figures 3-4 and 3-5 show the Routers web page for a singlenet and a multinet.)

Figure 3-4 Routers Web Page for a Singlenet

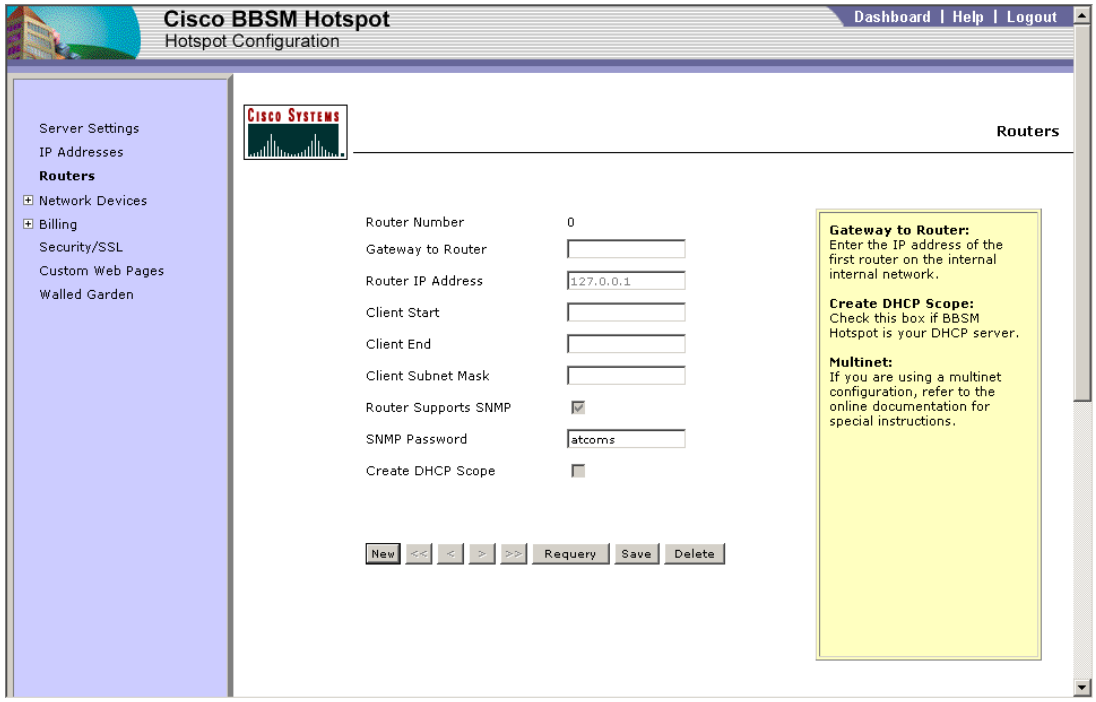
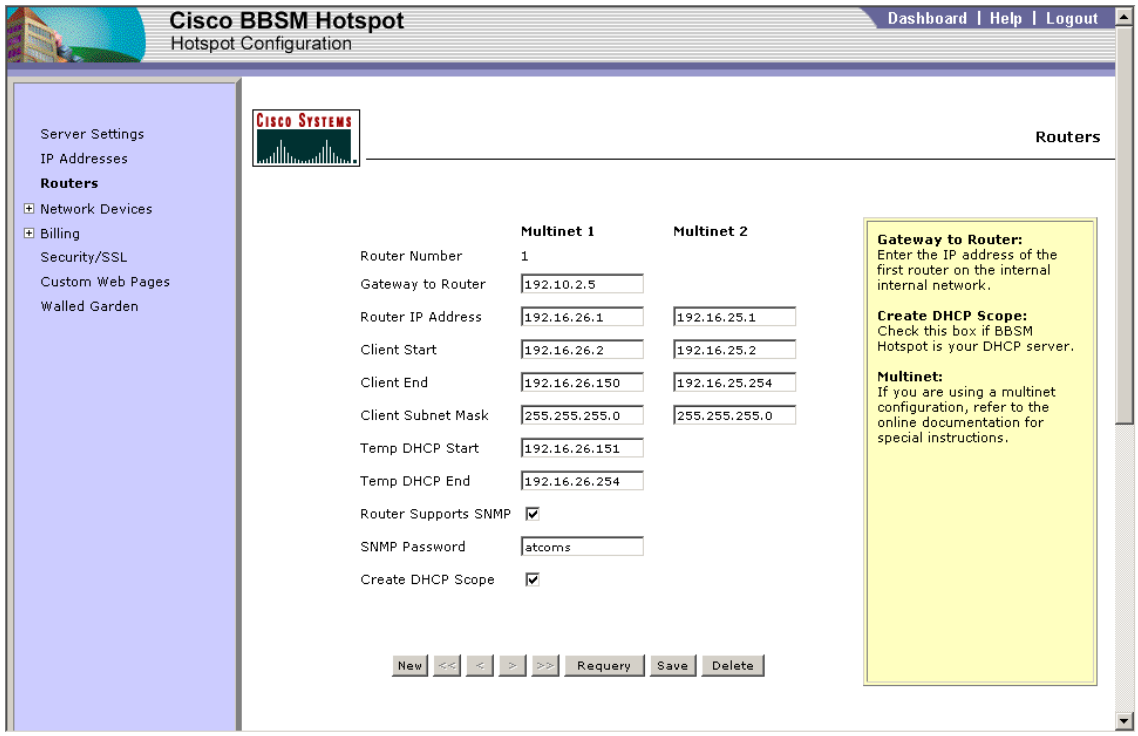


Figure 3-5 Routers Web Page for a Multinet



Step 3 Enter the router data, based on the information shown in Table 3-4. Note that for router number 0, which is the BBSM Hotspot server, all fields except Router Number and SNMP Password are disabled. These fields are only enabled if the router number is greater than 0.

Step 4 To save the changes, click **Save.**

Table 3-4 Routers Web Page Options

Field	Description
Router Number	Displays the router number of the router being configured. BBSM Hotspot autogenerates this number.
Gateway to Router	Enter the IP address of the first hop from the BBSM Hotspot server to the router. This address should be on the BBSM Hotspot server's internal network and is the router's external address if the router is connected directly to the BBSM Hotspot server's network.
Router IP Address	Displays the client-side IP address of the router. On clients, this IP address is the default gateway. In the case of clients connected to the BBSM Hotspot server internal network, the gateway is the BBSM Hotspot server's internal NIC address. The default is 127.0.0.1. (This loopback IP address refers to the BBSM Hotspot server and cannot be changed for router 0.)
Client Start Client End Client Subnet Mask	Enter the starting and ending DHCP IP addresses and the subnet mask for the clients connecting to this router.
Router Supports SNMP	If you are using a router that supports SNMP, check the check box: • For router 0 (the BBSM Hotspot server), the check box is checked and read only. The SNMP password field is enabled. • For routers other than router 0, the field is enabled. If the administrator checks the check box, the SNMP password field is enabled. Otherwise, the SNMP password is disabled. ⚠ **Caution** Note the following restrictions to disabling Router Supports SNMP. Because BBSM Hotspot will not know the client's MAC address, BBSM Hotspot will not be able to use any network device to determine if the session is still active (the administrator must configure the null switch), which affects many BBSM Hotspot operations, including reporting, the Daily access policy Welcome Back feature, and any per-port policy.
SNMP Password	Enter the SNMP password (community string) that is used when communicating with the router. The default is "atcoms."
Create DHCP Scope	Check this check box if BBSM Hotspot is your DHCP server. A DHCP scope is created on the BBSM Hotspot server for the router subnet, as determined by the IP addresses in the Client Start and End fields. Leave the check box unchecked if you are using a DHCP server other than BBSM Hotspot.
Buttons	
New	Adds a new router web page with a router number. (When you add routers, make sure that you physically install them before attempting to configure them.)
Requery	Before you have saved any changes, click to return the web page to the previously saved settings.
Save	Saves the changes made to the web page.
Delete	Deletes the router from the site.

Configuring Network Devices

BBSM Hotspot supports the use of access points and switches for network devices. This section describes how to configure or change them.

Caution The SNMP password located in Hotspot Configuration under Network Devices must match the SNMP Read/Write Community String password that is configured in the network device software. If the BBSM Hotspot password does not match the SNMP password (community string), BBSM Hotspot cannot communicate with or locate end users connected to the network device. To change the network device password, follow the manufacturer's instructions. To change the BBSM Hotspot SNMP password, refer to the following access point or switch configuration subsection.

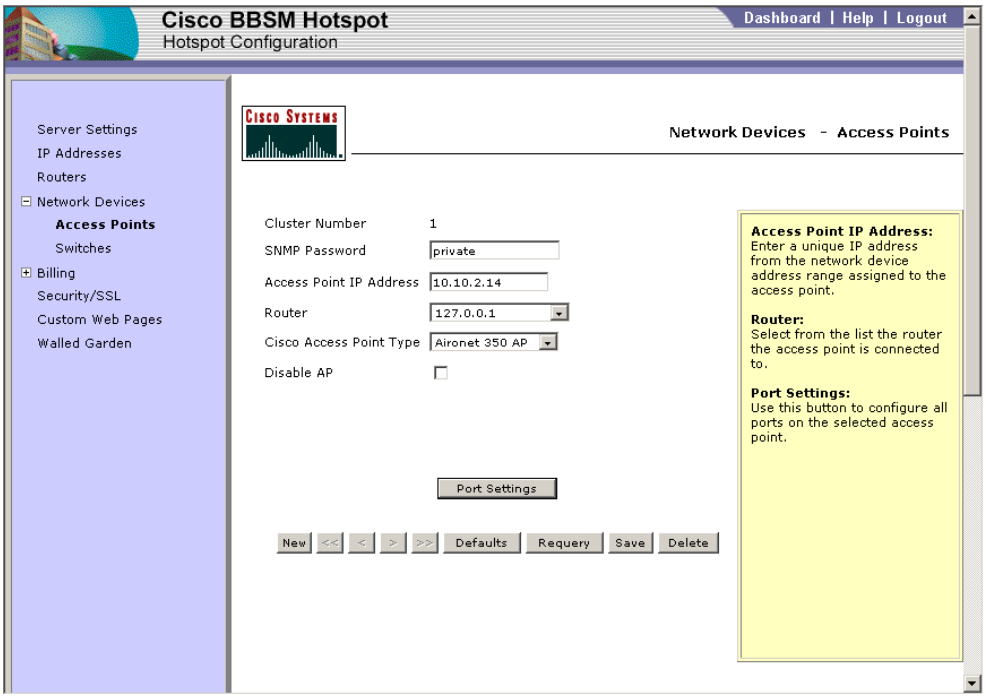
Configuring Access Points

Use the following procedure to configure an access point.

Step 1 From the Dashboard, click **Hotspot Configuration**. The Server Settings web page appears.

Step 2 In the NavBar, navigate to the Access Points web page by choosing **Network Devices > Access Points**. The Access Points web page appears. (See Figure 3-6.)

Figure 3-6 Access Points Web Page



Step 3 Configure the access points, based on the information shown in Table 3-5, and then click **Save**. The Network Devices - Port Settings window appears. (Figure 3-7 shows the window for a multinet configuration.)

Note If port configuration records already exist, the Network Devices - Port Settings window does not pop up automatically. Click **Port Settings**.

Step 4 Enter the applicable information, based on the information in Table 3-6.

Step 5 To save the data, click **Submit**. You are returned to the Access Points web page.

Table 3-5 Access Points Web Page Options

Field	Description
Cluster Number	Displays the cluster number associated with the access point to be configured.
Access Point IP Address	Enter a unique IP address from the network device IP address range.
Router	From the drop-down menu, select the IP address of the router that this access point is connected to.
Cisco Access Point Type	From the drop-down menu, select the type of Cisco access point.
Disable AP	Check this check box if you do not want BBSM Hotspot to look for clients on the ports for the access point. Use this feature when troubleshooting or when the access point is not yet installed on the network. **Note** If you disable an access point, its IP address remains reserved. If you need to reuse the IP address for a different network device, change the IP address of the disabled access point.
SNMP Password	Enter the SNMP community string (password) that is used when communicating with the access point. The default is "private." **Caution** We recommend that you change the default password on the access points and on BBSM Hotspot, because the default password is well known and could compromise network security.
Buttons	
Port Settings	Click to configure the access point ports. The Network Devices - Port Settings window appears. Enter the correct information, as described in Table 3-6, and then click **Submit**.
New	Click to add a new access point. The web page changes to reflect this new access point.
Defaults	Displays the default parameter settings.
Requery	Before you have saved any changes, click to return the web page to the previously saved settings.
Save	Saves the changes made to the web page.
Delete	Deletes the access point.

Figure 3-7 Network Devices - Port Settings Window (Multinet Example)

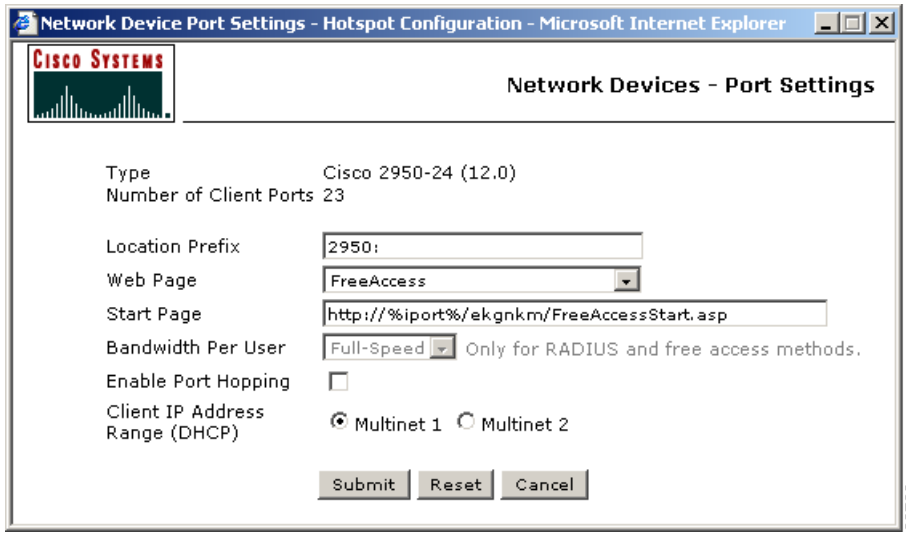


Table 3-6 Network Devices - Port Settings Window Options

Field	Description
Type	Displays the type of configured access point or switch.
No. of Client Ports *(switches only)*	*This field only appears when you are using a switch.* Displays the number of client ports on the switch. The default number varies, depending on the selected switch.
Location Prefix	If desired, enter a location prefix. The prefix can contain a maximum of 40 characters. (This field is optional.)
Web Page	From the drop-down menu, choose the desired web page set. For descriptions of the default web pages that ship with BBSM Hotspot, refer to Table 2-10 on page 2-34. **Note** If you will be using SSL and have not yet installed your SSL certificate, select the "Clear" version of the web page until you install the certificate and then change your web page to the SSL web page. For example, select RADIUSClear until the certificate is installed, then after installing the certificate, change the web page to RADIUS. If you select an SSL web page before installing the certificate, the end user will not be able to connect.
Start Page	BBSM Hotspot automatically enters the Start page for the network device, based on the web page set. If you want to change the Start page, enter the complete URL for your web page.
Bandwidth Per User *(RADIUS or free access web pages only)*	*This field is enabled only when RADIUS or free access web pages are being used.* From the drop-down menu, choose the desired bandwidth throttling value, in kbps, for clients connected to this network device. The bandwidth is effective only if bandwidth throttling is turned on. (Refer to the "Configuring Server Settings" section on page 3-2.) If you select a web page that gives the end user a bandwidth choice, that selection overrides this setting. The default is "Full-Speed." **Note** If you are using a web page that supports several access types, such as Hotspot, HotspotClear, or a custom web page, the Bandwidth Per User field is enabled only to support end users that connect using RADIUS. End users that connect using credit cards will still be choosing their own bandwidth when they connect. In addition, if the RADIUS server is configured to send back a particular bandwidth when the user connects, that bandwidth overrides any bandwidth chosen by using the Port Settings window.
Enable Port Hopping	Check this check box to enable port hopping.
Client IP Address Range (DHCP) *(multinets only)*	*This field only appears when you are using multinets.* If you are using multiple networks, click the default multinet number for clients connected to this network device: Multinet 1 or Multinet 2. **Note** If you select a web page set that gives the end user the choice of a public or private IP address, that selection overrides this setting.
Buttons	
Submit	Enters the changes you have made.
Reset	Before you have submitted the changes, resets the data to the stored information.
Cancel	Cancels any changes.

Configuring Switches

Use the following procedure to configure each switch. Most installations have two types of switches: base switches and client switches:

- A base switch, also known as an aggregation switch, provides connections to client switches.
- Client switches provide connections to clients, such as laptops.

Unused ports on the base switch can be used as client ports if the base switch is added to the Switches web page and if a sufficient number of switch ports are available. When the base switch is also being used as a client switch, the ports connected to client switches must be marked as uplink.

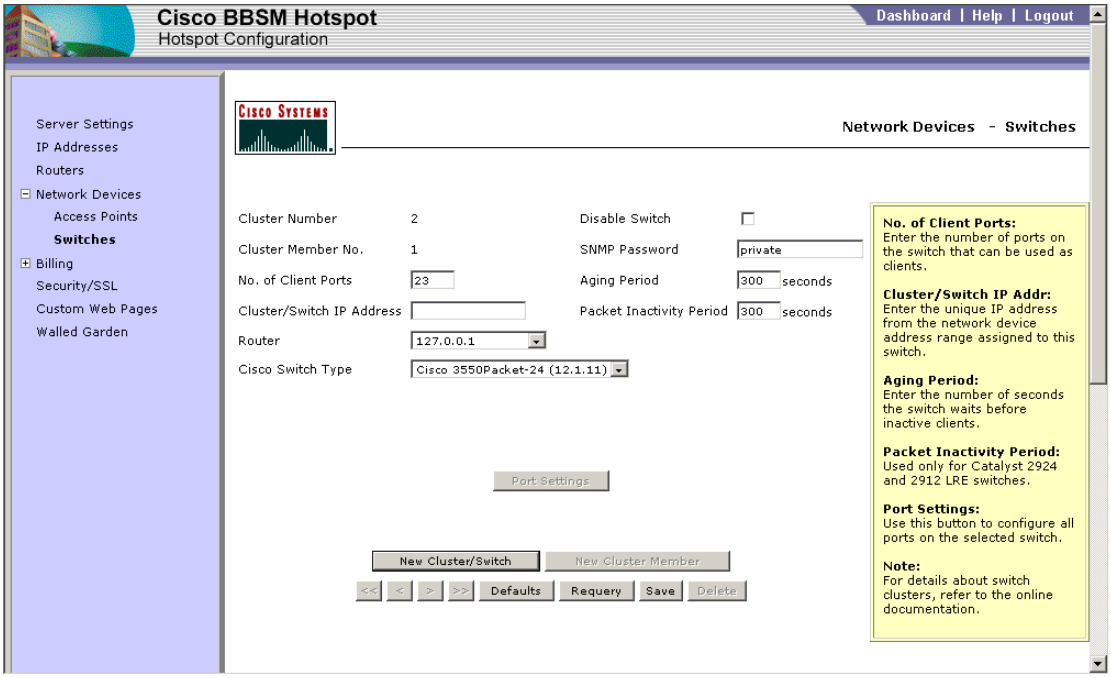
You can also refer to the following sections:

- For instructions on how to mark a port for uplink, refer to Configuring Ports (Port Configuration), page 3-27.
- For additional information about switch clustering, refer to Cisco Switch Clustering, page 2-40.

Step 1 From the Dashboard, click **Hotspot Configuration**. The Server Settings web page appears.

Step 2 In the NavBar, navigate to the Switches web page by choosing **Network Devices > Switches**. The Switches web page appears. (See Figure 3-8.)

Figure 3-8 Switches Web Page



Step 3 Configure the switches, based on the information shown in Table 3-7, and then click **Save**. The Network Devices - Port Settings window appears. (See Figure 3-7 on page 3-12.) (If port configuration records already exist, the Network Devices - Port Settings window does not pop up automatically. Click **Port Settings**.)

Step 4 Enter the applicable information, based on the information in Table 3-6 on page 3-13.

Step 5 To save the data, click **Submit**. You are returned to the Switches web page.

Table 3-7 Switches Web Page Options

Field	Description
Cluster Number Cluster Member No.	Displays the cluster and member number associated with the switch to be configured.
No. of Client Ports	Enter the number of ports that can be used as clients on switch 1 of the cluster or a single switch. The default is 24.
Cluster/Switch IP Address	Enter a unique IP address in the network device IP address range assigned to the cluster. Check with the person installing your clusters and switches if you are unsure of this IP address. **Note** If you are not using clustering, just enter the IP address of your switch.
Router	From the drop-down menu, choose the IP address of the router that this site and cluster are connected to. If the site and cluster are directly connected to the BBSM Hotspot server, use the default IP address for the BBSM Hotspot server, which is "127.0.0.1."
Cisco Switch Type	From the drop-down menu, select the supported switch type, such as Cisco Catalyst 2950. For a list of supported switch types, refer to the following web site: http://www.cisco.com
Disable Switch	Check this check box if you do not want BBSM Hotspot to look for clients on the cluster ports. Use this feature when troubleshooting or when the switch is not yet installed on the network. (If you disable a switch, its IP address remains reserved. If you need to reuse the IP address for a different switch, change the IP address of the disabled switch temporarily; otherwise, you will not be able to update Hotspot Configuration.)
SNMP Password	Enter the SNMP password (community string) that is used when communicating with switches. **Note** We recommend that the default password on the switches and on BBSM Hotspot be changed, because the default password is well known and could compromise network security.
Aging Period	Enter the number of seconds that the network device will wait before eliminating inactive clients from its internal tables, which causes BBSM Hotspot to automatically sign off the client. The default time period is 300 seconds (5 minutes).
Packet Inactivity Period	*This field is disabled for any switch type that does not support packet activity.* Enter the number of seconds that a user can be idle before being automatically signed off by BBSM Hotspot.
Buttons	
Port Settings	Click to configure the settings for all ports on this switch. The Network Devices - Port Settings window appears. Enter the correct information, as described in Table 3-6 on page 3-13, and then click **Submit**.
New Cluster/Switch	Adds a new cluster to the site. A new web page appears with blank fields so the new cluster and the associated switches can be configured.
New Cluster Member	Adds a new network device to an existing cluster. A new web page appears with blank fields so the associated parameters can be configured. Note that if a switch is not cluster capable or not configured as a cluster switch, BBSM Hotspot considers the switch as a cluster of a single switch.
Defaults	Displays the default parameter settings.
Requery	Before you have saved any changes, click to return the web page to the previously saved settings.
Save	Saves the changes made to the web page.
Delete	Deletes the switch.

Configuring Billing Options

If you want to bill end users for Internet access, instead of allowing free access, you must decide which billing options you want to use—RADIUS, credit cards, and/or access codes—and then configure BBSM Hotspot for the options. BBSM Hotspot supports any combination of these billing options.

Access codes do not require any special configuration. For information on access codes, refer to Managing Access Codes, page 4-15.

The following sections describe how to configure these options.

Configuring Credit Card Billing

If you are using credit card billing, you must configure a credit card authorization server. This section also describes how to configure and test the credit card interface.

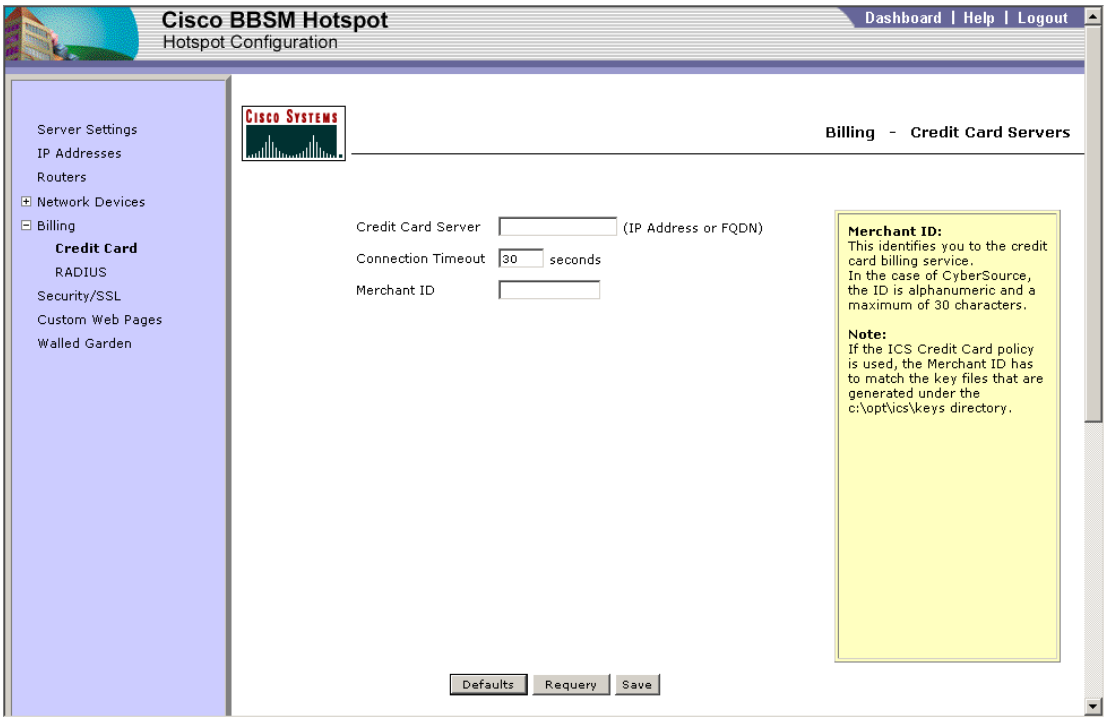
Configuring the Credit Card Billing Options

Use the following procedure to configure the credit card billing options.

Step 1 From the Dashboard, click **Hotspot Configuration**. The Server Settings web page appears.

Step 2 In the NavBar, navigate to the Credit Card web page by choosing **Billing > Credit Card**. The Server web page appears. (See Figure 3-9.)

Figure 3-9 Credit Card Web Page



Step 3 Configure the credit card options, as described in Table 3-8.

Step 4 To save the changes, click **Save**.

Table 3-8 Credit Card Web Page Options

Field	Description
Billing Server Address	Enter the IP address or FQDN for the credit card server. The FQDN is limited to 100 characters.
Connect Timeout	Enter the number of seconds during which BBSM Hotspot attempts to connect to the credit card server. The default is 30 seconds.
Merchant ID	Enter the merchant ID. This identifier specifies the merchant, such as the hotel or hotspot owner, that originates the charges being sent to the credit card billing service provider, such as CyberSource. If the credit card billing service provider is CyberSource, the merchant ID must be alphanumeric with a maximum of 30 characters. Other credit card billing service providers may have different rules for the format of the merchant ID. **Note** For the ICS Credit Card accounting policy that ships with BBSM Hotspot, the merchant ID has to match the name of the key files generated under c:\opt\ics\keys directory.
Buttons	
Defaults	Displays the default parameter settings.
Requery	Before you have saved any changes, click to return the web page to the previously saved settings.
Save	Saves the changes made to the web page.

Testing the Credit Card Interface

BBSM Hotspot performs credit card authentication and billing through the CyberSource ICS billing server. Before deploying BBSM Hotspot, the credit card interface needs to be tested to make sure that it functions properly.

Use the following procedure to test the interface.

Step 1 Set up an account for testing. At the CyberSource website, www.cybersource.com/register, fill out the form to obtain the free testing account.

Step 2 Wait for a response email from CyberSource that contains the merchant ID.

Step 3 Download the ecert program from CyberSource and use it to create the needed keys.

a. From a DOS window, navigate to this directory:

c:\opt\ics\keys

b. Enter this command: Ecert <merchant ID>.)

See the following example:

```
C:\opt\ics\keys>ecert test1
   The application will now send the newly created key pair and
      certificate request to the server.

   Merchant id, test1
   Server host name, setup.ic3.com
   Server port number, 80

   This process will add your new keys into the test environment.

   Certificate generation completed successfully

Merchant password data written to, C:\opt\ics\keys\test1.pwd
Merchant certificate data written to, C:\opt\ics\keys\test1.crt
Merchant private key data written to, C:\opt\ics\keys\test1.pvt
Server certificate data written to, C:\opt\ics\keys\
   CyberSource_SJC_US.crt

You are now ready to access the CyberSource test server. Upon request
CyberSource will activate your newly generated keys in the production
environment. At that time a CyberSource employee will verbally confirm your
password as given below, please make a note of it.

Certificate generation verification password, 9999-9999-9999-99999-99999

C:\opt\ics\keys>
```

Step 4 On the Dashboard, click **Hotspot Configuration**. The BBSM Hotspot Server Settings web page appears.

Step 5 Enter the billing server address and connect timeout:

- **a.** Navigate to the Credit Server web page by choosing **Billing > Credit Card**.
- **b.** In the Credit Card Server field, enter the IP address or FQDN of the signed credit card server; for example, MyCreditCardServer.com.
- **c.** In the Connect Timeout Seconds field, enter the number of seconds that BBSM Hotspot attempts to validate a credit card before rejecting the end user's input.
- **d.** In the Merchant ID field, enter the merchant ID.
- **e.** To save the changes, click **Save**.

Step 6 Enter the currency type:

- **a.** In Hotspot Configuration, click **Server Settings**. The Server Settings web page appears.
- **b.** From the drop-down menu, enter the local currency type that the credit card server uses. Note that this currency type will be the currency type that the entire BBSM Hotspot server uses. The default is USD (U.S. dollars).
- **c.** To save the changes, click **Save**.

Step 7 Select the appropriate web page, such as MinuteICS/MinuteICSClear, BlockICS/BlockICSClear or DailyICS/DailyICSClear:

- **a.** Navigate to the **Access Points** or **Switches** web page (depending on your usage) by choosing **Network Devices > Access Points (or Switches)**.
- **b.** To access the Network Devices - Port Settings pop-up window, click **Port Settings**.
- **c.** From the Page Set drop-down menu, select **MinuteICS** or **MinuteICSClear**:

- If you have SSL installed, select **MinuteICS**.
- If you do not have SSL installed, select **MinuteICSClear**.

d. To save the changes, click **Save**.

Step 8 From a laptop, verify that you can access the Internet through the selected web page:

a. Connect a client to the BBSM Hotspot network and open the browser. The Start page appears.

b. Enter valid names and addresses.

c. Enter the credit card number and expiration dates provided by CyberSource:

- For the credit card number, enter **4111111111111111** (the number 4 followed by 15 ones)
- For the expiration date, from the drop-down menus, choose a month and year, such as **07(JUL) 2005**.

d. Click **Submit**. You will soon be connected to the Internet. Once connected, browse for at least 2 minutes before disconnecting.

Step 9 Verify with CyberSource that the transactions were successful by logging onto the following website:

```
http://icstest.ic3.com/cs/search_request.pl
```

a. To logon, use your Merchant ID as both the user name and password.

b. Do a search for ALL, Today's Requests.

c. Check under services that you get an Auth and a Bill.

Configuring RADIUS Billing

If you are using RADIUS for billing, you must configure BBSM Hotspot to operate as a RADIUS client. Configuring BBSM Hotspot for RADIUS billing allows BBSM Hotspot clients to be authenticated against a RADIUS server

BBSM Hotspot provides support for prepaid RADIUS accounts, which are configured on the RADIUS server. For prepaid RADIUS accounts, after the end user is authenticated, a web page appears that tells the user how many minutes are left on the account. Then the user clicks Continue and is taken to the configured web portal. The disconnect window shows the countdown of the minutes remaining until the session ends. At the end of the session, the window displays that the user is out of time, and the session terminates.

For additional information using RADIUS, see the "Using RADIUS with BBSM Hotspot" section on page 2-34.

Note You must install an SSL certificate to allow secure communication between the client and BBSM Hotspot. Refer to Appendix B, "Installing an SSL Certificate."

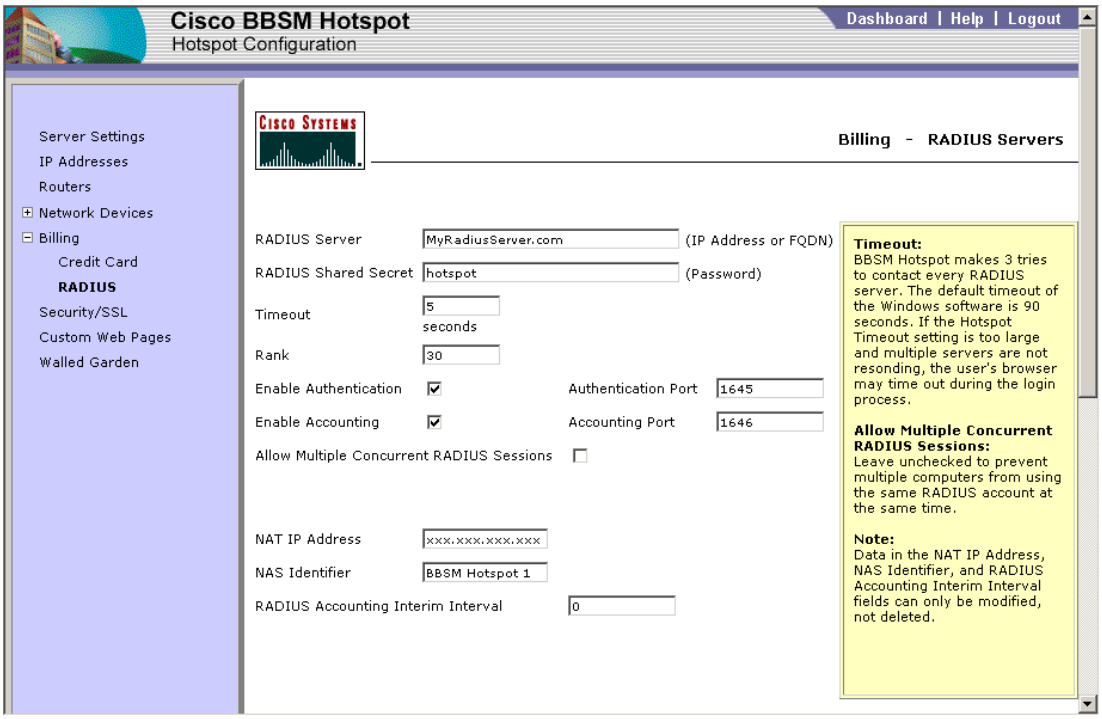
Use the following procedure to configure the RADIUS server billing options.

This procedure assumes that you have already run the Setup Wizard to configure the ports to use either the RADIUS page set or a custom page set. (Refer to the "Running the Setup Wizard" section on page 2-2.)

Step 1 From the Dashboard, click **Hotspot Configuration**. The Server Settings web page appears.

Step 2 In the NavBar, navigate to the RADIUS web page by choosing **Billing > RADIUS**. The RADIUS web page appears. (See Figure 3-10.)

Figure 3-10 RADIUS Web Page



Step 3 Configure the RADIUS server parameters, as described in Table 3-9.

Step 4 To save the changes, click **Save**.

Table 3-9 RADIUS Options

Field	Description
RADIUS Server	Enter the IP address or FQDN of the RADIUS server. The DNS name can contain a maximum of 64 characters.
RADIUS Shared Secret	Enter the RADIUS client password used to access the RADIUS server.
Timeout	Enter the number of seconds that the BBSM Hotspot server waits before attempting to access the RADIUS server a second or third time or before going to the next RADIUS server. Note that BBSM Hotspot 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. **Note** 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 and more than one RADIUS server is unavailable, the total time period during which BBSM Hotspot attempts to contact the RADIUS servers may be greater than the timeout period for the browser itself. This will cause the end-user's browser to time out during authentication. For example, if the timeout period set is 20 seconds and two RADIUS servers are not responding, BBSM Hotspot attempts to contact the first RADIUS server three times within 60 seconds. If BBSM Hotspot 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 Hotspot finishes searching for the second RADIUS server.
Rank	Enter the order in which the BBSM Hotspot server attempts to contact RADIUS servers to authenticate a user. The BBSM Hotspot server contacts servers in ascending order of rank. The default is 30.
NAT IP Address	If the BBSM Hotspot server is behind a NAT router, enter the public IP address that the router assigned to the BBSM Hotspot server. If the field is left blank, the RADIUS access policy uses the IP address of the external NIC. (Deleting the RADIUS server will not clear the data in this field. To clear this data, you must manually clear it and click Save.) **Note** Changing this IP address for one RADIUS server changes it for all previously configured RADIUS servers.
NAS Identifier	Enter a unique server identifier, such as "BBSM HotspotServer1." 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. (Deleting the RADIUS server will not clear the data in this field. To clear this data, you must manually clear it and click Save.) **Note** Changing the NAS identifier for one RADIUS server changes it for all previously configured RADIUS servers.
RADIUS Accounting Interim Interval	Enter 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. (Deleting the RADIUS server will not clear the data in this field. To clear this data, you must manually clear it and click Save.) **Note** Changing the RADIUS accounting interim interval for one RADIUS server changes it for all previously configured RADIUS servers.
Enable Authentication	Check to enable BBSM Hotspot to verify the username and password with this RADIUS Authentication server (Authentication Access-Request message).
Authentication Port	Enter the TCP port on the BBSM Hotspot server that the RADIUS server uses to communicate with the RADIUS authentication server. The default is 1645.

Table 3-9 RADIUS Options (continued)

Field	Description
Enable Accounting	Check to enable BBSM Hotspot to contact this RADIUS Accounting server to log the Start, Interim-Update Accounting, and Stop accounting messages.
Accounting Port	Enter the TCP port on the BBSM Hotspot server that the RADIUS server uses to communicate with the RADIUS accounting server. The default is 1646.
Allow Multiple Concurrent RADIUS Sessions	Check this check box to enable a RADIUS user to have a BBSM Hotspot session active on more than one client at the same time. Leaving it unchecked prevents multiple clients from using the same RADIUS account at the same time.
Buttons	
New	Click to enter a new RADIUS server. A new RADIUS web page appears the parameters can be configured.
Requery	Before you have saved any changes, click to return the web page to the previously saved settings.
Save	Saves the changes made to the web page.
Delete	Deletes the RADIUS server.

Configuring Security/SSL

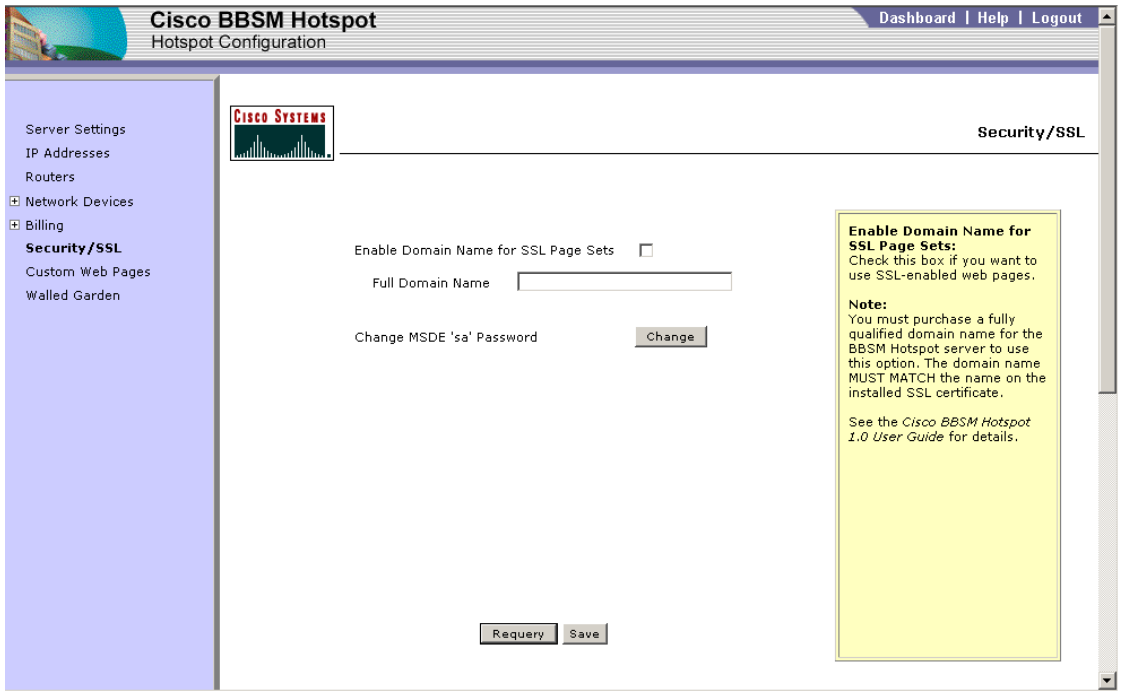
For securing client-BBSM Hotspot communication, you must enable the SSL protocol and specify the associated domain name. This section also describes how to change the MSDE ‘sa’ password.

Follow the steps below to configure SSL and change the MSDE password.

Step 1 From the Dashboard, click **Hotspot Configuration**. The BBSM Hotspot Server Settings web page appears.

Step 2 In the NavBar, click **Security/SSL**. The Security/SSL web page appears. (See Figure 3-11.)

Figure 3-11 Security/SSL Web Page



Step 3 Configure the security options, based on the information shown in Table 3-10.

Table 3-10 Security/SSL Web Page Options

Field	Description
Enable Domain Name for SSL Web Pages	Check this check box if you want to use SSL-enabled web page sets. **Note** You must purchase a fully qualified domain name for the BBSM Hotspot server to use SSL security. Refer to Appendix B, "Installing an SSL Certificate."
Full Domain Name	Enter the full domain name for the BBSM Hotspot server that web page sets will use to reach the BBSM Hotspot server. This domain name must match the name on the SSL certificate that is installed on BBSM Hotspot; for example, cisco.com. This is the name entered in Appendix B, "Installing an SSL Certificate." "Generating a Certificate Signing Request" section on page B-2, Step 13.
Change MSDE 'sa' Password	Click **Change** to access the MSDE 'sa' Password Form, and change the password. (Refer to "Changing the MSDE 'sa' Password" section on page 2-25.)
Buttons	
Requery	Before you have saved any changes, click to return the web page to the previously saved settings.
Save	Saves the changes made to the web page.

Step 4 To save the changes, click **Save**.

Adding Custom Web Pages to BBSM Hotspot

The web page set configured for a port controls the GUI displayed to the end users connecting on that port and how the users are authenticated for Internet access. You can use the BBSM Hotspot default web page sets or you, or your web developer, can create either completely new web pages or customize existing web pages by modifying the BBSM Hotspot default web pages. Refer to the following information about customizing web page sets:

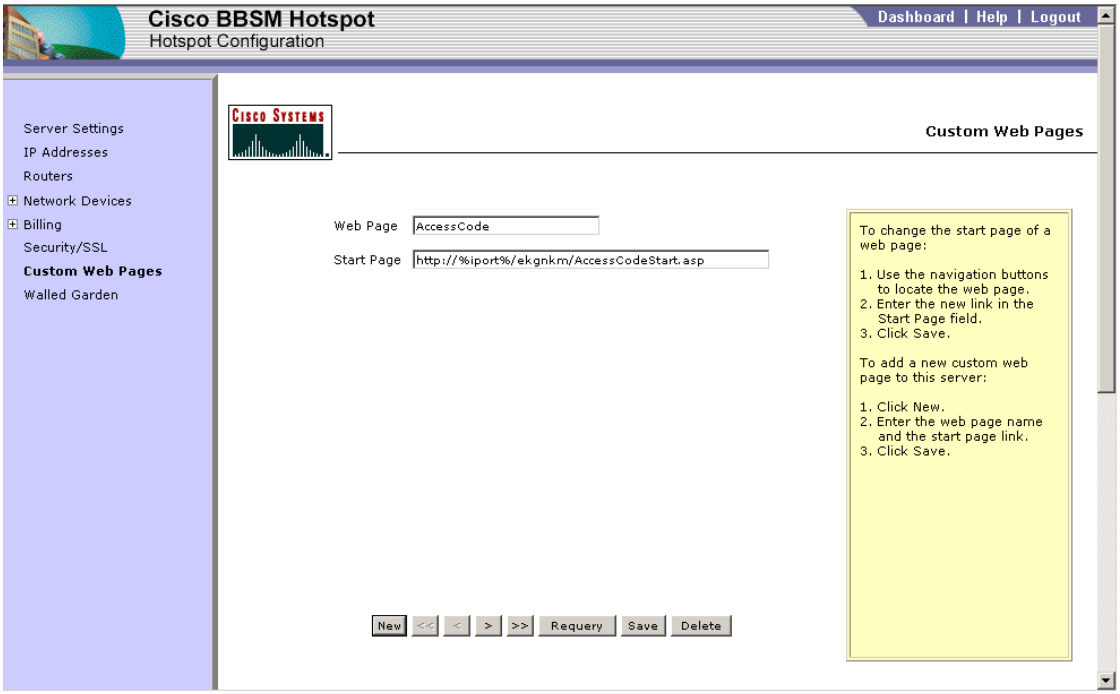
- To create a custom web page set using the Custom Web Page Wizard, refer to the following section, Using the Custom Web Page Wizard, page 3-32. The custom web page that you create is added automatically to BBSM Hotspot. You do not need to add the page manually.
- For information on manually creating a custom web page, refer to the *Cisco BBSM 5.2 SDK Developer Guide*. If necessary, contact the Cisco TAC to be sure that BBSM Hotspot can support the web page that you would like to create. Refer to the Obtaining Technical Assistance section in the Preface to this user guide.
- For an overview of web page sets and the BBSM Hotspot default web pages, refer to the "Using Web Pages" section on page 2-32.

After you manually create a custom web page set, you must add it to the list of available web pages in BBSM Hotspot. Use the following procedure to add the custom web page set.

Step 1 From the Dashboard, click **Hotspot Configuration**. The Server Settings web page appears.

Step 2 In the NavBar, click **Custom Web Pages**. The Custom Web Pages web page appears. (See Figure 3-12.)

Figure 3-12 Custom Web Pages Web Page



Step 3 Add the custom web page to BBSM Hotspot, based on the information shown in Table 3-11.

Step 4 To save the information, click **Save**.

Table 3-11 Custom Web Pages Options

Field	Description
Web Page	Enter the name of the web page set.
Start Page	Enter the complete URL of the Start page for your web page. The URL must be in the form "http://%iport%...," because BBSM Hotspot translates %iport% to be either the BBSM Hotspot internal IP address or the BBSM Hotspot domain name, if applicable.
Buttons	
New	Click to enter a new web page. A new blank web page appears so the web page and Start page can be added.
Requery	Before you have saved any changes, click to return the web page to the previously saved settings.
Save	Saves the changes made to the web page.
Delete	Deletes this web page.

Configuring Walled Gardens

BBSM Hotspot allows you to define free access to specific websites. This subset of the Internet that unauthenticated BBSM Hotspot end users can access is called a *walled garden*. These walled gardens offer you the opportunity to increase revenue by marketing various services to your guests, which in turn reduces your costs.

The following are typical walled garden links:

- Local weather and attractions
- Business traveller loyalty program portals
- Vendor services, such as car rental agencies

BBSM Hotspot defines each site in a walled garden by a full domain name, a network IP address, and a network subnet mask.

End users normally access walled garden sites through links on the Start page. If you want some ports to have access to walled garden sites, while other ports do not, create different Start pages for the applicable ports.

To add walled garden functionality to your web page sets, your web developer modifies the web pages with links to the walled garden sites.

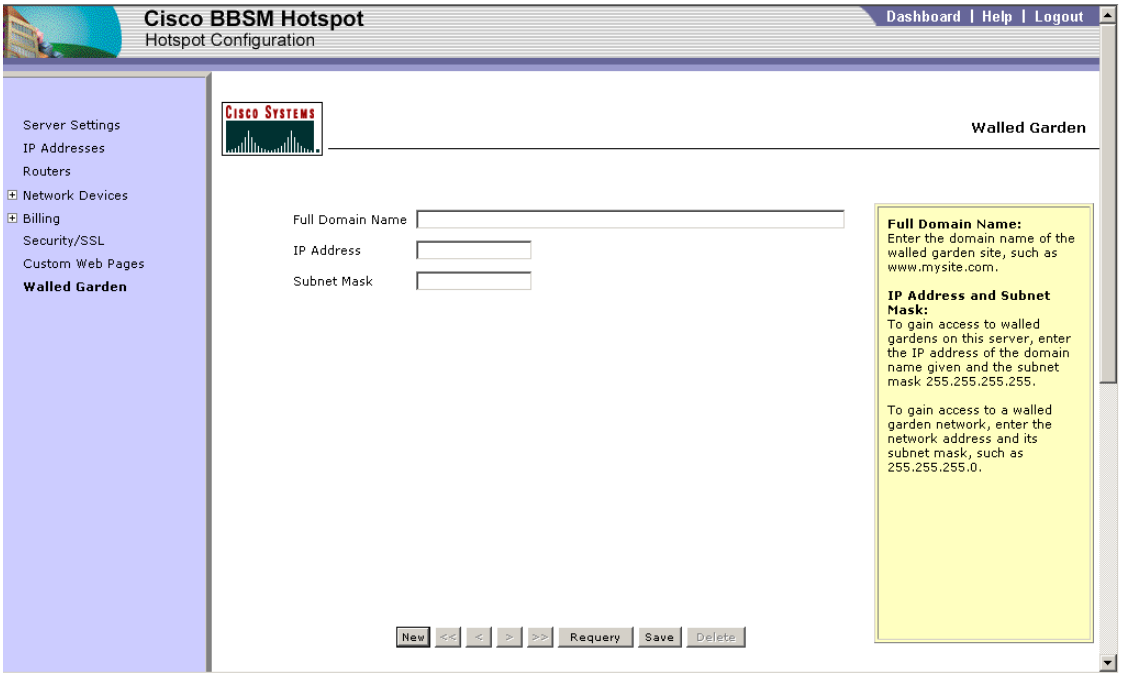
Caution Configuring an excessive number of walled garden sites (100+) can impact BBSM Hotspot server performance.

Use the following procedure to establish each walled garden site.

Step 1 From the Dashboard, click **Hotspot Configuration**. The Server Settings web page appears.

Step 2 In the NavBar, select **Walled Garden**. The Walled Garden web page appears. (See Figure 3-13.)

Figure 3-13 Walled Garden Web Page



Step 3 Configure the Walled Garden options, based on the information shown in Table 3-12.

Step 4 To save the changes, click **Save**.

Step 5 Use a client to open a browser and test access to your walled gardens. If the page looks incomplete, the walled garden website may be using several servers for page content. You must enter a domain name, IP address, and subnet mask for each of the these servers.

Table 3-12 Walled Garden Web Page Options

Field	Description
Full Domain Name	Enter the domain name of the walled garden website; for example, www.cisco.com.
IP Address Subnet Mask	To gain access to walled gardens on a server, enter the domain name's IP address and the subnet mask of 255.255.255.255; for example, where: www.cisco.com = 198.133.219.25: • IP address = 198.133.219.25 • Subnet mask = 255.255.255.255 To gain access to walled gardens on a network, enter the network address and the subnet mask; for example, where: www.cisco.com = 198.133.219.25 business.cisco.com = 198.133.219.124 newsroom.cisco.com = 198.133.219.119 To add all three of these Cisco URLs to the walled garden list, you could enter them all individually, as in the first example, or because they are all on the same subnet (all start with 198.133.219.x), you can enter all of them with just one entry: • IP address = 192.133.219.0 • Subnet mask = 255.255.255.0 The x.x.x.0 tells BBSM Hotspot that the walled garden is a group of addresses, not just a single IP address. All IP addresses on the 198.133.219.x subnet are now part of the walled garden. This includes the range of addresses from 198.133.219.1 to 198.133.219.255. Different subnet masks will include different ranges of IP addresses.
Buttons	
New	Click to enter a new walled garden site. Text fields on the page are cleared so that new data can be entered.
Requery	Before you have saved any changes, click to return the web page to the previously saved settings.
Save	Saves the changes made to the web page.
Delete	Deletes this website from BBSM Hotspot.

Configuring Ports (Port Configuration)

This section describes how you can update network device port data by using the Port Configuration tool. This section is divided into two subsections:

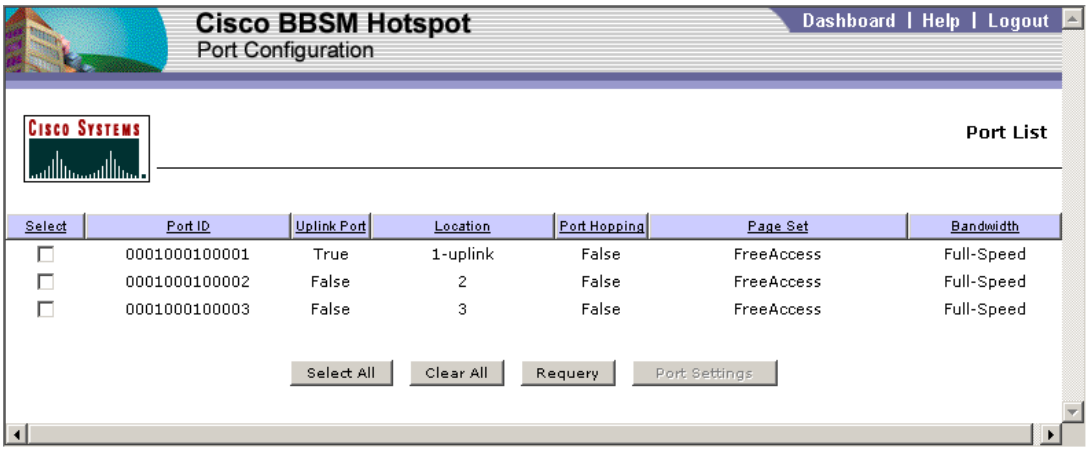
- Changing Port Settings for One Port, page 3-28—How to change the port data for one port on a single switch or access point.
- Changing Port Settings for More than one Port, page 3-31—How to change the port data for more than one port on switches and access points.

Changing Port Settings for One Port

Use the following procedure to change the port data for one port on a switch or access point.

Step 1 From the Dashboard, click **Port Configuration**. The Port List web page appears. (See Figure 3-14.)

Figure 3-14 Port List Web Page

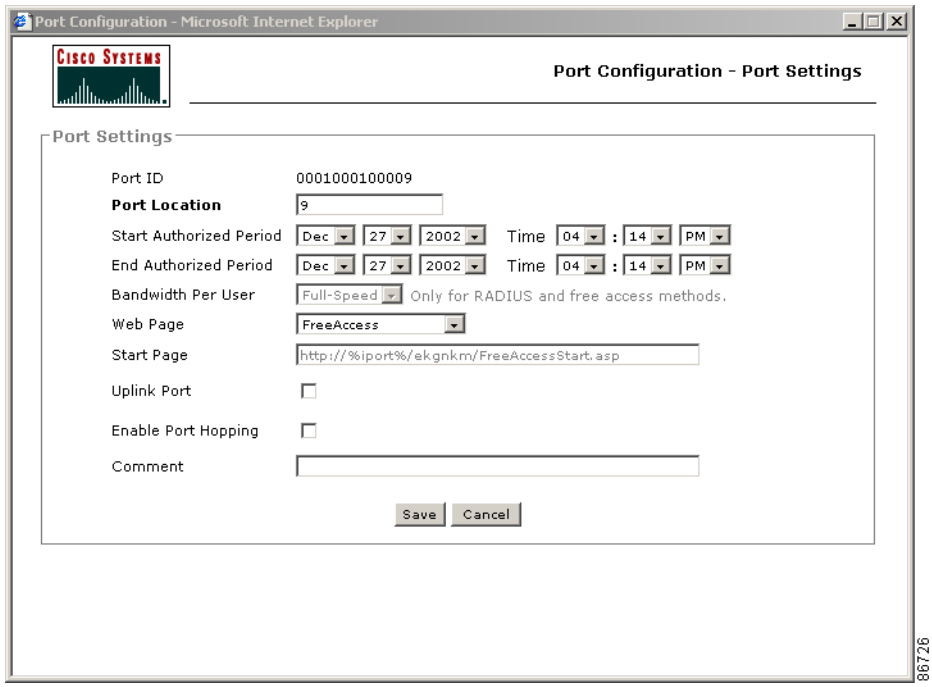


Step 2 In the left-hand column, check the port that you want to update. (To return the web page to the previously saved settings, click **Requery**.)

Step 3 Click **Port Settings**. The Port Configuration - Port Settings window for a single port change appears. (See Figure 3-15.)

Note If the fields displayed in the Port Settings window do not match the port that was checked in the Port List, press **F5** to refresh the window.

Figure 3-15 Port Configuration - Port Settings Window for One Port (Singlenet Example)



Step 4 Make the desired changes, based on the information in Table 3-13.

Step 5 To save the port changes that you made, click **Save**. A confirmation dialog box appears to indicate that the changes were successful.

Step 6 To close the dialog box, click **OK**. You are returned to the Port List web page.

Table 3-13 Port Configuration - Port Settings Field Descriptions

Field	Description
Port Settings	
Port ID	Displays the unique number automatically assigned to each port during the Network Devices port configuration. This number cannot be changed. The port ID incorporates the cluster, switch, and port number on the switch. The format is xxxxyyyyzzzzz, where xxxx is the cluster, yyyy is the switch, and zzzzz is the port.
Port Location	Enter the location associated with this port. This location can be a number or text.
Start Authorized Period *(not used)*	*This field is not used.*
End Authorized Period *(not used)*	*This field is not used.*
Bandwidth Per User *(RADIUS and free access web pages only)*	*This field is enabled only when RADIUS or free access web pages are being used.* From the drop-down menu, choose the desired bandwidth throttling value, in kbps, for clients connected to this network device. The bandwidth is effective only if bandwidth throttling is turned on. (Refer to the "Configuring Server Settings" section on page 3-2.) If you select a web page that gives the end user a bandwidth choice, that selection will override this default setting. The default is "Full-Speed." **Note** If you are using a web page that supports several access types, such as Hotspot, HotspotClear, or a custom web page, the Bandwidth Per User field is enabled only to support end users that connect using RADIUS. End users that connect using credit cards will still be choosing their own bandwidth when they connect. In addition, if the RADIUS server is configured to send back a particular bandwidth when the user connects, that bandwidth overrides any bandwidth chosen by using the Port Settings window.
Web Page	From the drop-down menu, choose the desired web page set. For descriptions of the default web pages that ship with BBSM Hotspot, refer to Table 2-10 on page 2-34. **Note** If you will be using SSL and have not yet installed your SSL certificate, select the "Clear" version of the web page until you install the certificate and then change your web page to the SSL web page. For example, select RADIUSClear until the certificate is installed, then after installing the certificate, change the web page to RADIUS. If you install the SSL web page before installing the certificate, the Start page will not display.
Start Page	*This field is autogenerated based on the web page selected and is read only.*
Uplink Port	Check this check box if the port is used as an uplink to another switch. For these uplink ports, BBSM Hotspot ignores MAC addresses so it does not report that clients are connected to the ports.
Enable Port Hopping	Check this check box if you want to enable port hopping.
Client IP Address Range (DHCP) *(multinets only)*	**Note** If you are using multiple networks, click the default multinet number for clients connected to this network device: Multinet 1 or Multinet 2. This setting determines the final multinet that the client will use after accepting the service. If you select a web page set that gives the end user the choice of a public or private IP address, that selection overrides this setting.
Comment	Use this field to enter additional information about this port.
Buttons	
Save	Saves the changes that were made.
Cancel	Cancels the changes and returns you to the Port Configuration web page.

Changing Port Settings for More than one Port

Use the following procedure to change the port data for more than one port.

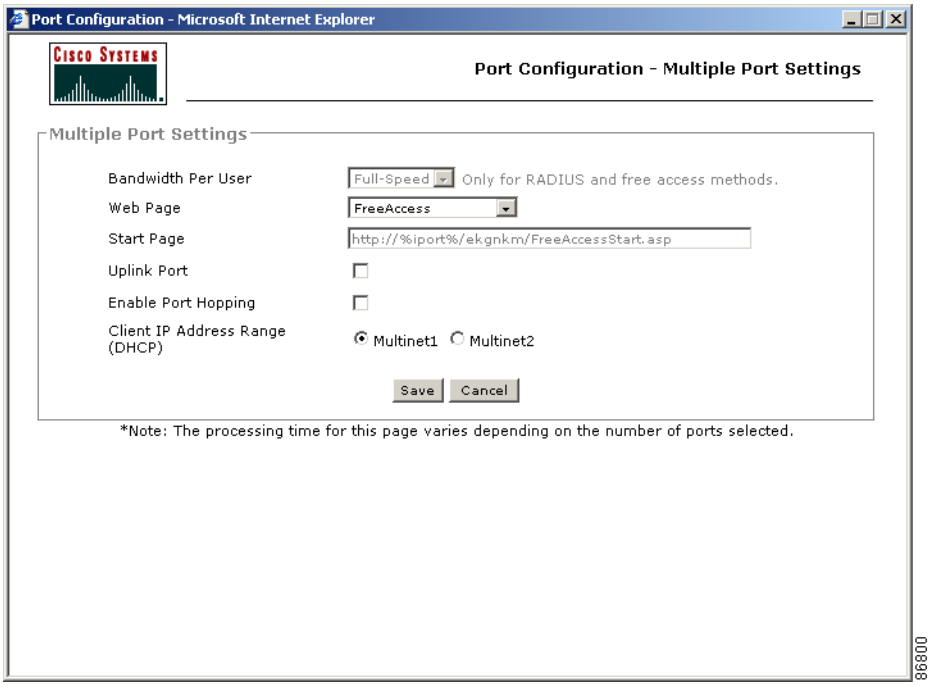
Step 1 From the Dashboard, click **Port Configuration**. The Port Configuration web page appears. (See Figure 3-14.)

Step 2 In the left-hand column, check the ports that you want to update. If you want to select all of the ports, click **Select All**.

Step 3 Click **Port Settings**. The Port Configuration - Multiple Port Settings window for multiple port changes appears. This example show a multinet configuration. (See Figure 3-16.)

Note If the fields displayed in the Port Settings window do not match the ports that were checked in the Port List, press **F5** to refresh the window.

Figure 3-16 Port Configuration - Multiple Port Settings Window (Multinet Example)



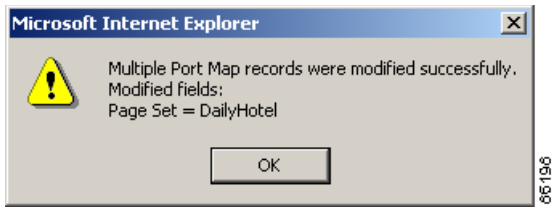
Step 4 Make the desired changes, based on the field descriptions shown in Table 3-13.

Note When multiple ports are selected, the options available from the Port Settings window are only those that apply to a group of ports.

Step 5 Confirm the changes by checking the Port Configuration window.

Step 6 To save the port changes that you made, click **Save**. A confirmation dialog box appears to show that the changes were successful, what fields were changed, and the changed values. (See Figure 3-17.)

Figure 3-17 Confirmation Dialog Box



Step 7 Click **OK** to close the dialog box. You are returned to the Port Configuration web page.

Using the Custom Web Page Wizard

The Custom Web Page Wizard tool is located under Configuration on the Dashboard. This tool allows the administrator to easily create a basic custom web page. You can also use the Custom Web Page Wizard to modify or delete an existing custom web page that was created with the wizard.

The wizard allows you to add a photo and a logo to each new web page. These graphics must conform to maximum height and width requirements. The wizard automatically adds the new web page to the web page drop-down list of web pages in the Network Devices - Port Settings pop-up window.

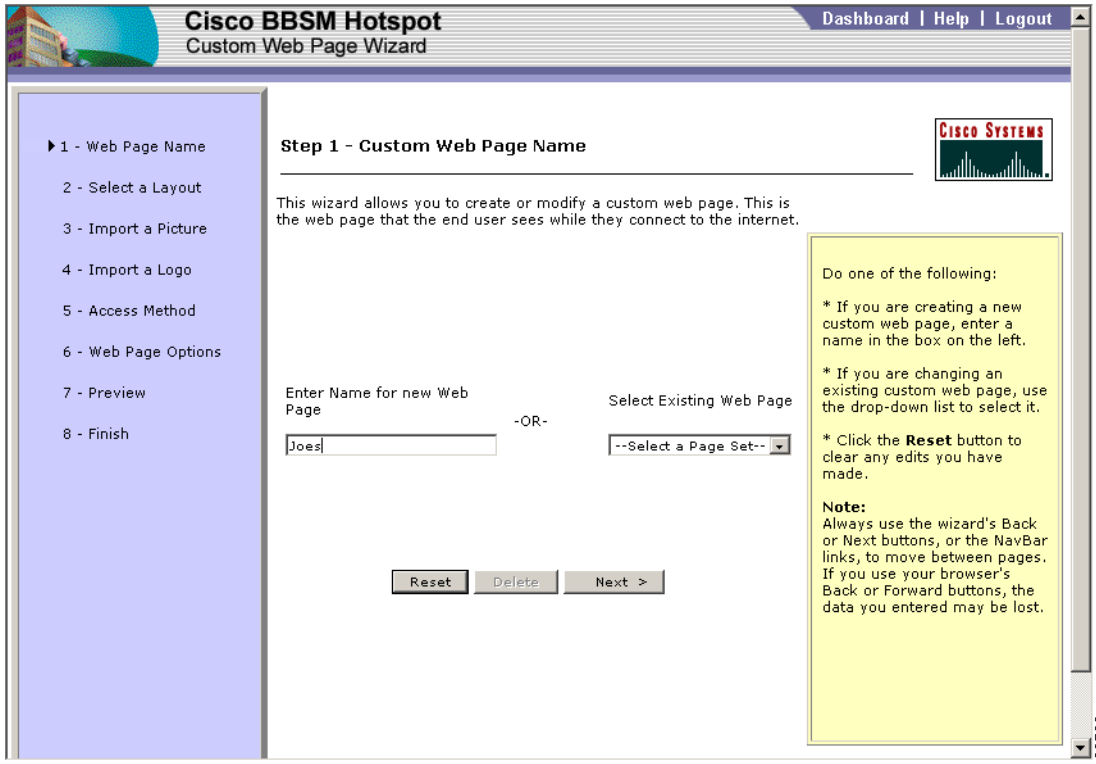
Caution Be sure to close all active sessions before running any BBSM Hotspot wizard, including the Custom Web Page Wizard. Refer to the "Deactivating Client Sessions" section on page 4-21.

Note When running the wizard, you must use the web page navigation buttons, such as Back and Next. If you click the Internet Explorer browser's **Back** button, your changes will be lost.

Use the following procedure to create a new custom web page:

Step 1 From the Dashboard, click **Custom Web Page Wizard**. The Step 1 - Custom Web Page Name web page appears. (See Figure 3-18.)

Figure 3-18 Step 1 - Custom Web Page Name Web Page

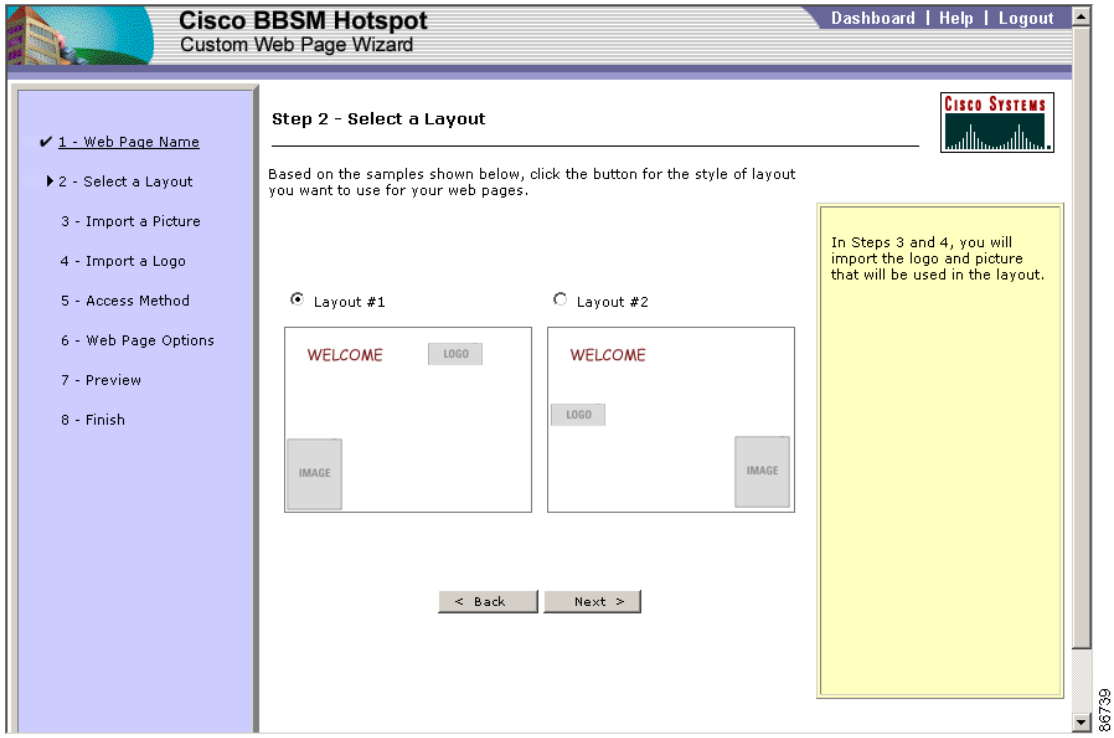


Step 2 Do one of the following, based on whether you are creating a completely new web page, changing an existing one that was created earlier with this wizard, or deleting a web page:

- If you are creating a completely new web page, in the Enter Name for New Web Page field, enter the web page name.
- If you are changing an existing web page that was created with this wizard, from the Select Existing Web Page drop-down menu, choose the web page that you want to change.
- If you are deleting a web page, from the Select Existing Web Page drop-down menu, select the desired web page. Then click **Delete**. The web page is deleted.

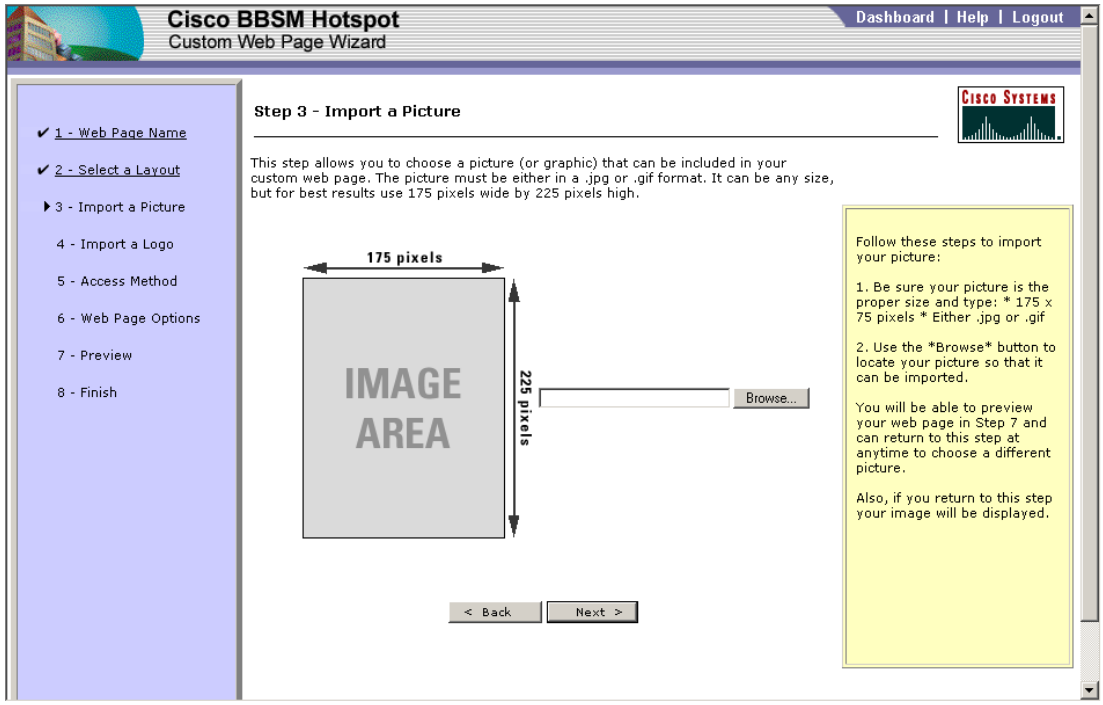
Step 3 Click **Next**. The Step 2 - Select a Layout web page appears. (See Figure 3-19.)

Figure 3-19 Step 2 - Select a Layout Web Page



Step 4 Click the desired web page layout, and then click **Next**. The Step 3 - Import a Picture web page appears. (See Figure 3-20.)

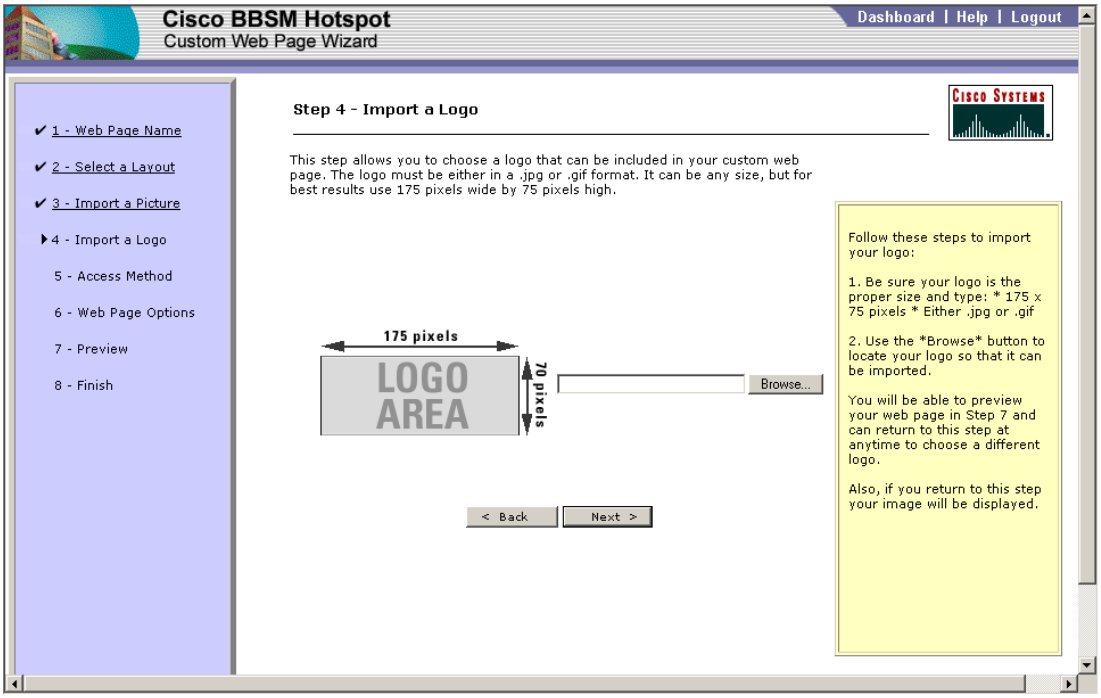
Figure 3-20 Step 3 - Import a Picture Web Page



Step 5 If you want to add a picture to the Start page at this time, click **Browse** to navigate to the file of the picture. The picture should be 175 by 225 pixels or smaller. (If you do not want to add a picture now, leave the file name blank.) Then click **Next**. The Step 4 - Import a Logo web page appears. (See Figure 3-21.)

Note If you added a picture, click **Back** to view it.

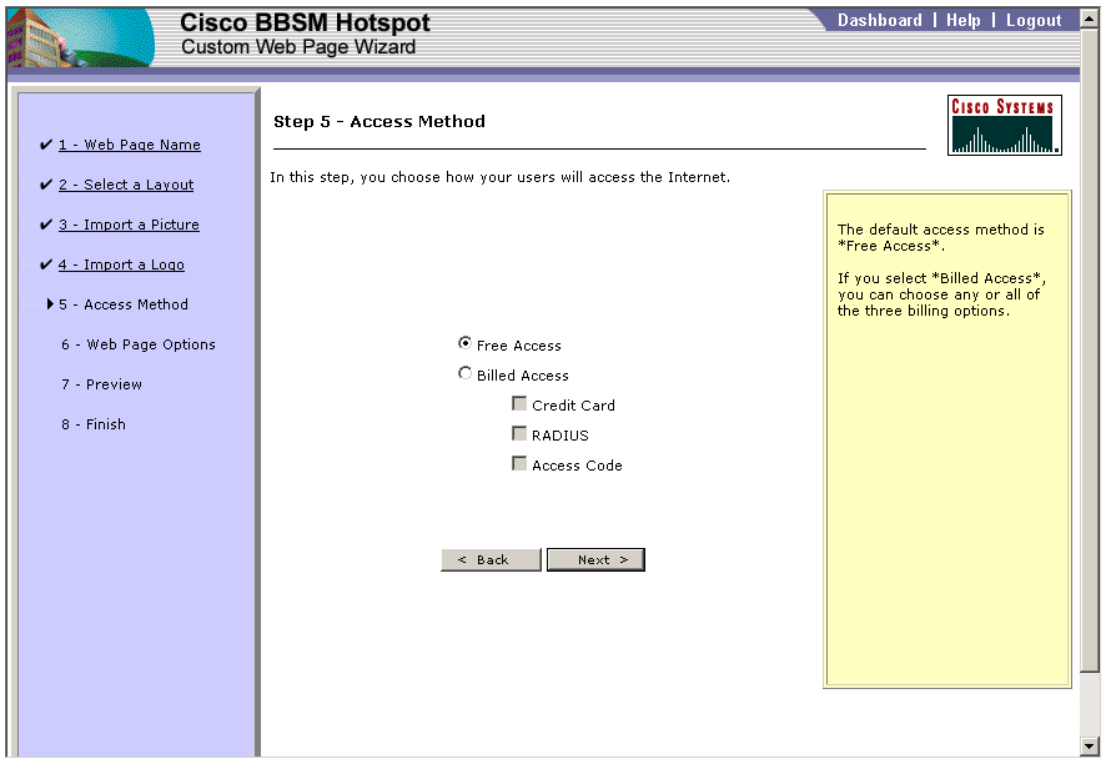
Figure 3-21 Step 4 - Import a Logo Web Page



Step 6 If you want to add a logo to the Start page at this time, click **Browse** to navigate to the file of the logo. The logo should be 175 by 70 pixels or smaller. (If you do not want to add a logo now, leave the file name blank.) Then click **Next**. The Step 5 - Access Method web page appears. (See Figure 3-22.)

Note If you added a logo, click **Back** to view it.

Figure 3-22 Step 5 - Access Method Web Page



Step 7 Click the desired access method: **Free Access** or **Billed Access**. The web pages that appear next depend on which access method you select. Free access is the default.

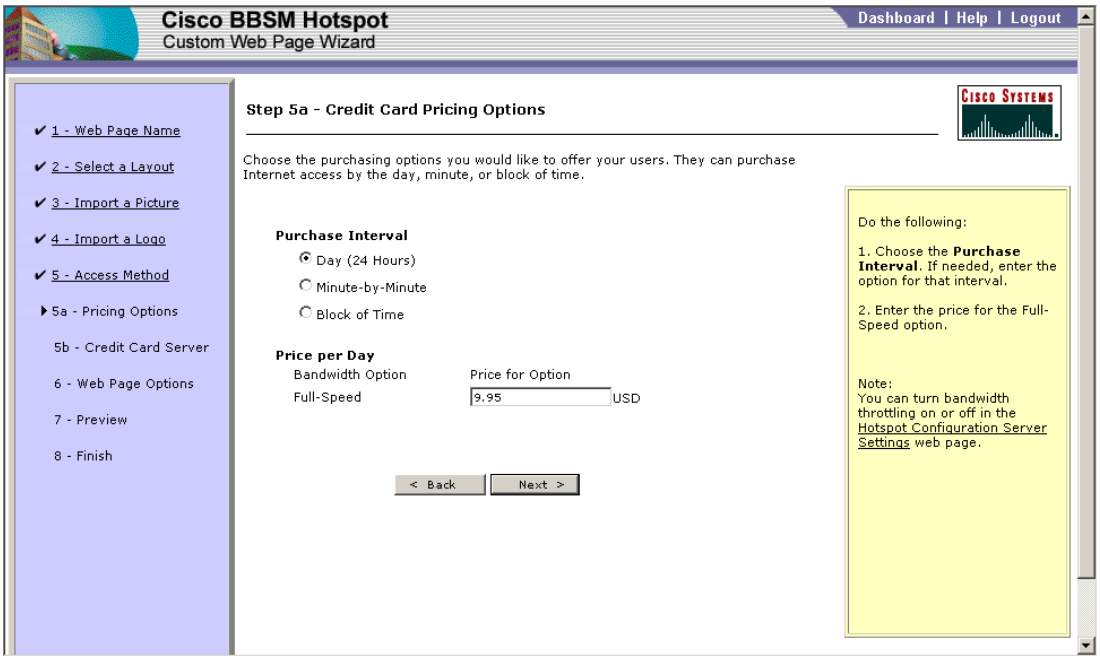
Step 8 If you selected Billed Access, check the type of billing you want to offer: **Credit Card**, **RADIUS**, and/or **Access Code**. Note that you are able to choose any combination of billing types. Then click **Next**.

Step 9 Go to the appropriate step in the procedure, based on the access methods you chose in Step 7:

- If you chose the Credit Card billing option, go to Step 10.
- If you chose the RADIUS billing option, go to Step 12.
- If you chose the Access Code billing option, go to Step 13.

Step 10 If you checked the Credit Card billing option in Step 7, the Step 5a - Credit Card Pricing Options web page appears. (See Figure 3-23.)

Figure 3-23 Step 5a - Credit Card Pricing Options Web Page



Make the following selections. (If this information was previously set up on the server, these fields will show default this data.) Enter the data as follows:

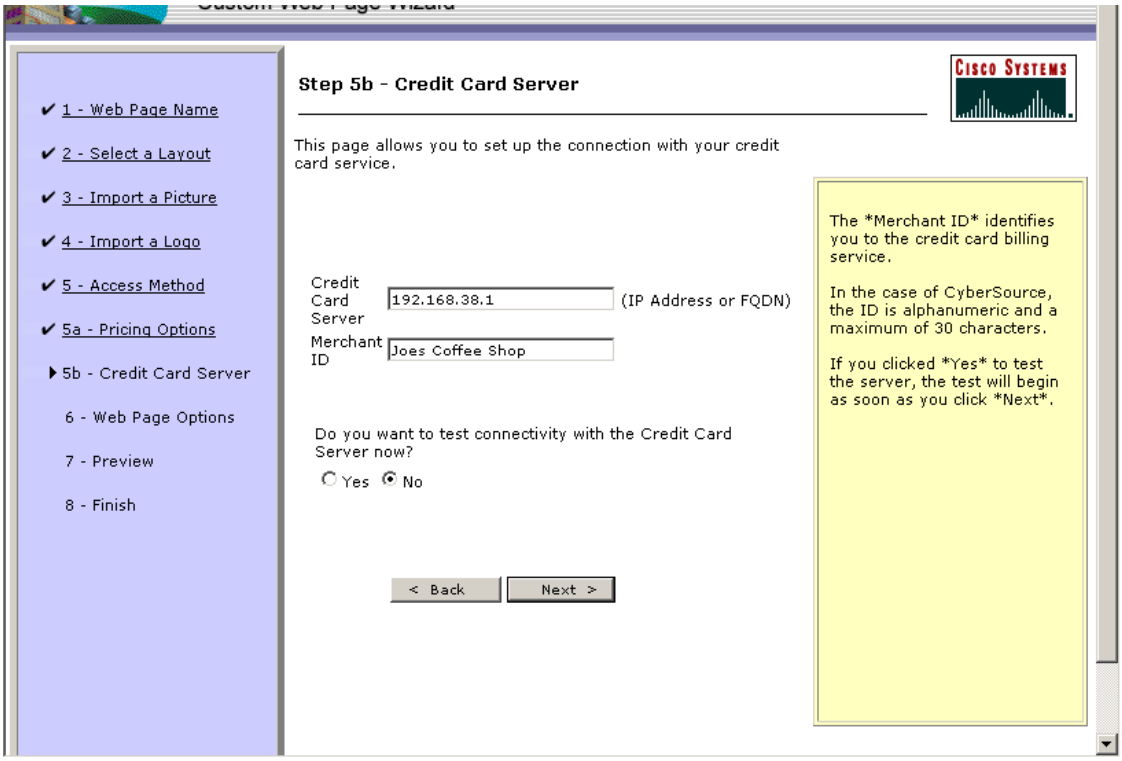
a. Check the Purchase Interval you want to offer: **Day**, **Minute-by-Minute**, or **Block of Time**:

- If you chose Minute-by-Minute, the Total Pre-Approval Amount field appears. Enter the desired amount credit card amount. The end user's credit card must approve for this amount. If their credit card does not approve this amount, the end user will be denied access to the Internet.
- If you chose Block of Time, the Duration of Block Time field appears. Enter the desired number of minutes that the end user can access the Internet.

b. If you enabled bandwidth throttling on the Server Settings web page in Hotspot Configuration, check the bandwidth speeds you want to want to offer credit card user and, if desired, change the default prices. For example, if you want to offer a 512-kbps speed for $5.00 and a 256-kbps speed for $3.00, check only the boxes next to 512 kbps and 256 kbps and enter your price for each.

c. Click **Next** and continue with Step 11. The Step 5b - Credit Card Server appears. (See Figure 3-24.)

Figure 3-24 Step 5b - Credit Card Server Web Page



Step 11 On the Step 5b - Credit Card Server web page, make the following selections:

a. Enter the IP address or FQDN for the credit card server, as provided by your credit card billing service, such as CyberSource.

b. Enter the Merchant ID that is provided by your credit card service.

c. If you want to test the connection to the credit card server, click **Yes**.

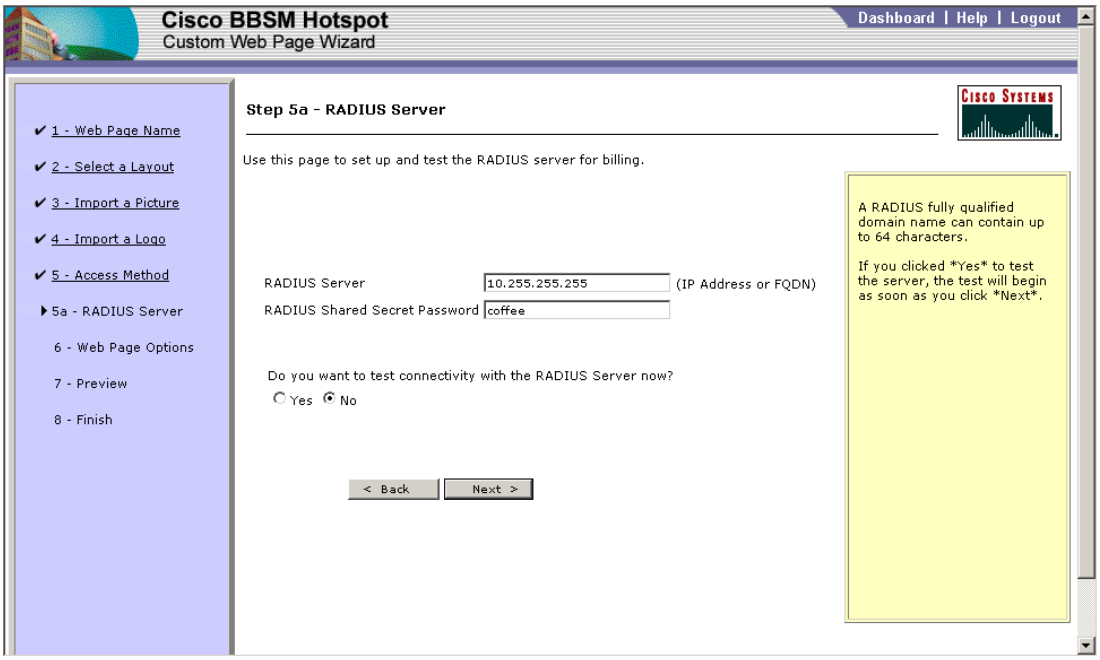
d. To begin the test, click **Next**.

e. If you chose to test the connection to the credit card server, text appears under the buttons to indicate that the test is in progress. When either the success or fail dialog box appears, click **OK** to continue to the next step or **Cancel** to return to this step to change the server information.

Step 12 If you checked the RADIUS billing option in Step 7, the Step 5a - RADIUS Server web page appears. (See Figure 3-25.)

Note If you chose both the Credit Card and RADIUS billing options, the RADIUS Server web page will be labeled step 5c instead of step 5a.

Figure 3-25 Step 5a - RADIUS Server Web Page



Make the following selections. (If this information was previously set up on the server, these fields will show default this data.) Enter the data as follows:

a. In the RADIUS Server field, enter the IP address or FQDN.

b. In the RADIUS Shared Secret field, enter the server password.

c. If you want to test the connection to the server, click **Yes**.

d. To begin the test, click **Next**.

e. If you chose to test the connection to the RADIUS server, text appears under the buttons to indicate that the test is in progress. When either the success or fail dialog box appears, click **OK** to continue to the next step or **Cancel** to return to this step to change the server information.

Note For additional RADIUS configuration parameters, refer to the "Configuring RADIUS Billing" section on page 3-19.

Step 13 Enter the final components needed for your web page. Depending on which access options you chose, the Step 6 - Web Page Options web page that appears after Steps 11 or 12 contains different information. All selected choices offer the standard options; however, if you chose credit card and/or RADIUS, you will also see a security option:

- If you chose free access or access codes, the Step 6 - Web Page Options web page for the free access or access code method appears. (See Figure 3-26.)
- If you chose credit cards or RADIUS access, the Step 6 - Web Page Options web page for the credit card or RADIUS method appears. A security option is included for these access methods. (See Figure 3-27.)

Figure 3-26 Step 6 - Custom Web Page Options Web Page using Free Access or Access Codes Only

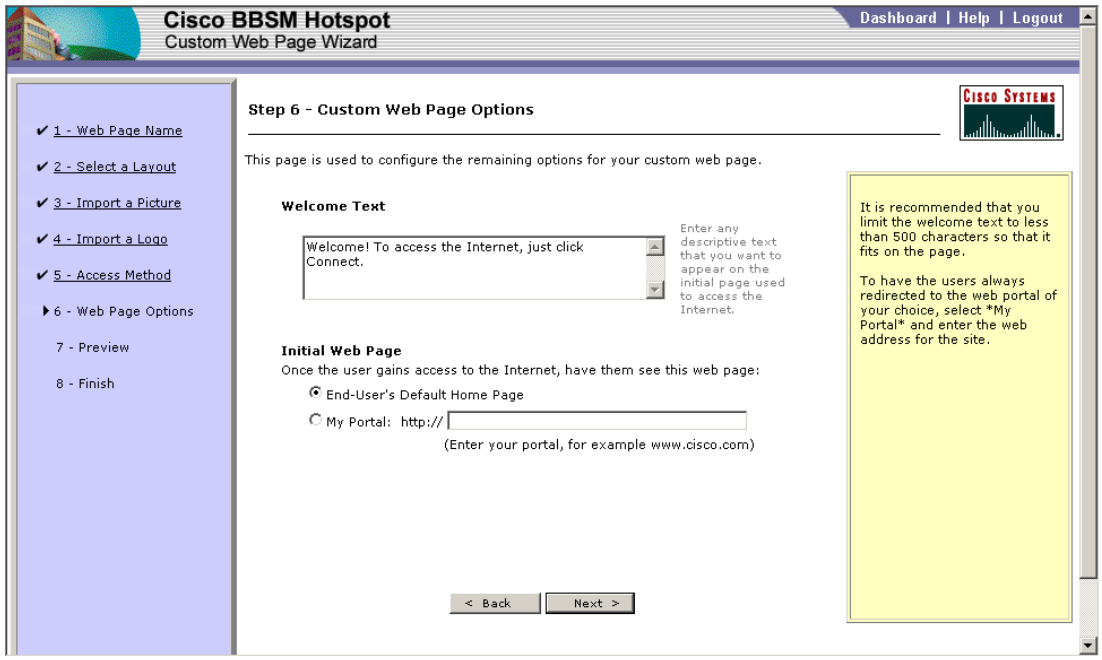
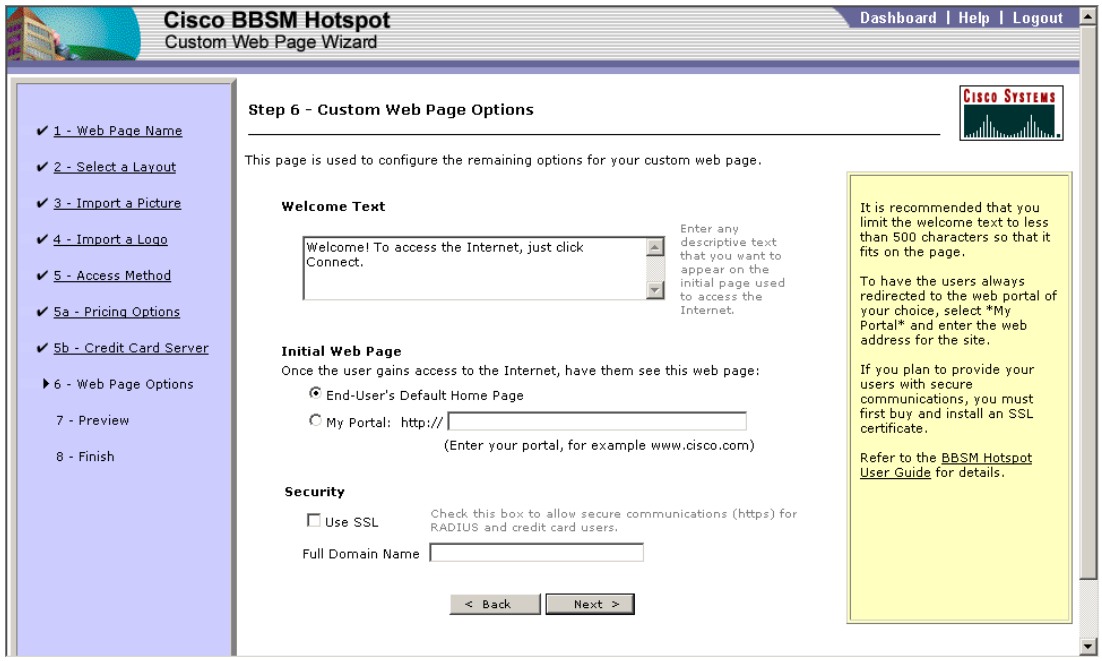


Figure 3-27 Step 6 - Custom Web Page Options Web Page using Credit Cards and/or RADIUS



Enter the final components for your web page:

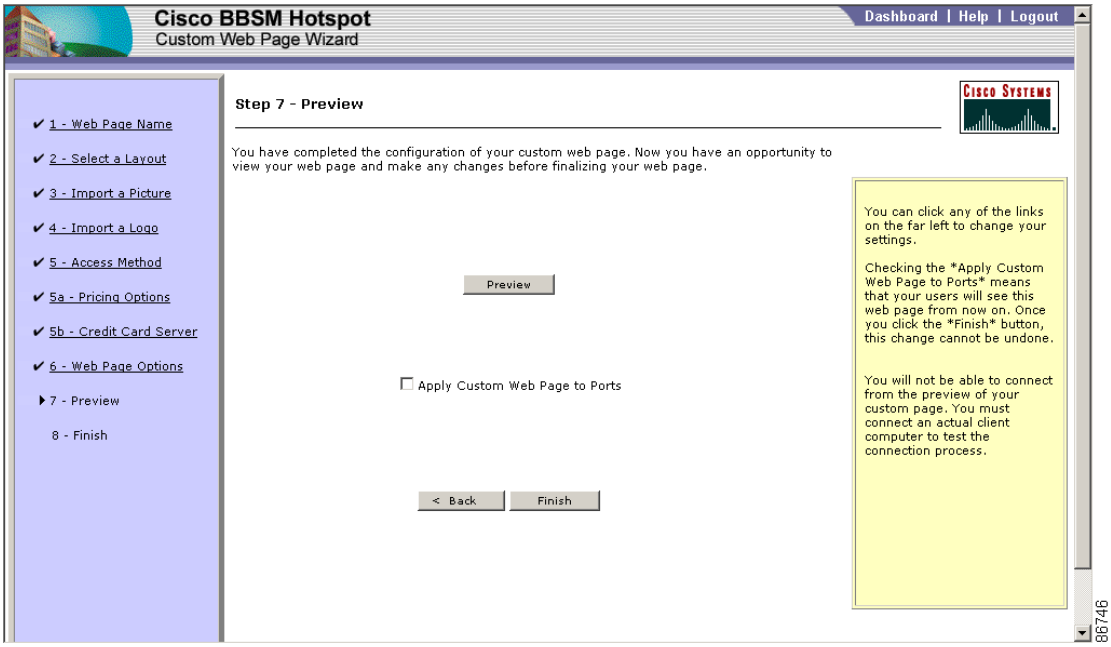
a. In the Welcome Text field, enter the text that you want to display on the Start page that the end user will use to access the Internet.

b. In the Initial Web Page area, choose the desired option for the initial page that the end user sees when they connect to the Internet:
   - If you want the end user to see their previously established default home page, click **End-User's Default Home Page**.
   - If you want the end user to see a home page different from their personal home page, click **My Portal** and enter the URL of the desired web page.

c. If you are using credit cards and/or RADIUS, in the Security area, check **Use SSL** and enter the domain name.

d. Click **Next**. The Step 7 - Preview web page appears. (See Figure 3-28.)

Figure 3-28 Step 7 - Preview Web Page



Step 14 Click **Preview**. A preview of your custom web page appears. Note that this preview page does not allow you to connect. You must connect an actual client computer to test the connection process.

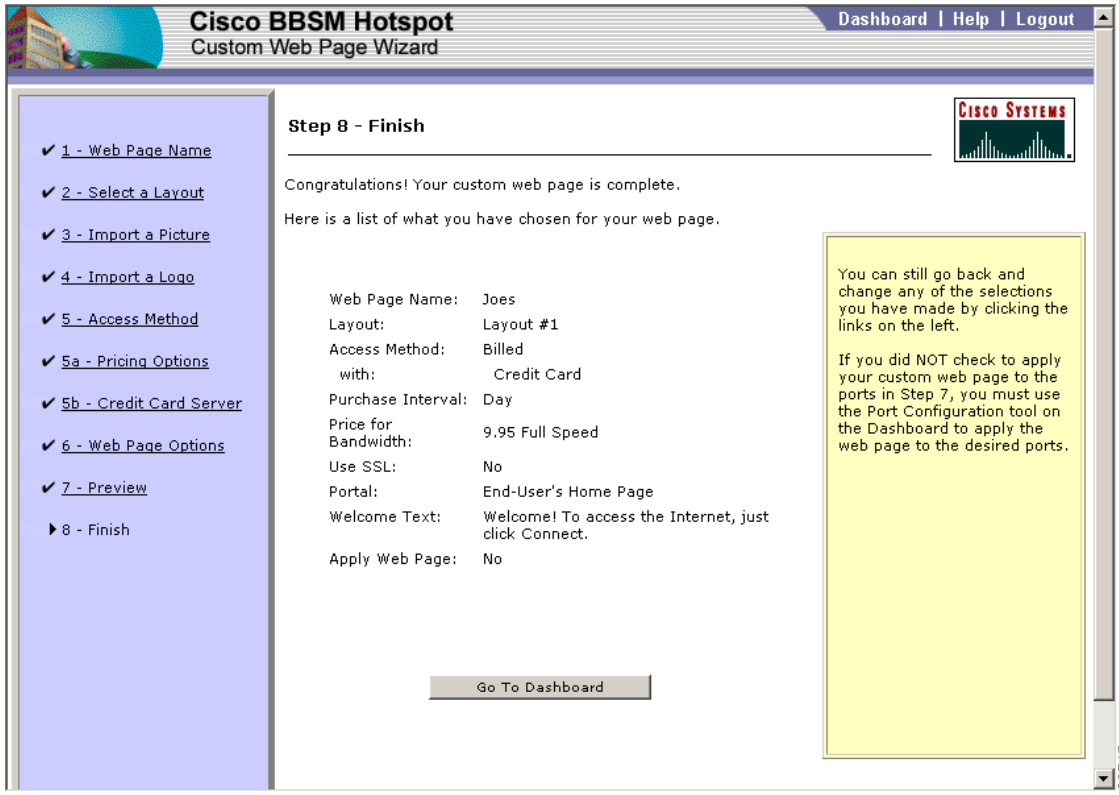
Step 15 On the preview page, verify whether or not your custom web page is correct and then close the page:

- If you want to modify your web page, click the appropriate link in the NavBar on the left, make your changes, and click **7 - Preview** in the NavBar to return to the preview page and verify the changes.
- If you want to apply this web page to all of your ports, click **Apply Custom Web Page to Ports**.

Note This option is only enabled if you have already completed the Setup Wizard.

Step 16 To save your new web page, click **Finish**. The Step 8 - Finish web page appears. (See Figure 3-29.) After clicking Finish, you still have the option to click any of the links in the NavBar to return to any of the previous steps.

Figure 3-29 Step 8 - Finish Web Page



Step 17 You have completed the wizard. If you did not click **Apply Custom Web Page to Ports** in Step 14 and apply the web page to all of your ports, you must use the Port Configuration tool to apply the web page to the desired ports. To access the Port Configuration tool and the Dashboard, click **Go To Dashboard**.

System Operation

This chapter describes how to perform all facets of system operation after the initial basic configuration:

- Viewing and Printing Reports, page 4-1
- Viewing port control data and performing port maintenance
- Creating and configuring access codes
- Deactivating and reactivating client sessions
- Viewing and Installing Service Packs or Patches (Updates), page 4-25
- Troubleshooting

Viewing and Printing Reports

You can view and print reports of BBSM Hotspot activities and functions on a site basis by clicking the Reports option on the Dashboard. Use Internet Explorer to view any of the following reports:

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

Accessing Reports

Use the following procedure to access BBSM Hotspot reports.

Step 1 From the Dashboard, click **Reports**. The Usage Report Options web page appears.

Step 2 To request a report, click the desired report on the menu bar at the top of the web page. (See Figure 4-1.)

Step 3 For all report web pages, select the way that you want the report to be sorted by clicking a column heading. Clicking the heading a second time switches the order of rank between ascending and descending.

Usage Reports

Usage reports allow you to obtain data about Internet use for the specified time range. You can request this data in three different formats:

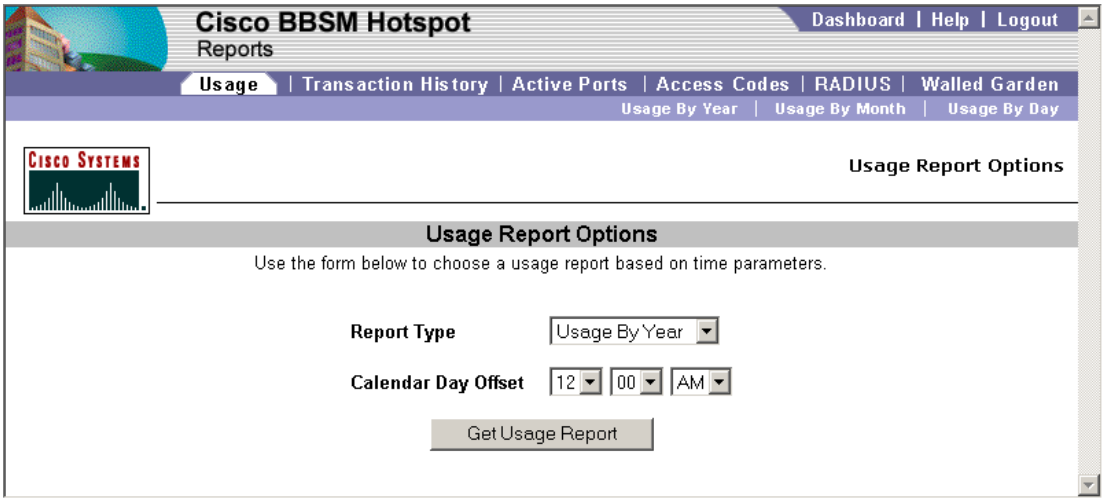
- Usage By Year
- Usage By Month
- Usage By Day

To generate usage reports based on a specified time range instead of the default of midnight, use the Calendar Day Offset feature. By using Calendar Day Offset, you can choose to realign the time boundaries with, for example, a shift change.

Use the following procedure to generate and view usage reports.

Step 1 From the Dashboard, click **Reports**. The Usage Report Options web page appears. (See Figure 4-1.)

Figure 4-1 Usage Report Options Web Page



Step 2 To generate and view the report, from the Report Type drop-down menu, choose the type of report that you want to generate. (You can also select the report type on the secondary navigation bar.)

- Usage by Year
- Usage by Month
- Usage by Day

Step 3 If desired, from the **Calendar Day Offset** drop-down menu, choose the start time of the report, such as 10:00 AM.

Step 4 To generate and view the report, click **Get Usage Report**. The report appears. (Figure 4-2 shows a Usage By Day report. Table 4-1 describes the report columns.)

You can use the data links in the left column of a report to move to the next more detailed report; for example, as follows:

- When you choose the Usage By Year report, you can click the underlined year in the left column to see a Usage By Month report for that year.

- From the Usage By Month report, you can click a particular month to view a Usage By Day report for that month.
- From the Usage By Day report, you can click a specific day to view a Usage by Day report for just that day. You can also click a location in the in the second column to view a Usage By Day report for just that location on that day.

Figure 4-2 Usage By Day Report

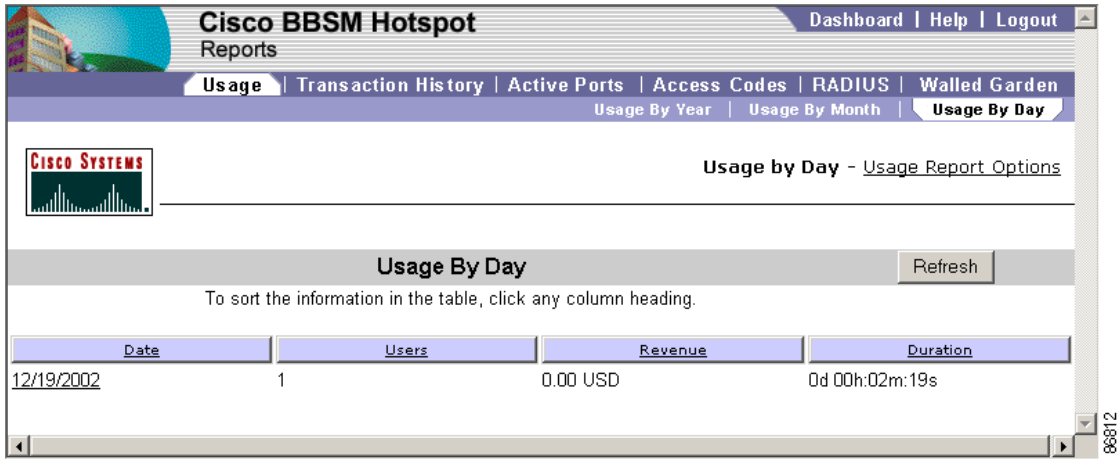


Table 4-1 Usage Report Column Descriptions

Column	Description
Year Month Date	Depending on the type of report requested, displays the generated data for the year, month, or day. For example, if you click year 2002, the Usage By Month report appears, showing you the monthly usage for 2002.
Users/Location	For the specified time period, shows the number of Internet users. In the Usage by Day report, when you click the left-hand Date column, the Users column changes to Location.
Revenue	Displays the revenue that was generated for that time period.
Duration	Displays the length of time that the Internet was used for the year, month, or day.

Transaction History Reports

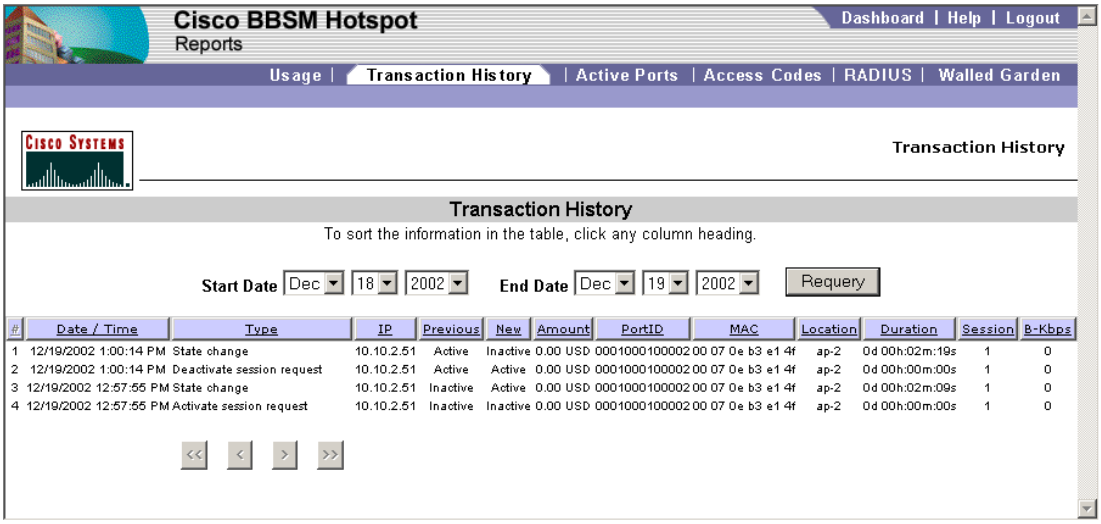
The Transaction History report contains one record for each BBSM Hotspot event. Example events are client activation and deactivation, credit card sales, and port hopping.

Use the following procedure to generate and view reports.

Step 1 From the Dashboard, click **Reports**. The Usage Report Options web page appears.

Step 2 Click **Transaction History**. The Transaction History web page appears. (See Figure 4-3.)

Figure 4-3 Transaction History Report



Step 3 Select the time period for the report:

a. From the Start Date drop-down menu, select the report start date.

b. From the End Date drop-down menu, select the report end date.

Step 4 To generate a new report, click **Requery**. Table 4-2 describes the Transaction History report columns.

Table 4-2 BBSM Hotspot Transaction History Report Columns

Column	Description
#	Displays the transaction number.
Date / Time	The date and time of the transaction.
Type	The type of transaction that occurred.
IP	The IP address of the applicable client.
Previous	Designates the state of the port, Active or Inactive, before the transaction.
New	Designates the state of the port, Active or Inactive, after the transaction.
Amount	The cost of the transaction, if any.
PortID	The Port ID of the applicable client.
MAC	The MAC address of the applicable client.
Location	The guest room or location number of the client.
Duration	The session duration.
Session	For each IP address, the unique number that identifies the session.
Multinet	The multinet, 1 or 2, that was used for the transaction.
B-kbps	This field displays the bandwidth throttling rate, in kbps, that applied to the session.

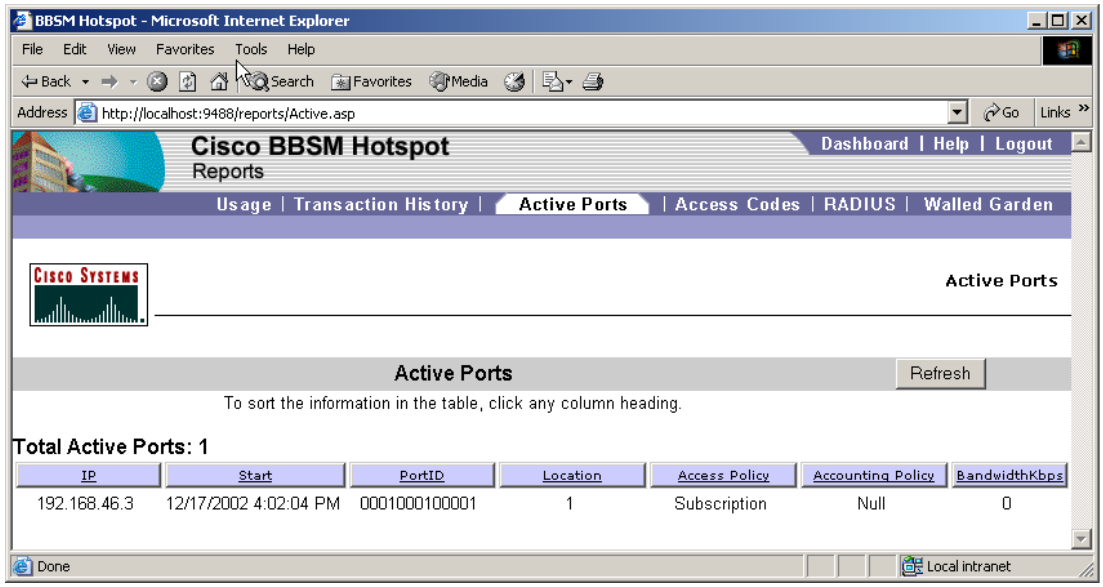
Active Ports Report

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

Step 1 From the Dashboard, click **Reports**. The Usage Report Options web page appears.

Step 2 Click **Active Ports**. The Active Ports report appears. (See Figure 4-4.)

Figure 4-4 Active Ports Report



Step 3 To sort the data in ascending or descending order, click a column heading. Table 4-3 describes the report columns.

Table 4-3 Active Ports Report Column Descriptions

Column	Description
IP	The IP address of the connected client.
Start	The time that the connection started.
PortID	The client port. The number includes the switch, cluster, and port identifiers.
Location	The location name or number: • If you used the Switch Discovery Wizard to configure the ports, the room or location designation is “unmapped.” • If you configured the ports using Hotspot Configuration and the Network Device Port Settings pop-up window, the location shows the prefix you selected in Port Settings with the port number after it, such as “SW1-128.”
Access Policy	The access policy used for the client.

Table 4-3 Active Ports Report Column Descriptions

Column	Description
Accounting Policy	The accounting policy used for the client.
Bandwidth kbps	The bandwidth throttling rate, with “0” indicating full speed.

Access Code Reports

Three different Access Code reports show the existing, unused, and expired access codes:

- Existing codes—Access Code Report
- Unused codes—Unused Code Report
- History of code use—Access Code History Report

The sections that follow describe how to generate and view the reports.

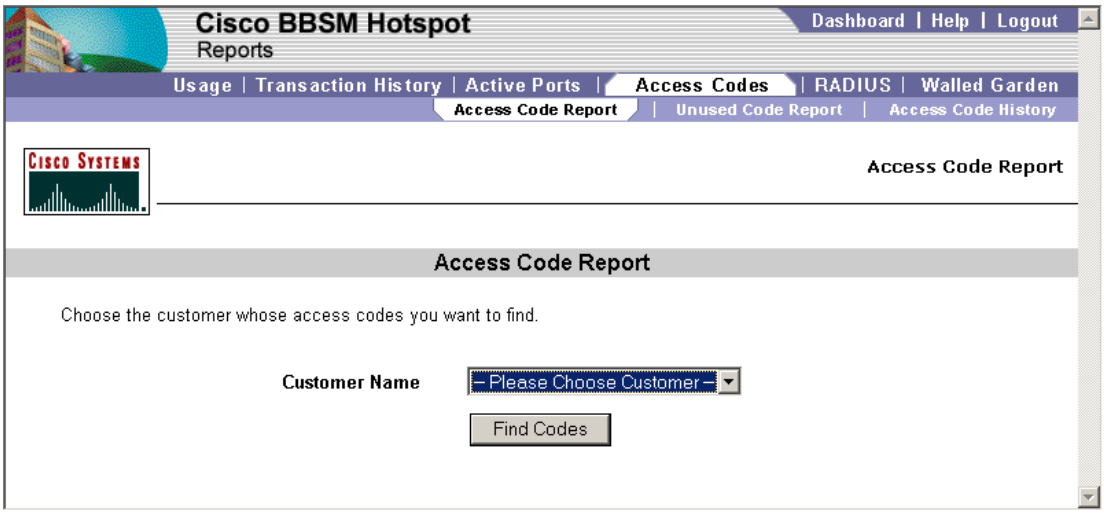
Access Code Report

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

Step 1 From the Dashboard, click **Reports**. The Usage Report Options web page appears.

Step 2 Click **Access Codes**. The Access Code Report options web page appears. (See Figure 4-5.)

Figure 4-5 Access Code Report Options Web Page



Step 3 From the Customer Name drop-down menu, choose the customer for which you want to view the access codes.

Step 4 To generate and view the report, click **Find Codes**. The Access Code Report appears. (See Figure 4-6. Table 4-1 describes the report columns.)

Figure 4-6 Access Code Report

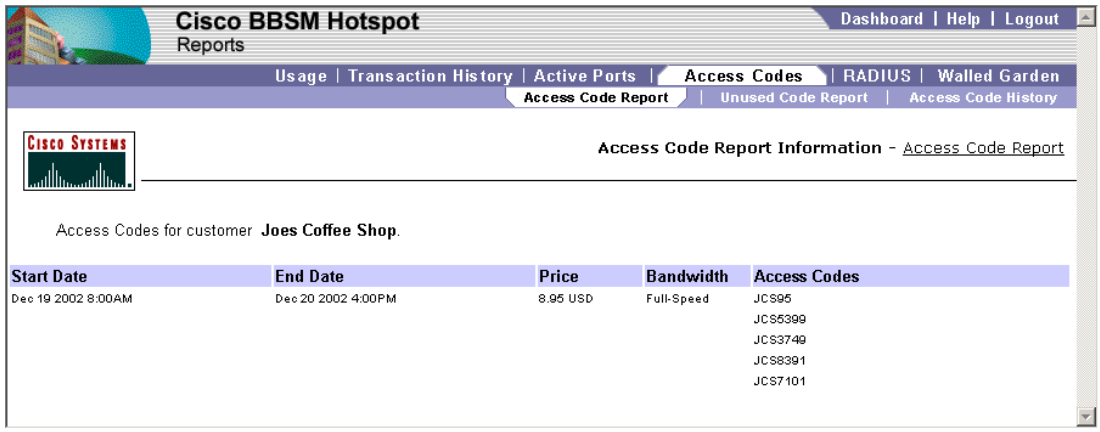


Table 4-4 Access Report Column Descriptions

Column	Description
Start Date	The start date that the access code will be used.
End Date	The end date that the access code will be used.
Price	The price for the access code.
Bandwidth	The minimum bandwidth (in kbps) of the access code.
Access Codes	The access codes that will be used.

Unused Code Report

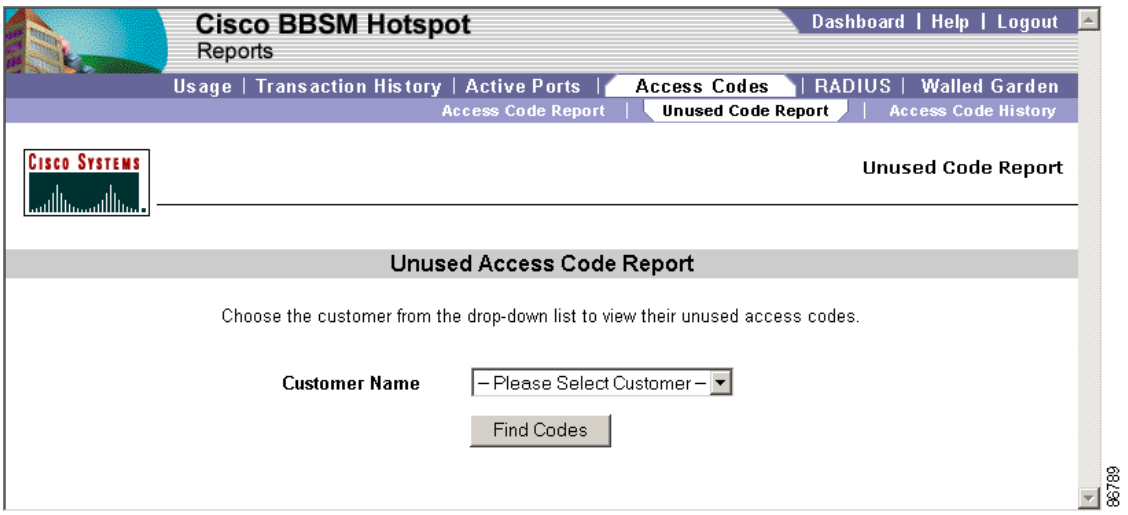
The Unused Code Report shows the unused access codes assigned to a customer. Use the following procedure to view the Unused Code report.

Step 1 From the Dashboard, click **Reports**. The Usage Report Options web page appears.

Step 2 Click **Access Codes**. The Access Code Report web page appears. (See Figure 4-5.)

Step 3 Click **Unused Code Report**. The Unused Code Report options web page appears. (See Figure 4-7.)

Figure 4-7 Unused Code Report Options Web Page



Step 4 From the Customer Name drop-down menu, choose the customer for which you want to view the access codes.

Step 5 To generate and view the report, click **Find Codes**. The Unused Code Report appears. (See Figure 4-8.) Table 4-5 describes the report columns.)

Figure 4-8 Unused Code Report

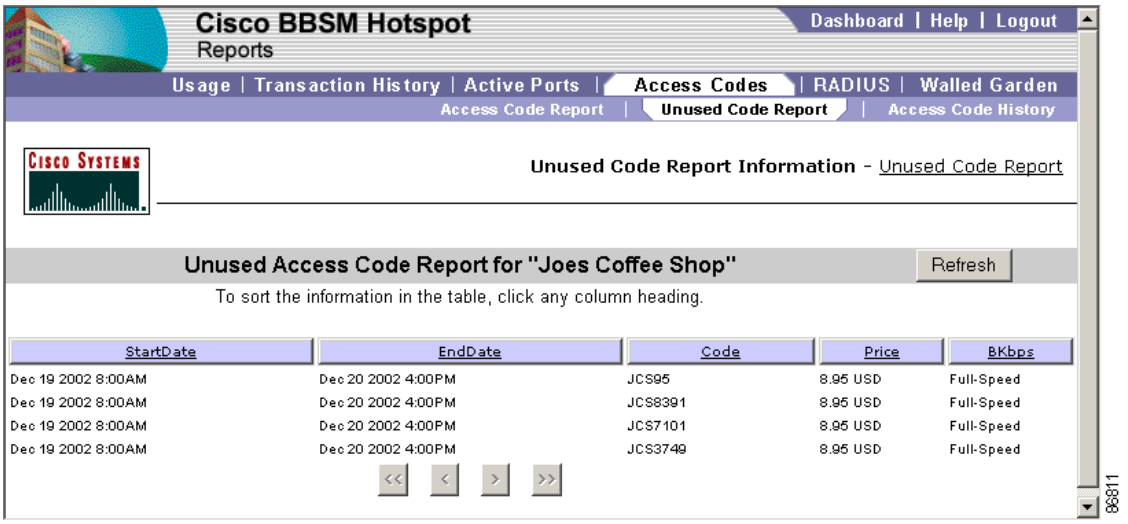


Table 4-5 Unused Code Report Column Descriptions

Column	Description
StartDate	The start date that the access code was to have been used.
EndDate	The end date that the access code was to have been used.
Code	The access code to have been used.
Price	The price for the access code.
Bkbps	The minimum bandwidth (in kbps) of the access code. If no bandwidth was specified, the rate is "None."

Access Code History Report

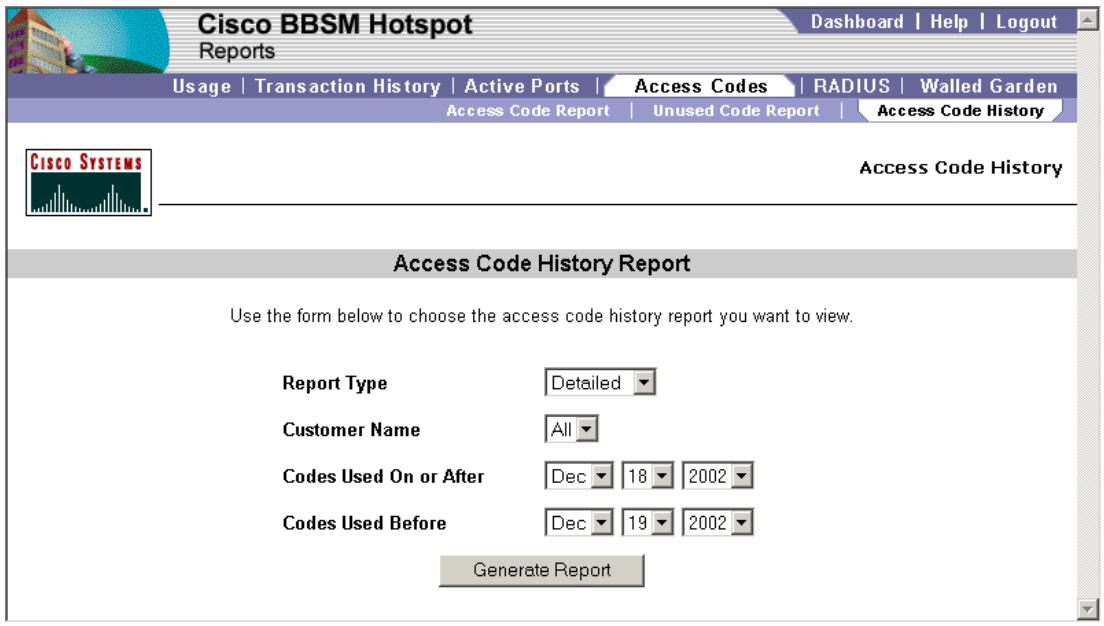
The Access Code History report shows the access codes that have been used. Use the following procedure to generate and view a summary or detailed report.

Step 1 From the Dashboard, click **Reports**. The Usage Report Options web page appears.

Step 2 Click **Access Codes**. The Access Code Report web page appears. (See Figure 4-5.)

Step 3 Click **Access Code History**. The Access Code History options web page appears. (See Figure 4-9.)

Figure 4-9 Access Code History Report Options 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 end date.

Step 8 To view the report, click **Generate Report**. The Access Code History report appears. (Figure 4-10 shows a summary report, and Figure 4-11 shows a detailed report. Table 4-6 describes the Access Code History report columns.)

Figure 4-10 Summary Access Code History Report

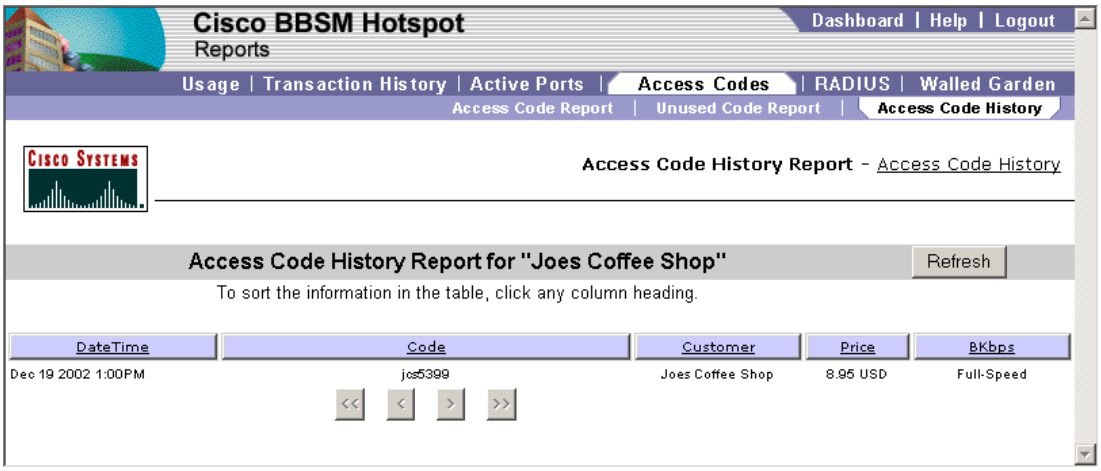


Figure 4-11 Detailed Access Code History Report

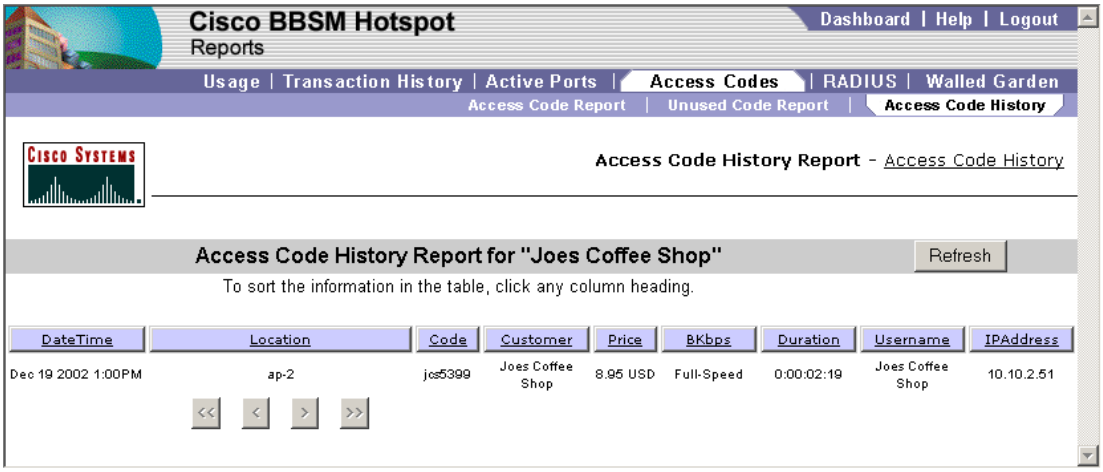


Table 4-6 Access Code History Report Column Descriptions

Column	Description
DateTime	The date and time that the end user logged off.
Location	The location name or number: • If you used the Switch Discovery Wizard to configure the ports, the room or location number is "unmapped." • If you configured the ports using Hotspot Configuration and the Network Device Port Settings pop-up window, the room number shows the location prefix you selected in Port Settings with the port number after it, such as "SW1-128."
Code	The access code used to log in.
Customer	The customer name used when the access code was created.
Price	The price and currency type for the access code or bandwidth rate.
BKbps	The bandwidth used for the access code, or if no bandwidth was specified, the actual bandwidth rate, such as "Full-Speed."
Duration	The length of time that the end user was logged on.
Username	The end user's name.
IPAddress	The end user's IP address.

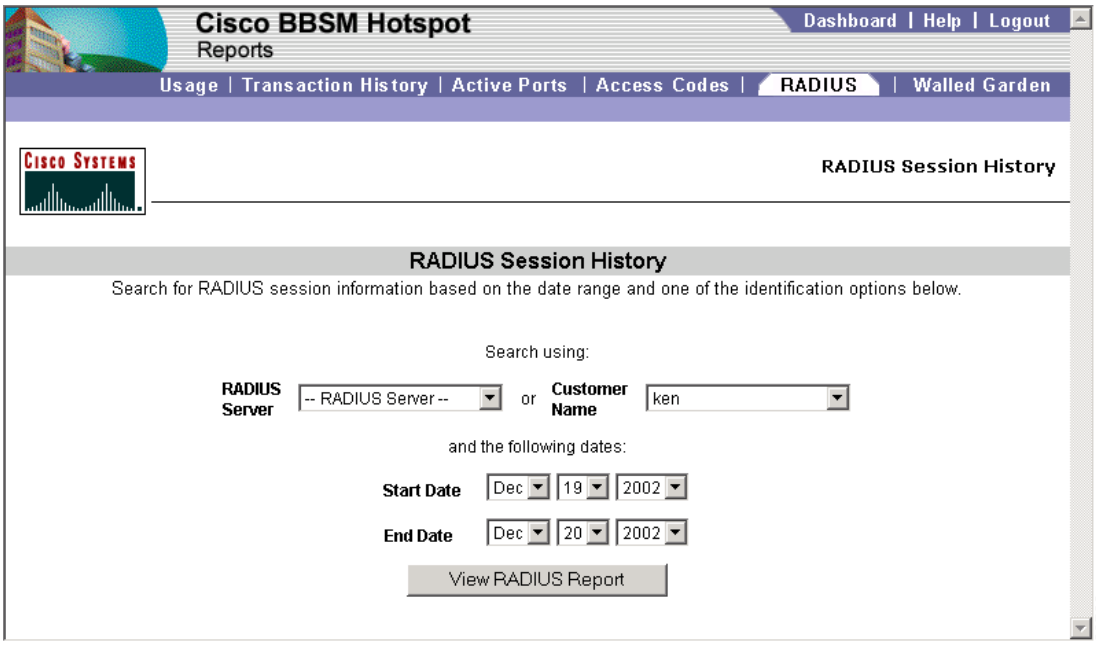
RADIUS Reports

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 Dashboard, click **Reports**. The Usage Report Options web page appears.

Step 2 Click **RADIUS**. The RADIUS Session History web page appears. (See Figure 4-12.)

Figure 4-12 RADIUS Session History Options Web Page



Step 3 From the RADIUS Server or Customer Name drop-down menus, select the desired RADIUS server or customer. (If RADIUS Accounting is not enabled, the RADIUS Server drop-down menu will not have any entries for selection. Then, only a customer name can be selected.)

Step 4 Select the time period for the report:

a. From the Start Date drop-down menu, select the report start date.

b. From the End Date drop-down menu, select the report end date.

Step 5 To generate and view the report, click **View RADIUS Report**. The RADIUS Session report appears. (See Figure 4-13.)

Note In this section, "Customer" refers to the end user that connects to the Internet, not you, the BBSM Hotspot customer.

Figure 4-13 RADIUS Session History Report

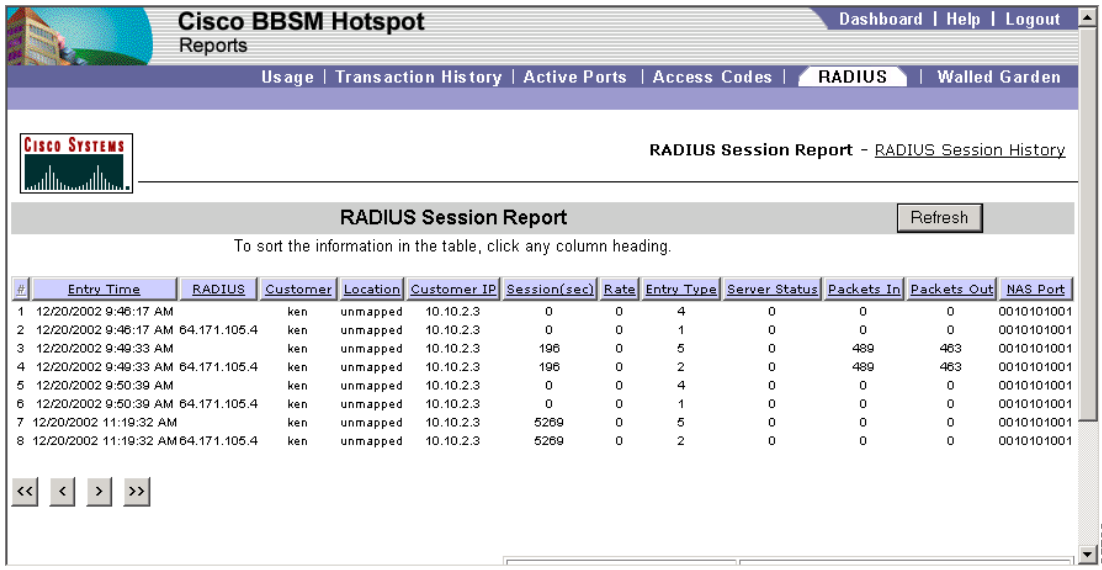


Table 4-7 describes the RADIUS Session report data.

Table 4-7 RADIUS Session History Report Columns

Column	Description
#	The session number.
Entry Time	The time that the end user logged in.
RADIUS	The IP address of the RADIUS server that the end user connected to.
Customer	The end user's login name.
Room	The end user's location.
Customer IP	The end user's IP address.
Session (sec)	The session duration in seconds.
Rate	The cost of the session.
Entry Type	Indicates the type of entry: • 1 = RADIUS Accounting Start • 2 = RADIUS Accounting Stop • 3 = RADIUS Accounting Interim-Update • 4 = Activate Session • 5 = Deactivate Session • 6 = Bandwidth Boost
Server Status	Indicates whether or not the login was successful: • 0 = Successful • 1 = RADIUS server not responding • 2 = Authentication/accounting response packet not valid • 3 = Other
Packets In	The number of packets that BBSM Hotspot received from the end user during the user's session.
Packets Out	The number of packets that BBSM Hotspot transmitted to the end user during the user's session.
NAS Port	The location of the NAS port.

Walled Garden Report

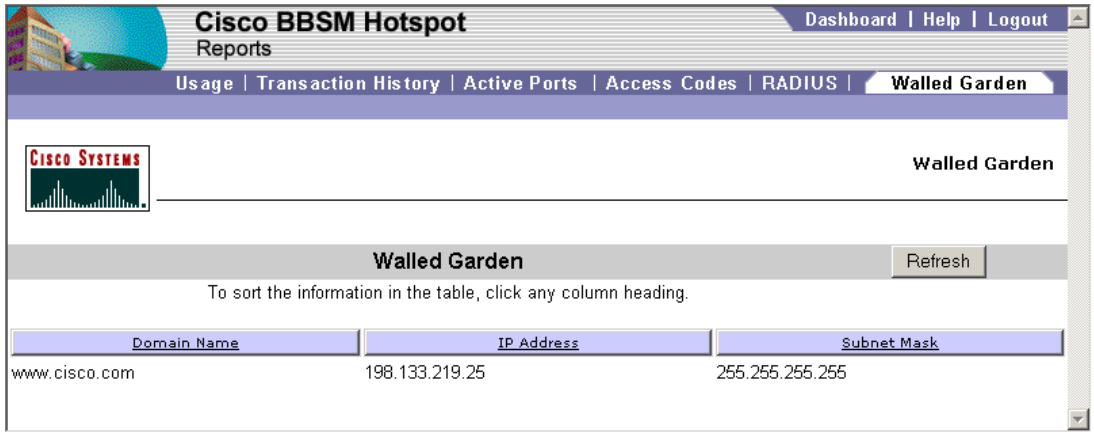
The Walled Garden report displays all of the current walled garden configurations that you created using the Walled Garden web page of Hotspot Configuration. Figure 4-14 shows an example of the report.

Use the following procedure to view the Walled Garden report.

Step 1 From the Dashboard, click **Reports**. The Usage Report Options web page appears.

Step 2 Click **Walled Garden**. The Walled Garden report web page appears. (See Figure 4-14.)

Figure 4-14 Walled Garden Report



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

Managing Access Codes

You can create, edit, delete, and view access codes by using the Access Code Management tool on the Dashboard. Access codes are alphanumeric strings that BBSM Hotspot generates for end users to access the Internet. The Internet access is paid for by purchasing the access code, which can be paid for when generating the access code or at the time the access code is used. No billing is done by BBSM Hotspot when users log in with access codes.

Before you can create the access codes using managed bandwidth, you must have configured the bandwidth management options. Refer to the "Configuring Server Settings" section on page 3-2.)

Managing Access Codes

After you have determined the bandwidth options in Hotspot Configuration, you can create and configure your access codes. Use the following procedure to manage your access codes.

Step 1 From the Dashboard, click **Access Code Management**. The Manage Codes web page appears. The web page differs, depending on the access codes bandwidth options that you configured on the Server Settings web page in Hotspot Configuration (refer to the "Configuring Server Settings" section on page 3-2):

- No Throttling—If you did not check Bandwidth Throttle on the Server Settings page, the bandwidth defaults to Full Speed.
- Throttle—If you checked Bandwidth Throttle on the Server Settings page, the Bandwidth drop-down menu appears on the Manage Codes web page.

Step 2 Configure the access code options, based on the information shown in Table 4-8.

Step 3 To save the changes, click **Save**.

Figure 4-15 Manage Codes Web Page

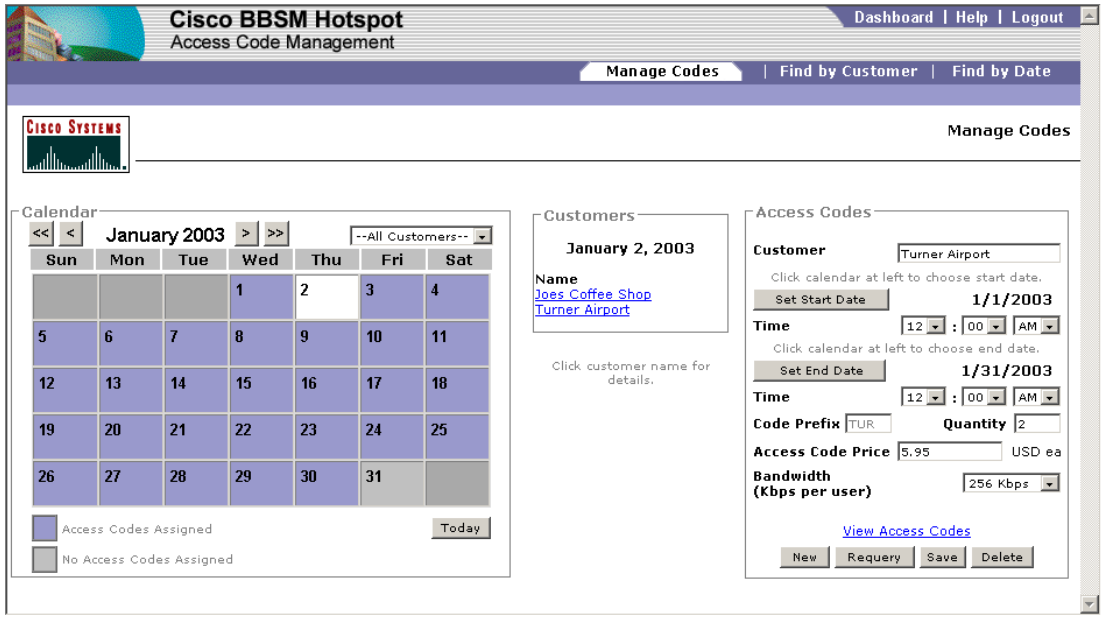


Table 4-8 Access Code Management Options

Field	Description
Calendar	
Monthly calendar	The calendar section shows you the following information: • By scrolling, you can see previous and future months or years and create access codes for that date by clicking the desired date. • From the drop-down menu on the right, you can see the access codes for all customers, which is the default, or choose a specific customer's access codes. • As shown in the lower left-hand corner, the calendar is color coded to highlight dates for which access codes have been created. • Click **Today** to highlight the current day and see its access codes.
Customers	
Date	Displays the selected calendar/access code date.
Name	Shows the customers for which access codes have been created on that date. Click the name to recall the access code details. (The fields at right are then populated with the details.)
Access Codes	
Customer	Enter a customer name.
Set Start Date Time	On the calendar at the left, click the desired start date. Click **Set Start Date** and select the desired start time. The default is 12:00am (midnight).
Set End Date Time	On the calendar at the left, click the desired end date. Click **Set End Date** and select the desired end time. The default is 12:00am (midnight).
Code Prefix	Enter an optional one- to three-letter customer code. After you save the changes, BBSM Hotspot appends a one- to four-digit number to the prefix. The combination is the access code.
Quantity	Enter the number of access codes that you need. The maximum is 1000 access codes.
Access Code Price	Enter the price that you want to charge for each access code. Although the price is recorded for auditing purposes, BBSM Hotspot does not perform any billing when users log in with access codes.
Bandwidth	From the drop-down menu, select the desired maximum bandwidth throttling rate in kbps that is applied to each user that logs in with an access code.
Buttons	
View Access Codes	Click to view the access codes that you configured.
New	Click to enter a new customer and its access codes. The Manage Codes web page appears with blank fields appears so the access codes can be created.
Requery	Before you have saved any changes, click to return the web page to the previously saved settings.
Save	Saves the changes made to the web page.
Delete	When you select a customer, click to delete the customer and its access codes.

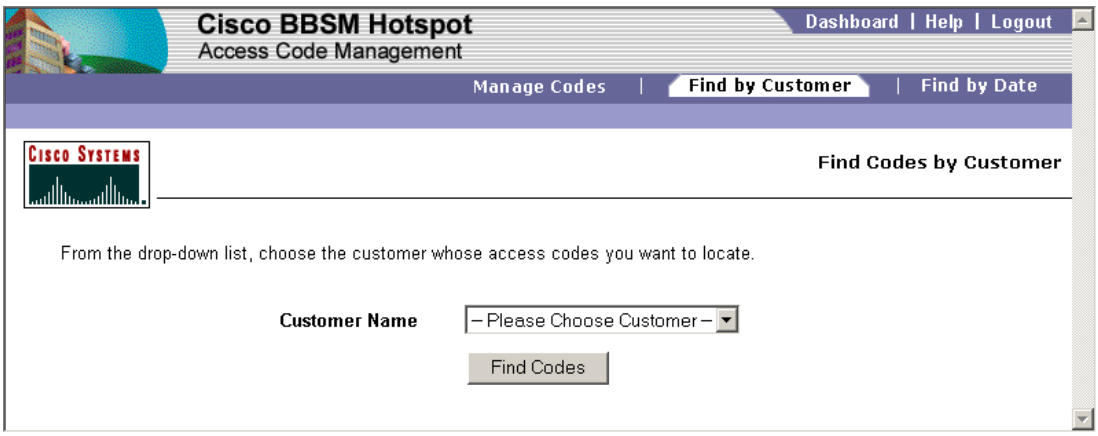
Finding Access Codes by Customer

Use the following procedure to find customers and their access codes by the customer name.

Step 1 From the Dashboard, click **Access Code Management**. The Manage Codes web page appears.

Step 2 From the menu bar, click **Find by Customer**. The Find Codes by Customer web page appears. (See Figure 4-16.)

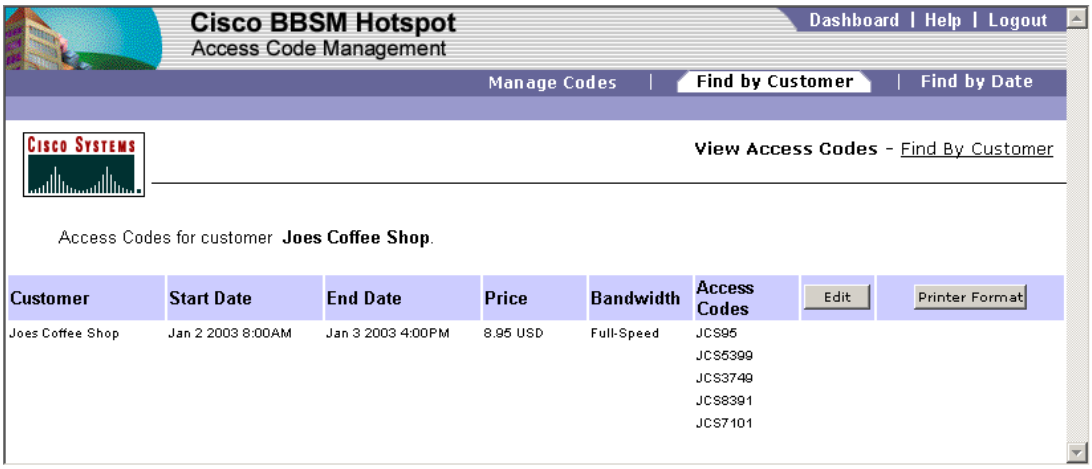
Figure 4-16 Find by Customer Web Page



Step 3 From the drop-down menu of customers with access codes, choose the desired customer.

Step 4 Click **Find Codes**. The View Access Codes - Find By Customer web page appears, showing the access codes for the customer. (See Figure 4-17.)

Figure 4-17 Find by Customer Search Results Web Page

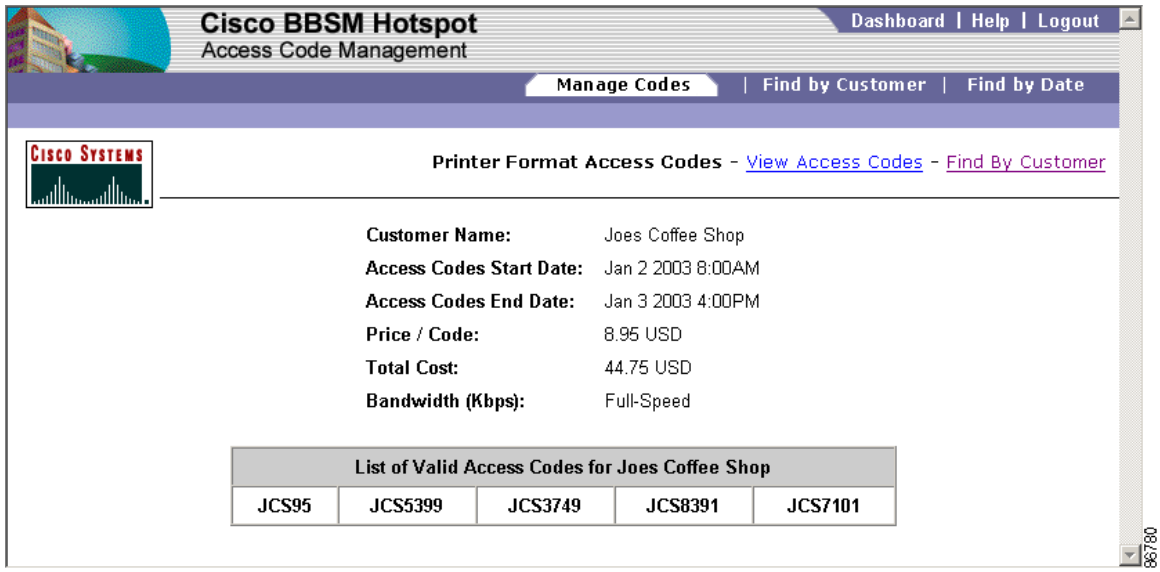


Step 5 To make sure that all of the information about the customer's access codes is correct, verify the settings.

Step 6 To change the settings, click **Edit**. The Manage Codes web page appears. Make changes as needed.

Step 7 To print the access codes in a larger format, click **Printer Format**. The Printer Format Access Codes web page appears. (See Figure 4-18.)

Figure 4-18 Find by Customer Search Results Web Page—Printer Format



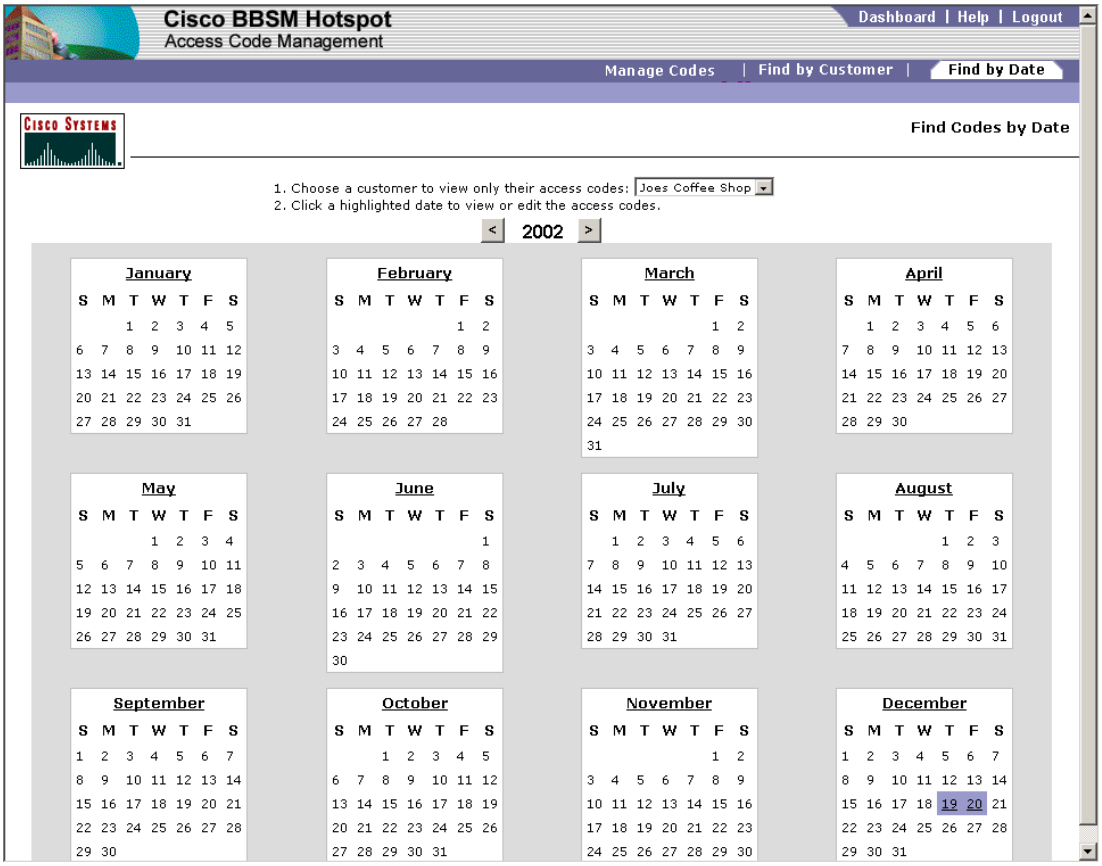
Finding Reservations by Date

Use the following procedure to find customers and their access codes by the date setting.

Step 1 From the Dashboard, click **Access Code Management**. The Manage Codes web page appears.

Step 2 From the menu bar, click **Find by Date**. The Find Codes by Date web page appears, showing highlighted dates for the existing reservations. (See Figure 4-19.)

Figure 4-19 Find by Date Web Page



Step 3 If desired, click the date to view the details about the reservation. The Manage Codes web page appears, showing the existing reservations for the date.

Deactivating and Reactivating Client Sessions

The Client Deactivation feature allows you to remotely deactivate one or more active sessions, either temporarily or permanently. It also allows you to reactivate a permanently deactivated client. By deactivating clients, you can safely perform routine BBSM Hotspot testing and maintenance.

Caution We strongly recommend deactivating all client sessions when installing service packs, patches, and upgrades.

You temporarily or permanently deactivate a client based on its MAC address:

- A temporary deactivation allows clients access to the Start page to reconnect.
- A permanent deactivation prevents clients from reconnecting unless you reactivate them.

When navigating through the sessions, note that each column can be sorted, in ascending or descending order, by clicking the column heading.

Deactivating Client Sessions

Use the following procedure to temporarily or permanently deactivate client sessions.

Step 1 From the Dashboard, click **Client Deactivation**. The Deactivate Clients web page appears. (See Figure 4-20.)

Figure 4-20 Deactivate Clients Web Page

Step 2 Select the client sessions you want to temporarily or permanently deactivate, based on the information shown in Table 4-9.

Step 3 To deactivate the selected clients, click **Deactivate Clients**. After you permanently deactivate a client, they are redirected to the Deactivated Session web page when they try to access the Internet. (See Figure 4-21.)

Figure 4-21 Deactivated Session Web Page

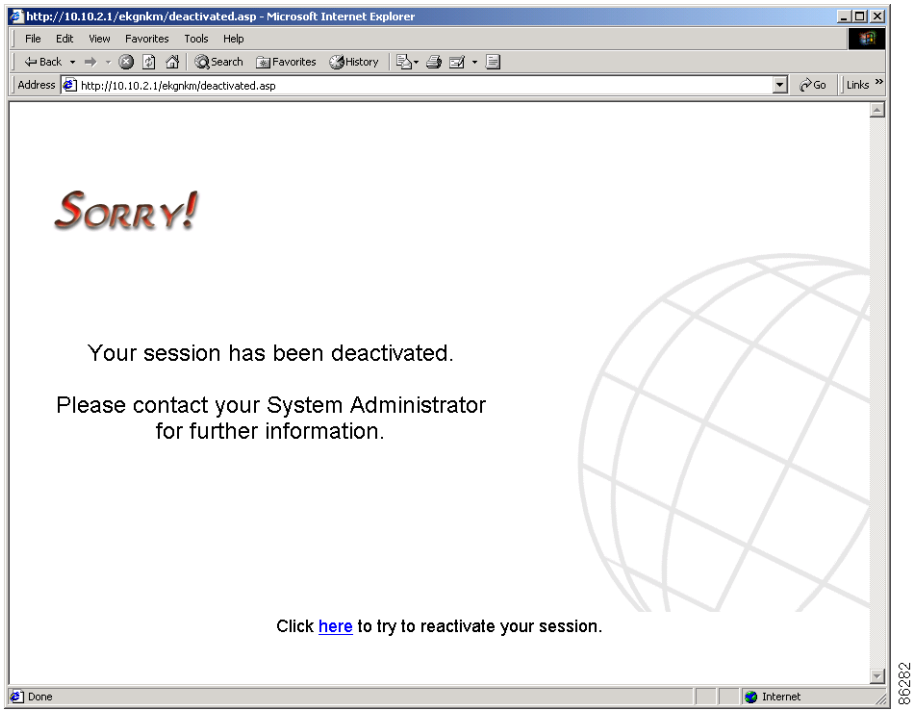


Table 4-9 Deactivate Clients Web Page Options

Option	Description
Deactivate	Check the box to select the session for deactivation.
Permanent	After you have checked Deactivate, check this box to select the session for permanent deactivation.
Client MAC Address	Displays the client's MAC address.
IP Address	Displays the client's IP address.
Start Time	Displays the date and time that the client's session began.
Port ID	Displays the port ID number that the client is connected to. For an explanation of the Port ID, refer to the "Configuring Ports (Port Configuration)" section on page 3-27.
Location	Displays the end user's location number.
Access Policy	Displays the access policy that is applied to this user.
Accounting Policy	Displays the accounting policy that is applied to this user.
Bandwidth	Displays the end user's bandwidth rate.
Buttons	
Requery	Before you have clicked Deactivate Clients, click to return the web page to the previously saved settings.
Select All	Click to select all client sessions at once.
Clear All	Click to deselect all client sessions.
Deactivate Clients	Click to deactivate the client sessions that you checked.

Reactivating Client Sessions

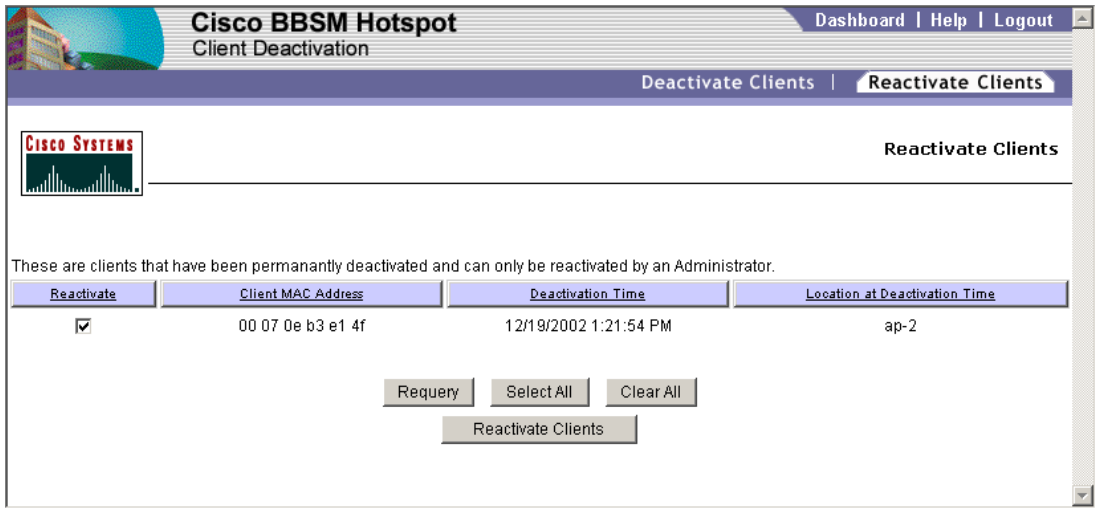
When clients have been permanently deactivated, the deactivation is absolutely permanent unless you reactivate them. For example, years later, the permanently deactivated MAC address will not be allowed on the system unless reactivated.

To reactivate a permanently deactivated client, follow the steps below.

Step 1 From the Dashboard, click **Client Deactivation**. The Deactivate Clients web page appears. (See Figure 4-20.)

Step 2 Click **Reactivate Clients**. The Reactivate Clients web page appears. (See Figure 4-22.)

Figure 4-22 Reactivate Clients Web Page



Step 3 Reactivate the desired clients, based on the information shown in Table 4-10.

Step 4 To save the changes, click **Reactivate Clients**.

Table 4-10 Reactivate Client Options

Option	Description
Reactivate	Check this check box to reactivate a client that was permanently deactivated.
Client MAC Address	Displays the client's MAC address.
Deactivation Time	Displays the date and time that the client was permanently deactivated.
Location at Deactivation Time	Displays the physical location of the client that was permanently deactivated.
Buttons	
Requery	Before you have saved any changes, click to return the web page to the previously saved settings.
Select All	Selects all of the clients.
Clear All	Deselects all of the clients.
Reactivate Clients	Click to reactivate the permanently deactivated clients.

Viewing and Installing Service Packs or Patches (Updates)

This section describes how to view, transfer, and install service packs or patches and view the patch log. BBSM Hotspot service packs or patches can be installed on any BBSM Hotspot server, or they can be installed on multiple servers from another computer in a remote location. Note that multiple files can be transferred to the BBSM Hotspot server before they are installed.

Before You Start

Before you begin transferring and installing files, read the following precautions to avoid problems:

- Transfer and install only service packs or patches properly obtained from Cisco to ensure successful updates.
- Make sure you select the proper file to avoid corrupting the database or preventing BBSM Hotspot from operating properly.
- Confirm that you can access the service pack executable file. Most BBSM Hotspot service packs and patches are available over the Internet. Be sure the file has been downloaded before continuing.
- We strongly recommend terminating all client sessions during these installations.
- Install service packs or patches during low-use time periods to minimize service interruptions and ensure proper functionality.
- If you are using Windows 2000 Professional or XP Professional and are logging onto the BBSM Hotspot server remotely, uncheck the Client for Microsoft Networks check box, as described in the steps below. By unchecking the check box, the ASP files will load much more quickly.

Step 1 Choose **Start > Settings > Network and Dial-up Connections**. The Network and Dial-up Connections window appears.

Step 2 Right-click **Local Area Connection**, and from the drop-down menu, choose **Properties**. The Local Area Connection Properties window appears. (See Figure 3-32 on page 3-28.)

Step 3 Uncheck the Client for Microsoft Networks check box.

Step 4 To close the windows, click **OK** three times.

Procedure

Use the following procedure to view or install service packs or patches and view the patch log.

Step 1 From the BBSM Hotspot Dashboard, click **WEBpatch**. The BBSM Hotspot Patches web page appears. (See Figure 4-23 and Table 4-11.)

Figure 4-23 BBSM Hotspot Patches Web Page

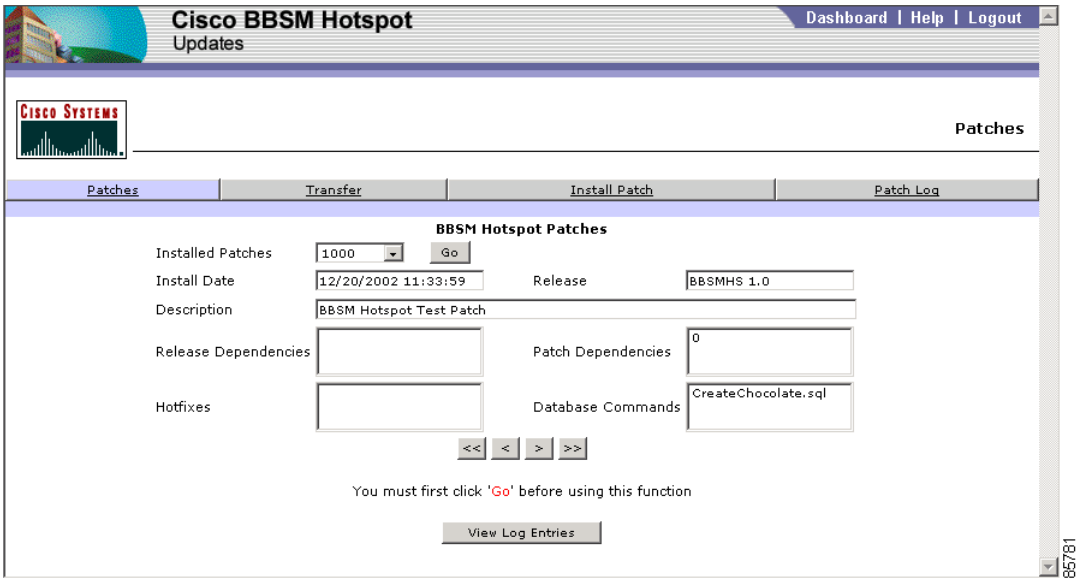


Table 4-11 BBSM Hotspot Patches Web Page Fields

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 Hotspot 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 Hotspot that must be installed on the target server before installing the service pack.
Patch Dependencies	Lists the previous service packs or patches that must be installed before the current service pack or patch can be installed.
Hotfixes	Shows the Microsoft hotfixes that are installed with the service pack or patch.
Database Commands	Displays the commands performed to modify or update the BBSM Hotspot database during the service pack/patch installation.

Step 2 View installed service packs, as follows:

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

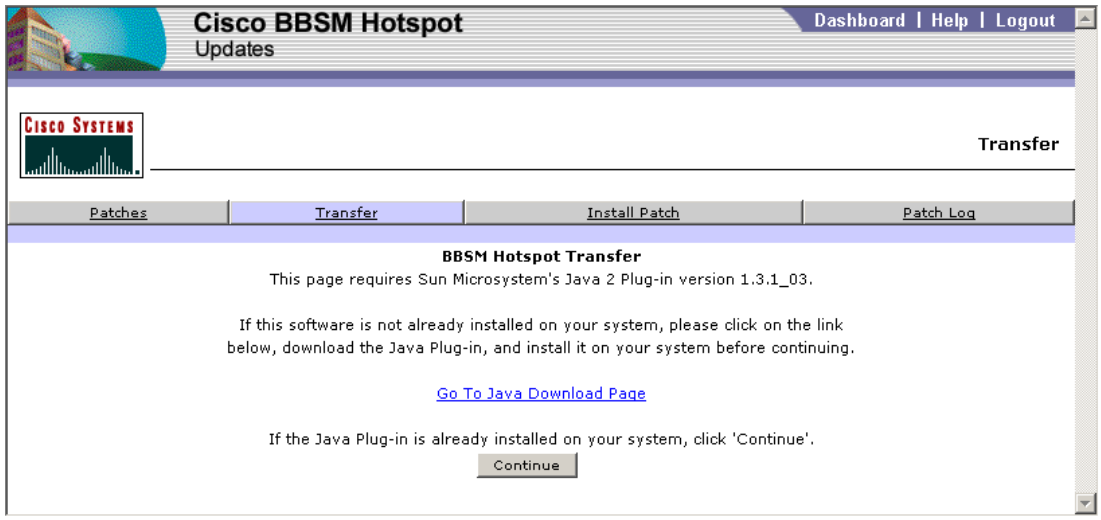
b. Click **Go**. The BBSM Hotspot Patches web page fields populate with the data for the specified service pack, and the View Log Entries button is enabled.

Step 3 Transfer and install service packs or patches, as follows:

a. Click **Transfer**. The BBSM Hotspot Transfer web page appears. (See Figure 4-24.)

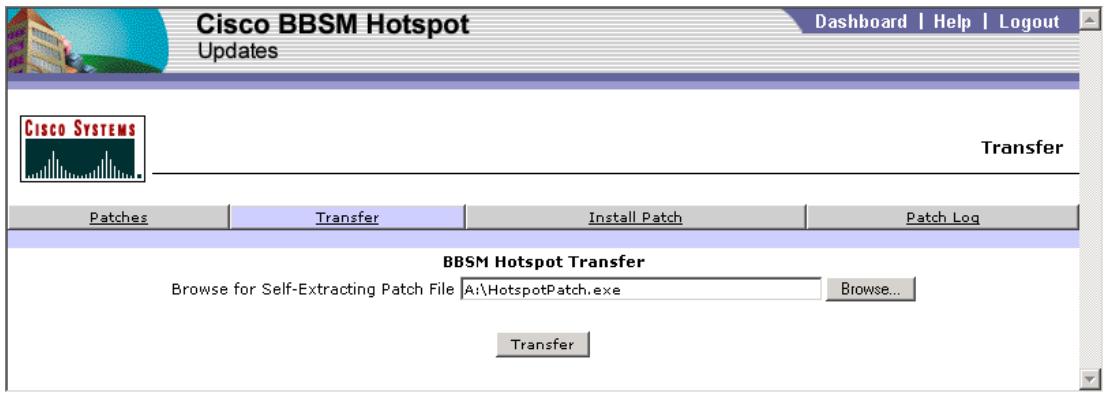
Note If you are updating BBSM Hotspot remotely and have not installed the Java 2 plug-in (version 1.3.1_03) that is needed to transfer files, click **Go To Java Download Page** and download and install the plug-in file. The BBSM Hotspot server ships with this plug-in already installed.

Figure 4-24 BBSM Hotspot Transfer Web Page



b. Click **Continue**. The BBSM Hotspot Transfer web page appears. (See Figure 4-25.)

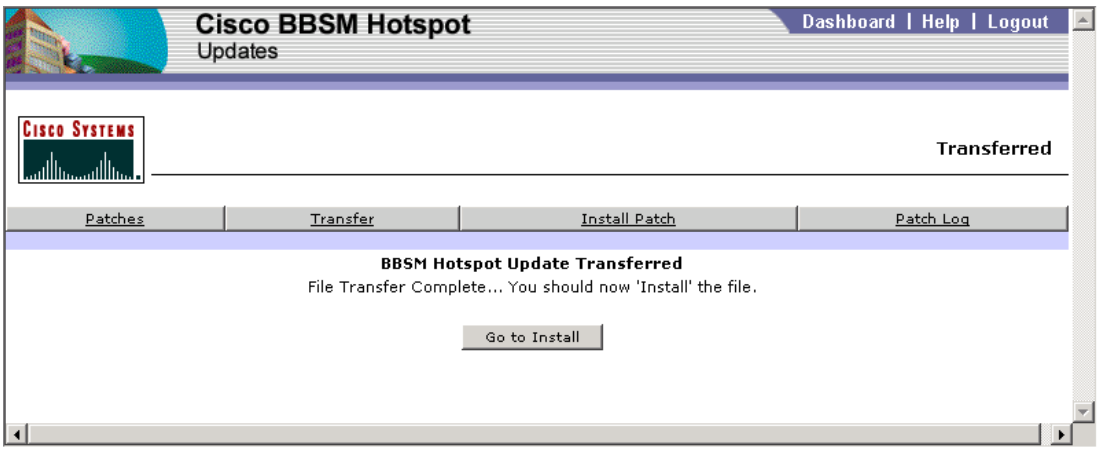
Figure 4-25 BBSM Hotspot Transfer, Browse Web Page



c. In the BBSM Hotspot Transfer field, click **Browse** to navigate to the file being installed, then click **Open**. The file name now appears in the BBSM Hotspot Transfer field.

d. Under the file name, click **Transfer**. The BBSM Hotspot WEBpatch Transferred web page appears, prompting you to install the file. (See Figure 4-26.)

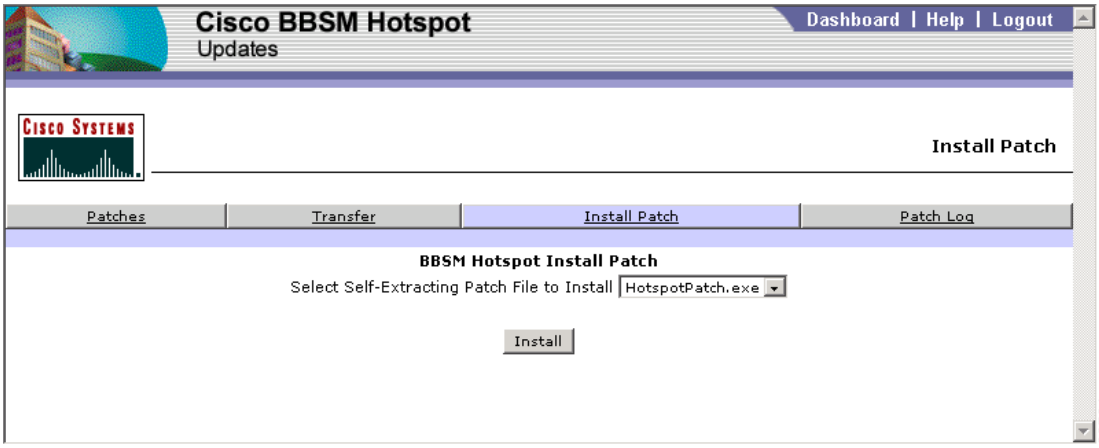
Figure 4-26 BBSM Hotspot WEBpatch Transferred Web Page



e. To install another file at the same time, click **Transfer** again to continue transferring files to be installed. After all files are transferred, continue with the installation.

f. Click **Go to Install**. The BBSM Hotspot Install Patch web page appears, displaying the transferred service pack in the drop-down menu. (See Figure 4-27.) (Instead of clicking Go to Install, you can also click Install Patch, which also takes you to the BBSM Hotspot Install Patch web page. From the drop-down menu, you can select the desired service pack to install.)

Figure 4-27 Install Patch Web Page



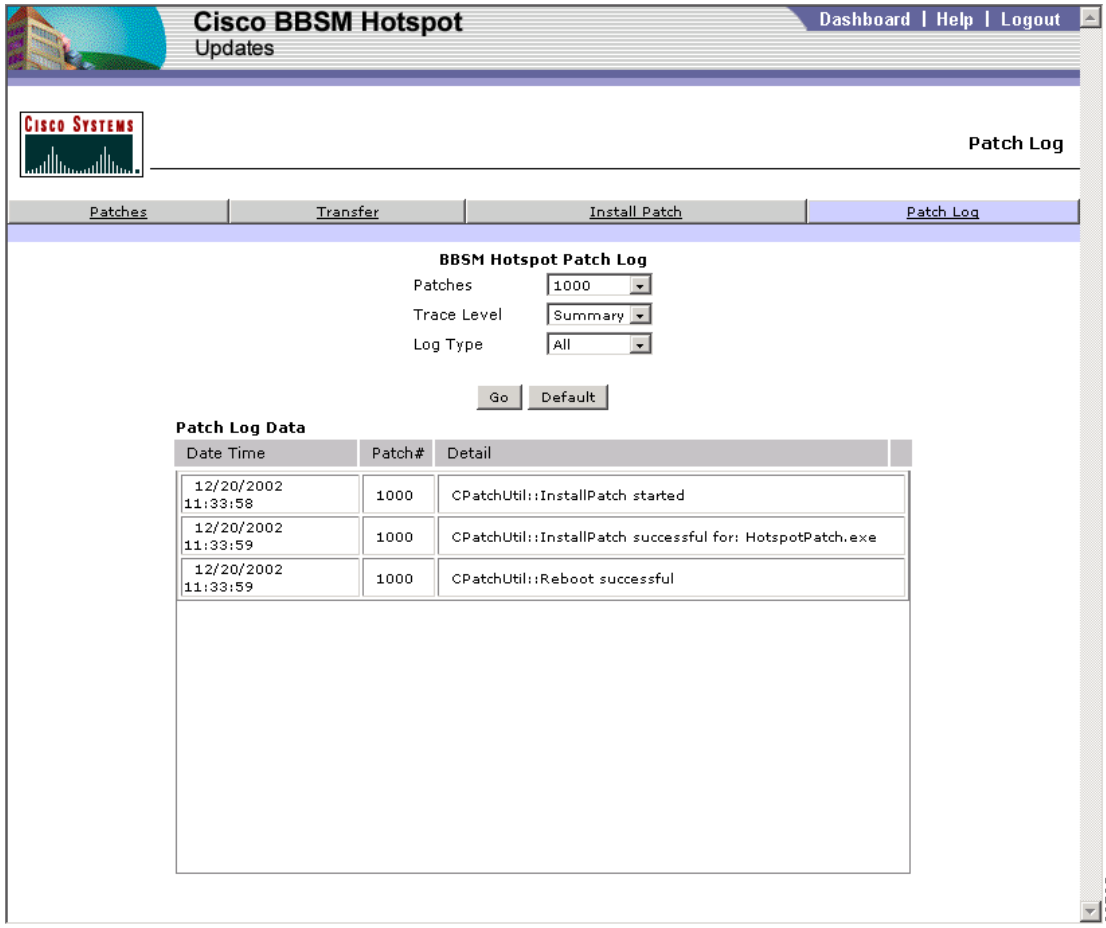
g. Click **Install**. The file is automatically verified and installed.

Note After the file has been installed, the BBSM Hotspot server may automatically reboot. You cannot access the BBSM Hotspot server while the server is rebooting.

Step 4 If desired, view the patch log for confirm that your patches have installed successfully and to view any messages, as follows:

a. Click **Patch Log**. The BBSM Hotspot Patch Log web page appears. (See Figure 4-28.) (This page can also be accessed from the Patches page by using the View Log Entries button.)

Figure 4-28 BBSM Hotspot Patch Log



b. From the drop-down menus at the top of the page, select the desired criteria, or click **Default**, which selects all service packs and patches, the Summary trace level, and All log types. (See Table 4-12.)

c. Click **Go**. The messages are displayed in the Patch Log Data table.

d. Note that if no log information meets the selected criteria, a dialog box appears, stating that no records exist for the selected criteria. (See Figure 4-29.) Click **OK** to return to the Patch Log page and change the search parameters.

Figure 4-29 No Records Dialog Box

Table 4-12 BBSM Hotspot Patch Log Web Page Fields

Field	Description
Drop-Down Menus	
Patches	• All (default setting)—Shows messages for all service packs or patches • <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 • Other—Displays messages generated by Windows and other programs during WEBpatch activities
Table Columns	
Date Time	The date and time that the patch was installed.
Patch #	The patch number.
Detail	The patch description.

Troubleshooting

Use this section to troubleshoot problems that may arise when using BBSM Hotspot. In addition to the information in this section, you can also find tips and answers to common questions by accessing the BBSM Hotspot website at http://www.cisco.com.

This section describes how to use the Trace debugging utility and the most common error messages and the suggested steps for resolving them.

Common Problems

The following are the most common problems that you or the end user might encounter when using BBSM Hotspot and the suggested corrective actions for resolving them.

No Start Page Received by End User

The end user tried to connect to the Internet and received this error message: "Sorry, a network error has occurred."

Probable Cause	Suggested Resolution
The user is trying to connect to BBSM Hotspot through an unsupported network device or through a network device that has not been set up within BBSM Hotspot.	Perform the steps below: • Verify that all network devices on site are on the supported hardware list and that they are correctly set up in BBSM Hotspot. • From the Hotspot Configuration NavBar, click **Network Devices**. Click Switches or Access Points to determine the IP address information of the various network devices. • Verify the connectivity to all network devices by pinging their IP address. • Verify the correct configuration of the network devices. • Correct any information and/or add any necessary network device information to the Hotspot Configuration pages. **Note** The port configuration may need to be updated if any changes were made to the switch information.
A previously generated port configuration has been corrupted, one or more network devices were added to this server and the port configuration was not updated, or a port configuration was never been generated for this site.	Perform the following steps: 1. Update or generate the port configuration. Refer to the "Configuring Network Devices" section on page 3-10. 2. Attempt to connect a client to see whether the problem has been resolved.
The SNMP read/write community string on the switch does not match the SNMP password on the BBSM Hotspot server.	Change the SNMP read/write community string so that both the server and the switch match. Refer to the "Configuring Network Devices" section on page 3-10.
A previously configured switch has lost its configuration.	Reconfigure the switch with the correct IP and SNMP parameters. These parameters may be obtained from an up-to-date copy of the network diagram. **Note** An on-site technician must perform this step.

No Internet Access

The end user receives the Start page, but cannot access the Internet.

Probable Cause	Suggested Resolution
When the following web pages are being used and the end user logs on to the Internet, the client is automatically redirected to the end user's home page: • FreeAccess • BlockICSClear • AccessCode • Hotspot • HotspotClear If the end user's home page URL is unresolvable, the end user will see one of the following error messages, although they are actually connected to the Internet: • "The page cannot be displayed..." The Disconnect box also opens. • "HTTP Proxy reports: (Connection timed out...)" • When the default ASP page is used, the end user sees the following error message: "You are Connected to the Internet... However, the Internet address you requested was unavailable. Please try another URL or try this one again later. Thank you."	In this case, the end user can simply enter another URL. In addition, if desired, the user can change the default home page.
The DNS server is not set to obtain DNS information from the Internet.	Enter the IP address of the ISP's DNS server. Refer to the "Configuring DNS Forwarding" section on page 2-30.
The DNS server has cached bad information or is not started.	Restart the DNS server: 1. Select **Start > Programs > Administrative Tools > Services**. 2. Right-click **DNS Server** and choose **Start** (or **Restart**).
The Internet may be slow or the site may not be responding.	Have the user try again later or try another site on the Internet.
The Internet connection (T-1 or T-3) from the ISP to the site may be down.	Submit a trouble call with the ISP.

E-mail

Users cannot send or receive e-mail using their normal ISP account while connected to BBSM Hotspot. Users may or may not be able to receive e-mail.

Probable Cause	Suggested Resolution
The end user's ISP does not accept e-mail from unrecognized sources or IP addresses to prevent its e-mail server from being used as a spam gateway. Normally, the user's computer receives its IP address from the ISP itself, so the address is recognized as valid. When the user logs on to the BBSM Hotspot network, the user's computer receives its IP address from the BBSM Hotspot server, which the ISP sees as foreign. When the user tries to send e-mail to this server, the server ignores the e-mail, because it does not recognize the source IP address as being on its own network.	If the BBSM Hotspot network provider has set up an SMTP server to resolve this problem, the IP address of that server can be configured within BBSM Hotspot. BBSM Hotspot will then intercept all SMTP packets and forward them to the IP address. This solution precludes the need for users to reconfigure their e-mail program. Set the SMTP forwarding address as follows: 1. From the Dashboard, click **Hotspot Configuration**. The Server Settings web page is appears. 2. Enter the IP address or FQDN of the SMTP server in the E-Mail Relay Server field. 3. Click **Save**.
The user normally connects to the Internet through their corporate network, which is behind a firewall.	In this instance, users must tunnel into their corporate network in order to receive e-mail. Refer to the resolution above to allow the users to send mail only.

RADIUS

The end user is unable to authenticate and cannot gain Internet access.

Probable Cause	Suggested Resolution
RADIUS is not correctly configured on the BBSM Hotspot server.	Check the following: • Verify that you can ping the RADIUS server IP address from the BBSM Hotspot server: – From the Hotspot Configuration NavBar, click **Billing** > **RADIUS**. – Verify that the RADIUS servers are configured with the same Shared Secret (password) as the BBSM Hotspot server. Refer to the "Configuring RADIUS Billing" section on page 3-19. – Verify that on the BBSM Hotspot server, RADIUS authentication is enabled and the authentication port is set to the same port that the RADIUS server is using. The default RADIUS port is 1645. Refer to the "Configuring RADIUS Billing" section on page 3-19. • Verify that the RADIUS server is configured to accept RADIUS requests from this site. • Verify that the user account is set up and is active on the RADIUS server. • Verify that the BBSM Hotspot server is using the correct page set.

No Functionality

BBSM Hotspot no longer functions.

Probable Cause	Suggested Resolution
In the process of changing all of the IP addresses, the procedure was not performed correctly.	Verify with the customer that the Address Change Wizard was used to change the BBSM Hotspot NIC IP addresses. If not, use the Network Control Panel to change the IP addresses of the BBSM Hotspot NICs back to the previous settings and run the Address Change Wizard to change the BBSM Hotspot NIC IP addresses to the correct settings. Refer to the "Running the Address Change Wizard" section on page A-1. Verify the Hotspot Configuration information and, if necessary, change it. Launch Hotspot Configuration and in the IP Addresses, Routers, and Network Devices web pages, change the IP address information. Refer to the "Configuring IP Addresses" section on page 3-3, the "Configuring Routers" section on page 3-6, and the "Configuring Network Devices" section on page 3-10. Verify the DNS server address and change it if necessary. Refer to the URL Error Page resolution below. Note that all network hardware must have its IP address settings changed separately by a technician.
A network device has been disconnected. The problem could be a bad Ethernet cable, an unplugged Ethernet or power cable, or the switch itself might be malfunctioning. If a switch is merely misconfigured, traffic will still pass through. In this case, the client would receive a DHCP address, and switches located downstream of the suspected switch would be reachable by support staff.	Using utilities such as ping and telnet, along with the network diagram, determine the most likely location of the failure using the following procedure. ⚠ **Caution** If replacing switches or moving cables, return the same cables to the exact same port, or the port configuration will be invalidated. 1. Determine which switches are not responding using the ping utility. 2. Telnet into a visible switch, if available, and try to ping the nonresponsive switches again. 3. If an IT staff is available and they do not mind assisting, ask them to help perform the following steps, or a technician must be sent to the property to perform these steps: – Check the unresponsive switches to ensure that all power and Ethernet cables are plugged snuggly into their respective sockets. – Ensure that any switch lights that are not lit. A link light that should be lit and is not may indicate that the wrong type of cable is being used. – Power cycle the switch by unplugging the power cable, waiting 5 to 10 seconds and plugging the power cable back into the switch. – Unplug the uplink cable from the suspected switch and plug it into a laptop configured for DHCP and try to get an IP address. If you can't get an IP address, the problem is likely upstream. If you can get an IP address, the problem is likely downstream. – Configure the laptop with the IP address of the BBSM Hotspot internal NIC and plug it into the uplink port of the suspected switch and try to ping the switch. 4. If the problem with a switch or switches cannot be resolved, replace the switches. **Note** Switch-to-switch and router-to-computer connections require a crossover cable. Switch-to-computer connections require a straight-through cable. Check the network diagram to determine which, if any, switches are downstream of the suspected switch. Note that the network diagram may not reflect recent changes.

Using the Trace Debugging Utility

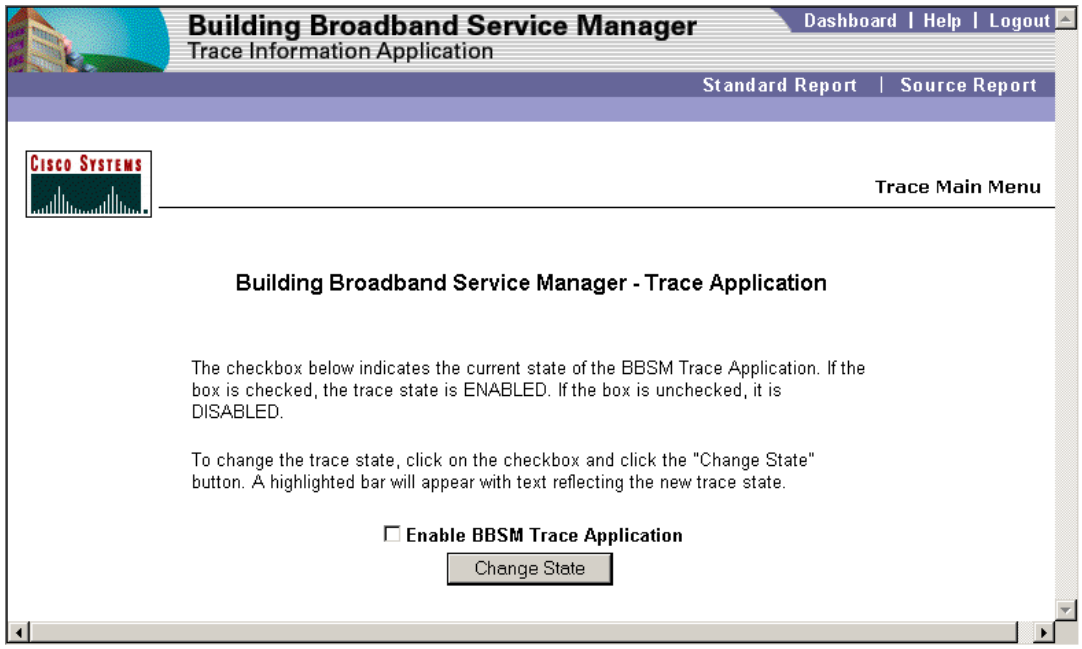
You can also use BBSM Hotspot's debugging utility, called *Trace*, to debug problems. This section provides basic steps for running the trace. The *Cisco BBSM 5.2 SDK Developer Guide* provides additional information about using trace that may be useful to developers.

Caution Enabling Trace impacts system performance, so we recommend disabling it after you have run the trace.

Step 1 Open Internet Explorer.

Step 2 Enter **http://<BBSM Hotspot_server:9488>/trace/** where <BBSM Hotspot_server> is the IP address of the BBSM Hotspot server in the address field. If you are running the browser on the server, you can replace <BBSM Hotspot_server> with "localhost" (without the quotes), and then hit **Enter**. The Trace Application Information web page appears. (See Figure 4-30.)

Figure 4-30 Trace Application Web Page



Step 3 To enable the trace application (or trace logging), check the **Enable BBSM Hotspot Trace Application** check box, and then click **Change State**.

Step 4 To view the results of the trace, click **Standard** or **Source**.

Step 5 To clear the trace information, click **Clear Trace Information Table**.

Step 6 After running the trace, disable trace logging to prevent system performance from being impacted. **Uncheck the Enable BBSM Hotspot Trace Application** check box and click **Change State**. Note that if you reboot the server, the trace is disabled.

Advanced Wizards

After you run the Setup Wizard in the initial configuration, you can run the Address Change Wizard or the Switch Discovery Wizard to change your configuration and add switches. For experienced technicians, you can also use these wizards, in conjunction with the BBSM Hotspot Dashboard options, to configure the server. These step-by-step procedures are described below:

Running the Address Change Wizard

This procedure describes how to run the Address Change Wizard for singlenet and multinet initial configurations. For the initial setup, run the Address Change Wizard after installing any service packs or patches. Because the NIC TCP/IP settings cannot be updated from Hotspot Configuration, use the Address Change Wizard to change IP addresses.

The default configuration is singlenet. Use the multinet configuration only if your BBSM server supports both private and public IP addresses. For a multinet configuration, you must configure Windows for multinet before running the Address Change Wizard.

Note If the TCP/IP properties are not set correctly, BBSM will not function properly.

Caution Be sure to close all active sessions before running any BBSM Hotspot wizard, including the Address Change Wizard. Refer to the "Deactivating Client Sessions" section on page 4-21.

Use the following procedure to configure the IP addresses.

Step 1 Choose **Start > BBSM Hotspot Wizards > Advanced Configuration > Address Change Wizard**. The IP Addresses window appears. (Figure A-1 shows the singlenet Port IP Addresses window, and Figure A-2 shows the multinet Port IP Addresses window.)

Figure A-1 BBSM Config Port IP Addresses Window (Singlenet)

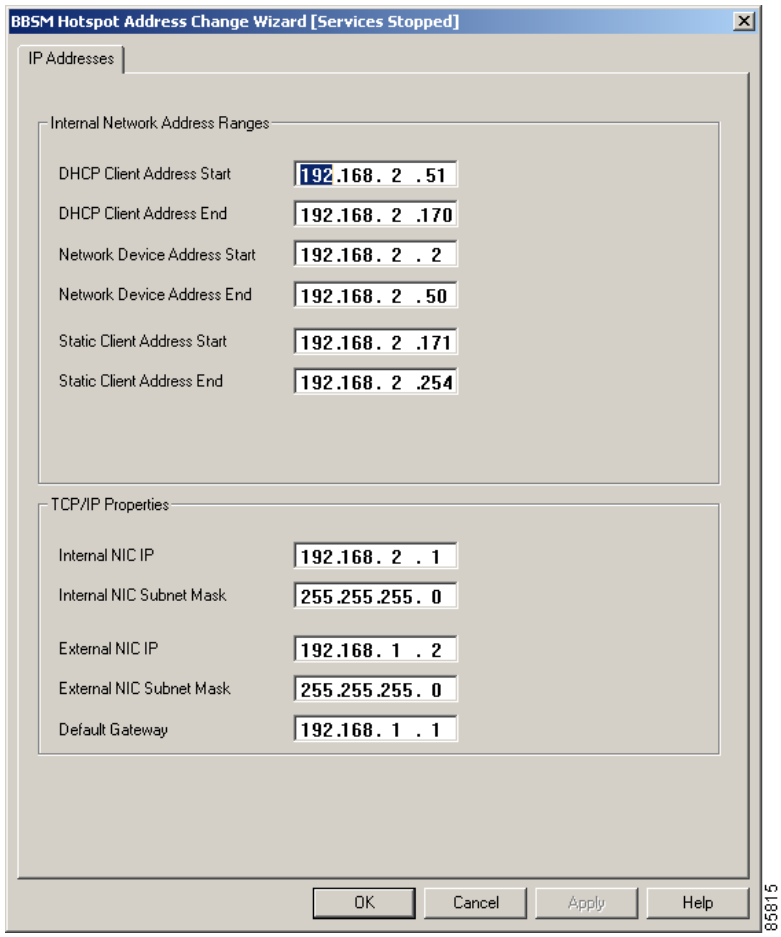
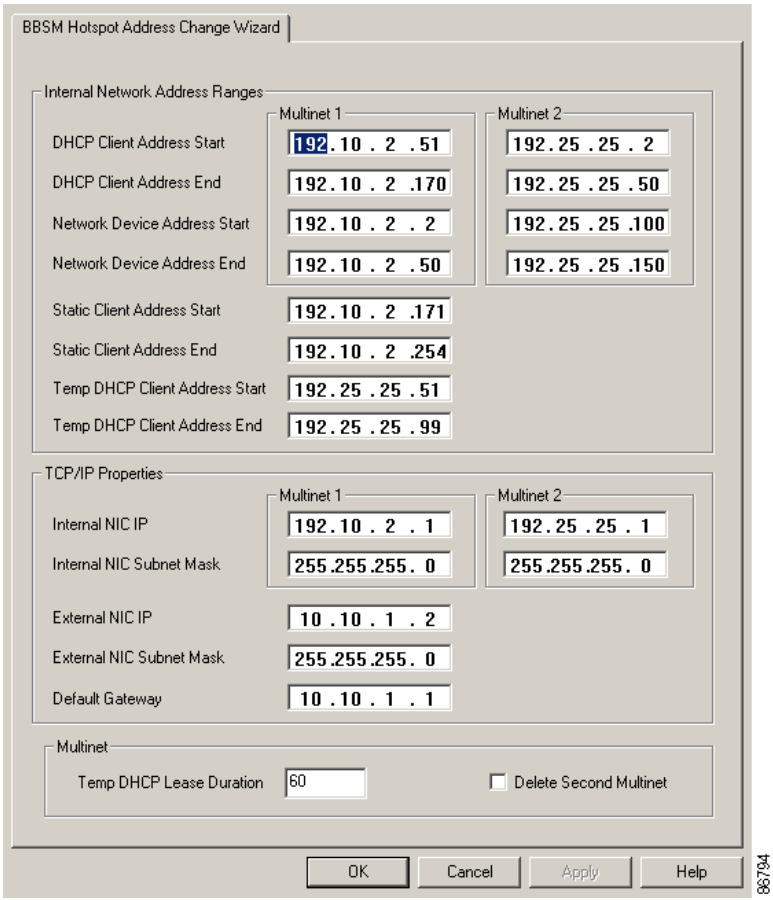


Figure A-2 IP Addresses Window (Multinet)



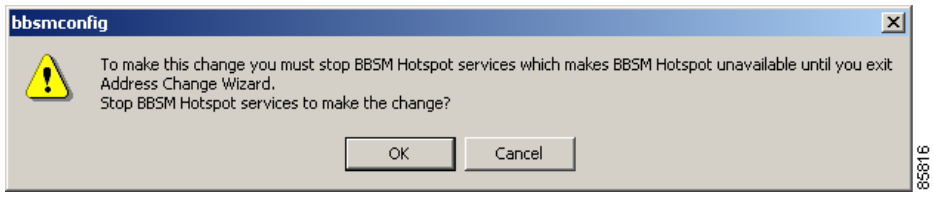
Step 2 Verify that the information in the BBSM TCP/IP Properties area is accurate.

Step 3 In the BBSM Internal Network Address Ranges area, enter the DHCP, Management, and Foreign (static) IP address range information. For the multinet configuration, enter the Temp DHCP information.

Note For field descriptions and notes, refer to Table 3-3 on page 3-6.

Step 4 Click **Apply**. A dialog box appears, telling you that you must stop BBSM Hotspot before you can run the Address Change Wizard. (See Figure A-3.)

Figure A-3 Stop BBSM Hotspot Services Dialog Box



Step 5 Click **OK** to stop BBSM Hotspot and close the dialog box. The Port IP Addresses window reappears.

Step 6 Click **OK**. The wizard begins the reconfiguration. When the configuration is complete, you must reboot the server for the changes to take effect. A dialog box appears, asking if you want to reboot the server at this time. (See Figure A-4.)

Figure A-4 Reboot Dialog Box

Step 7 To reboot the server, click **Yes**.

Step 8 After your server reboots, log in with the proper password.

Caution In a multinet configuration, to delete multinet 2 after the initial configuration, click **Delete Second Multinet** in the Multinet section. You must delete multinet 2 by using the Address Change Wizard. Although you used the Network and Dial-up Connections window to add multinet functionality, do not delete multinets through this window, because although multinet 2 is deleted from the GUI, it is not removed from the BBSM databases.

Running the Switch Discovery Wizard

The Switch Discovery wizard locates switches and access points connected to a BBSM network, determines their type, and creates records for them in the BBSM database. It works only with a network in a bridged configuration, not with a routed or mixed bridged and routed configuration.

The wizard finds only connected network switches or access points that have been configured with an IP address in the Network Device range (specified in the Address Change Wizard) and that have the same SNMP read/write community string.

Note that each cluster uses one IP address. The Switch Discovery Wizard does not create or enable the clusters; it only discovers the cluster members and adds their records to the BBSM database.

Caution If you want to cluster your switches, you must first create the Cisco clusters before running the Switch Discovery Wizard. Before you can create a cluster, you must have the Java plug-in on your machine.

To download the Java plug-in, go this website:

http://www.cisco.com/pcgi-bin/tablebuild.pl/java

For information that explains how to create a cluster, go to these Cisco websites:

http://www.cisco.com/warp/public/cc/techno/media/lan/ether/sgth/index.shtml

http://www.cisco.com/warp/public/cc/pd/si/casi/ca3550/prodlit/cclms_ds.htm

For information that explains how to debug switch connectivity problems, go to this website:

http://www.cisco.com/en/US/products/hw/switches/ps607/products_tech_note09186a0080094709.shtml#javaplugin

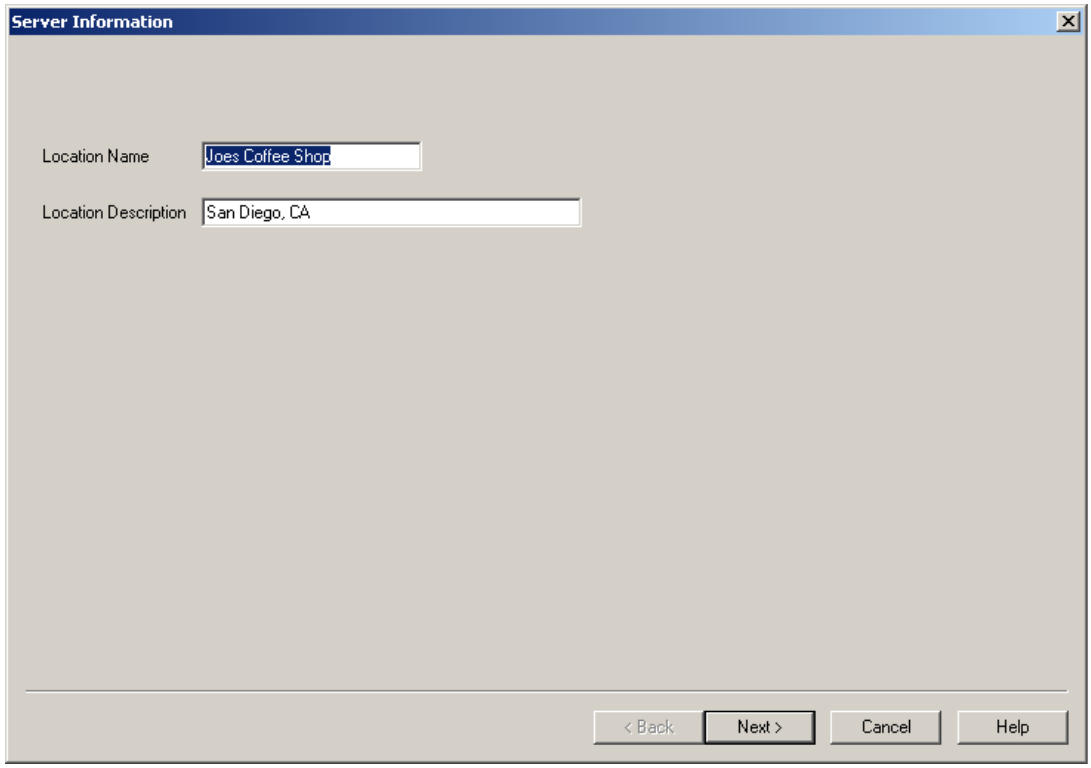
Note Because clustered switches cannot have the same SNMP password, you only need to enter the SNMP password of the master switch, and the Switch Discovery Wizard will locate all the switches in the cluster.

Caution Be sure to close all active sessions before running any BBSM Hotspot wizard, including the Switch Discovery Wizard. Refer to the "Deactivating Client Sessions" section on page 4-21.

Use the following procedure to run the Switch Discovery wizard:

Step 1 Choose **Start > BBSM Hotspot Wizards > Advanced Configuration > Switch Discovery Wizard**. The Server Information dialog box appears. (See Figure A-5.)

Figure A-5 Server Information Dialog Box



Step 2 Enter the server location name and description.

Step 3 Click **Next**. The Network Device Information dialog box appears. (See Figure A-6 for a singlenet configuration and Figure A-7 for a multinet configuration.)

Note The Network Device Information dialog box lets the administrator specify the IP address range of the network devices. If the switch's cluster capability is enabled, the application automatically detects the cluster members and adds them to the database.

Figure A-6 Network Device Information Dialog Box (Singlenet)

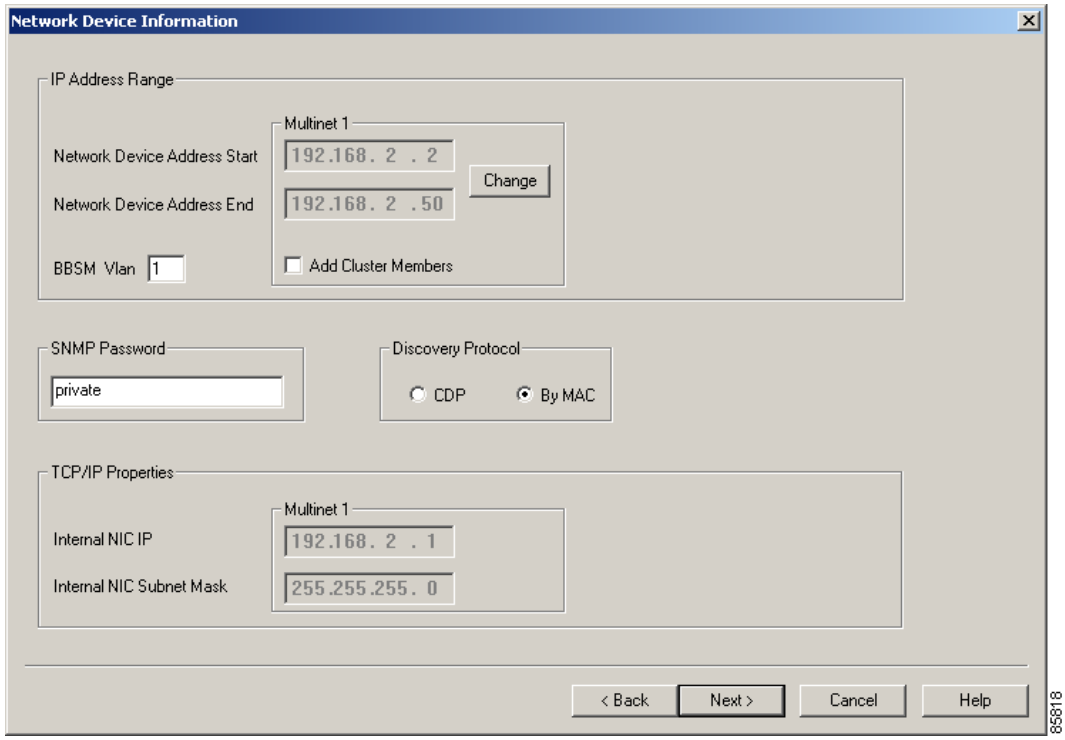
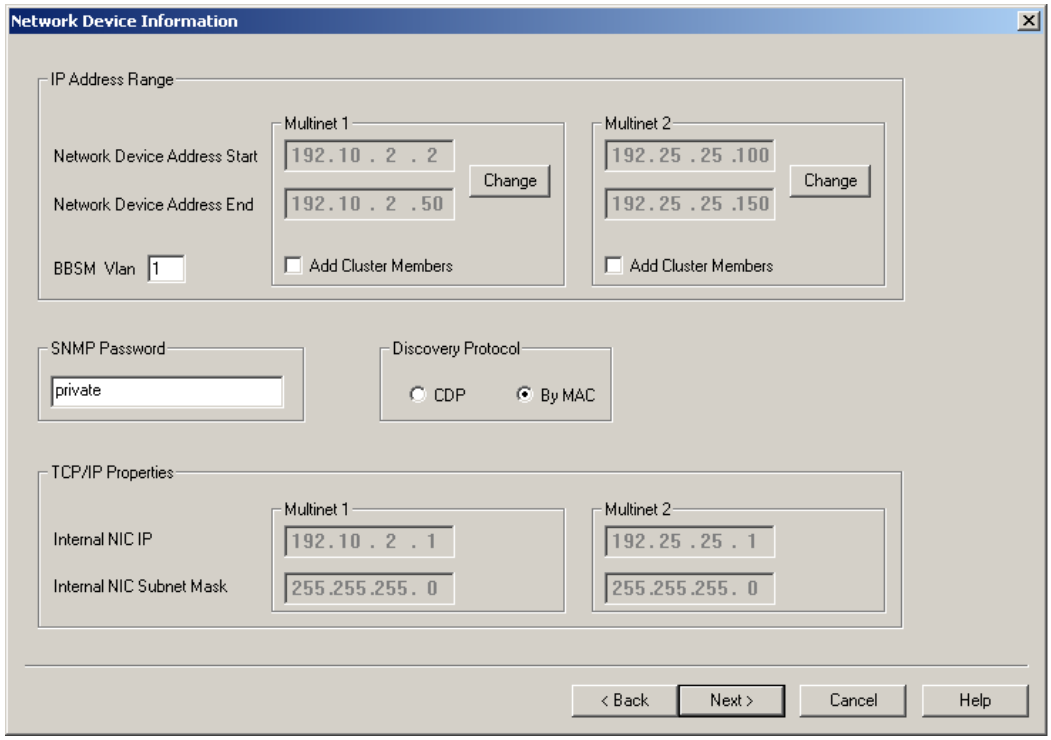


Figure A-7 Network Device Information Dialog Box (Multinet)



Step 4 Verify that the information is correct, or make any changes based on the information in Table A-1.

Table A-1 Network Devices Information Options

Field	Description
IP Address Range	
Network Device Address Start	Displays the beginning IP address of the Network Device IP address range. This IP address is obtained from the Address Change Wizard.
Network Device Address End	Displays the ending IP address of the Network Device IP address range. This IP address is obtained from the Address Change Wizard.
BBSM Vlan	Displays the default VLAN number. You need to change this value if you are using a non-default management VLAN number in your BBSM network. All network devices on the BBSM internal NIC must have this VLAN number.
Add Cluster Members	Check this check box if you want to add all cluster members to the Switches Table in the AtDial database. This application automatically detects the cluster members.
SNMP Password	
SNMP Password	Displays the default name “private.” You can change this name if you want to.
Discovery Protocol	
CDP	This is the Cisco Discovery Protocol. If you are using Cisco switches exclusively, this option is more efficient for discovering the network topology.

Table A-1 Network Devices Information Options

Field	Description
By MAC	If you are only using Cisco switches or a combination of Cisco and non-Cisco switches, use this option. This protocol uses the MAC address of the switch to discover the network topology.
TCP/IP Properties	
Internal NIC IP	Displays the Internal NIC IP address for Multinet 1 (and Multinet 2, if applicable), which is obtained from the Address Change Wizard.
Internal NIC Subnet Mask	Displays the Internal NIC Subnet Mask IP address, which is obtained from the Address Change Wizard that you used prior to the Switch Discovery Wizard.
Buttons	
Back	Click this button to return to the previous page of the Switch Discovery Wizard.
Next	Click this button to continue to the next page of the Switch Discovery Wizard.
Cancel	Click this button to exit from the Switch Discovery Wizard.
Help	Click this button to access the Switch Discovery Wizard online help.

Step 5 Click **Next**. The Locating Network Devices dialog box appears. (See Figure A-8 for a singlenet configuration and Figure A-9 for a multinet configuration.)

Caution If the switches are not correctly configured for clustering, BBSM will not add them to the correct cluster, and they will have to be added manually after they have been configured.

Figure A-8 Locating Network Devices Dialog Box (Singlenet)

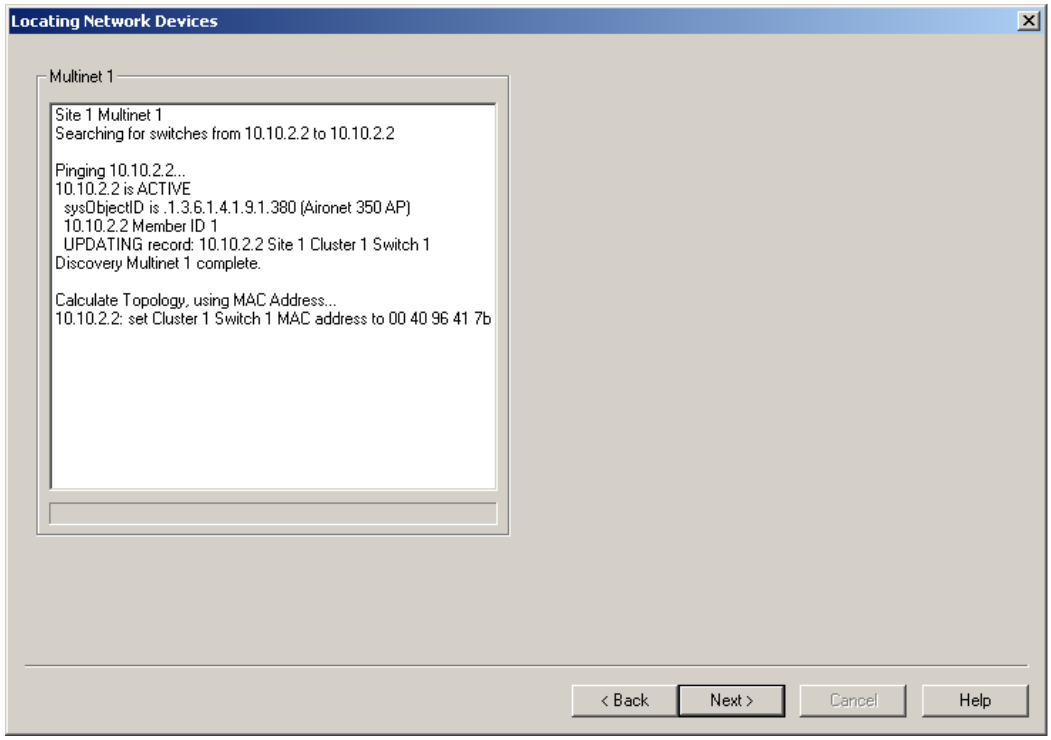
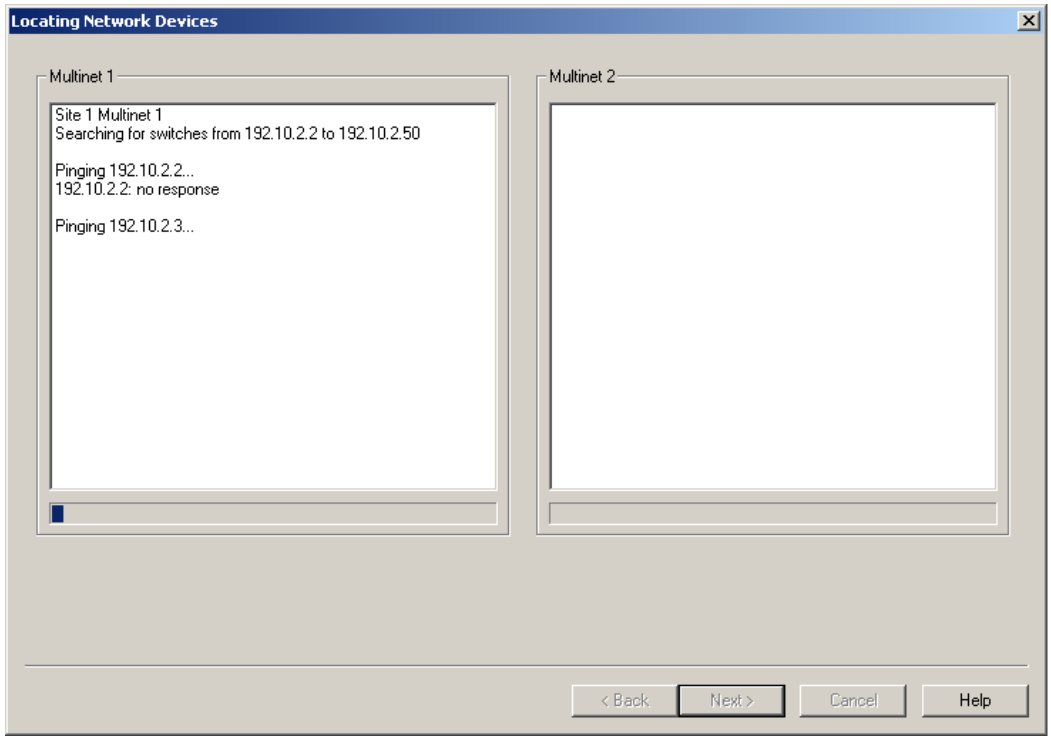


Figure A-9 Locating Network Devices Dialog Box (Multinet)



Note If more than one switch type with the same sysObjectID is discovered, the Select Switch Type dialog box appears. (See Figure A-10.) If this occurs, select the actual switch type, and click **OK**. The SwitchDiscovery dialog box then appears. (See Figure A-11.) Click **Yes** to verify that you selected the proper switch. You will only see the following two dialog boxes if there is more than one switch type with the same sysObjectID.

Figure A-10 Select Switch Type Dialog Box

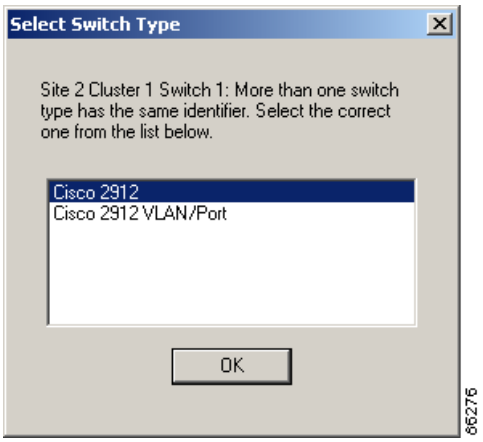
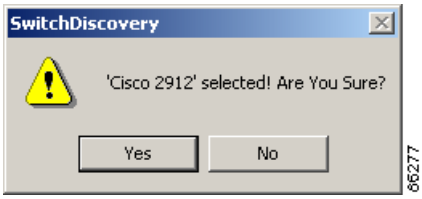


Figure A-11 SwitchDiscovery Dialog Box



Step 6 From the Locating Network Devices dialog box, click **Next**. The Port Settings dialog box appears. (Figures A-12 and A-13 show singlenet and multinet configurations.)

Figure A-12 Port Settings Dialog Box (Singlenet)

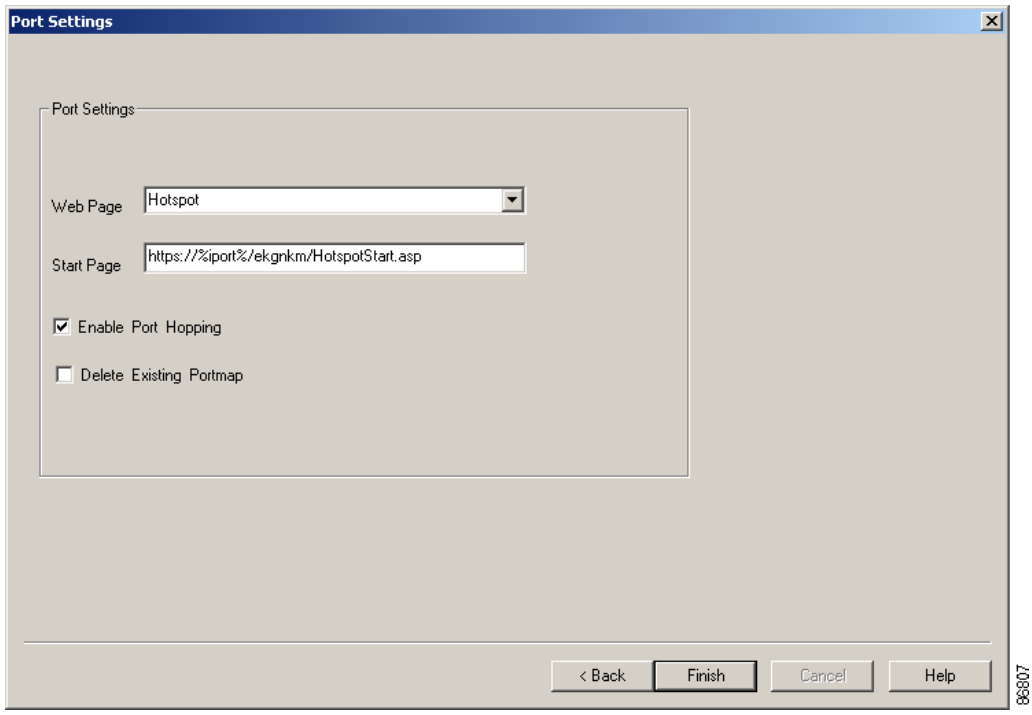
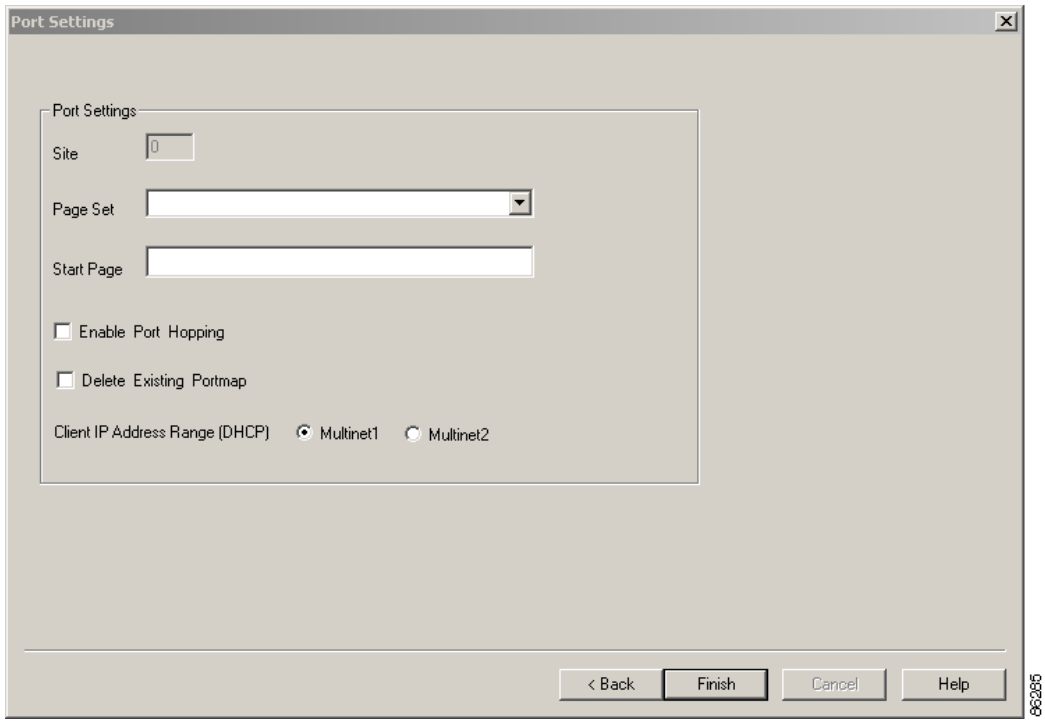


Figure A-13 Port Settings Dialog Box (Multinet)



Step 7 Configure the port settings based on the information shown in Table A-2.

Table A-2 Generating Port Settings Options

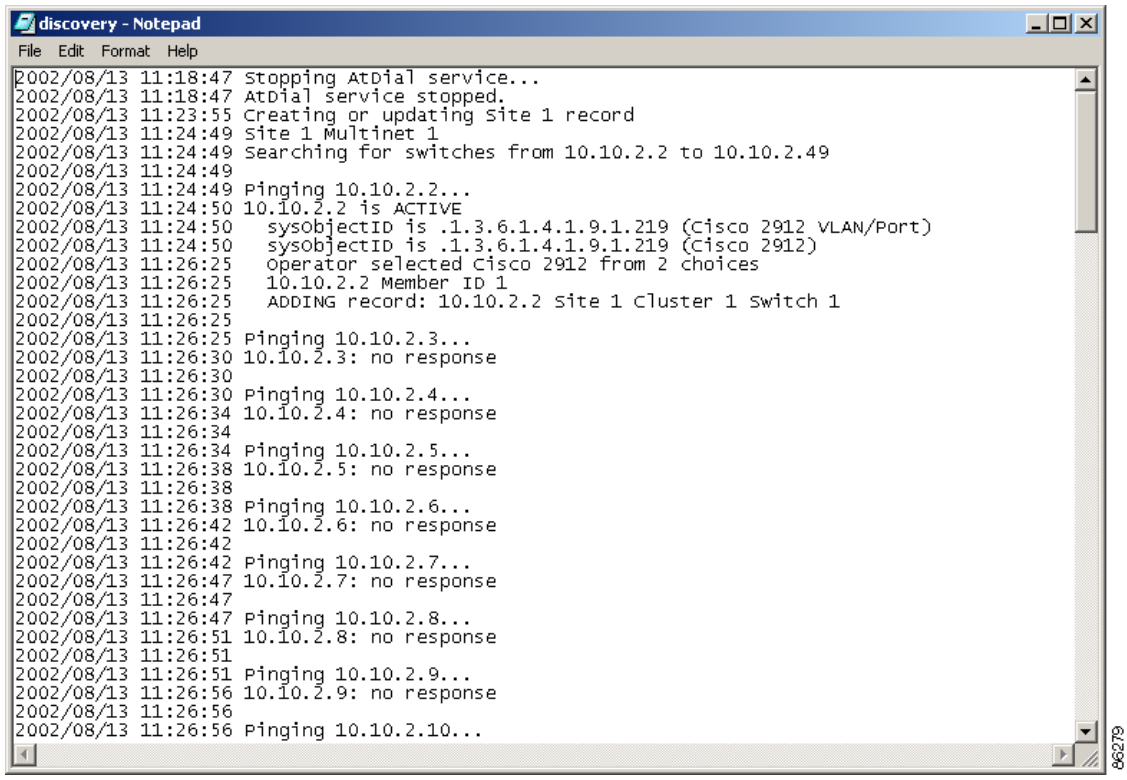
Field	Description
Port Mapping	
Web Page	From the drop-down menu, select the appropriate web page for the site that you are configuring. **Note** If you will be using SSL and have not yet installed your SSL certificate, select the "Clear" web page until you install the certificate and then change your web page to the SSL web page. For example, select RADIUSClear until the certificate is installed, then after installing the certificate, change the web page to RADIUS.
Start Page	The Start Page field will automatically populate with the URL that corresponds with the web page that you just selected.
Enable Port Hopping	Check this check box if you want to enable the BBSM port hopping feature. This will enable all switches for port hopping and allow the end user to move between network hardware such as access points or switch ports in a BBSM network without interrupting service. If you want to enable port hopping on specific ports, use the Network Device Port Settings pop-up window in Hotspot Configuration.
Delete Existing Port Map	Check this check box if you want to delete the existing port map.
Client IP Address Range (DHCP) *(multinets only)*	This field only appears during a multinet configuration. DHCP assigns leases to clients from either Multinet 1 or Multinet 2 IP address ranges. Select the appropriate multinet that you want to use. **Note** The web page overrides this setting if the web page specifies which multinet to use.
Buttons	
Back	Click this button to return to the previous page of the Switch Discovery Wizard.
Finish	Click this button to complete the last step of the Switch Discovery Wizard.
Cancel	Click this button to exit from the Switch Discovery Wizard.
Help	Click this button to access the Switch Discovery Wizard online help.

Step 8 Click **Finish**. The SwitchDiscovery completion dialog box appears. (See Figure A-14.)

Figure A-14 Switch Discovery Complete Dialog Box

Step 9 Click **OK**. Windows Notepad opens, displaying a log of Switch Discovery activities. (See Figure A-15.)

Figure A-15 Switch Discovery Activities Window



Step 10 After reviewing the log, close the window.

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 Hotspot 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 encryption, which refers 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 and configure the page sets for SSL to prevent the unauthorized interception of confidential data. BBSM Hotspot requires the use of 128-bit encryption.

Caution Until you install your SSL certificate, select the “Clear” version of the RADIUS or credit card page set and then change your page set to the SSL page set. For example, select RADIUSClear until the certificate is installed, then after installing the certificate, change the page set to RADIUS. If you do not install the certificate first, the Start page will not display.

Purchasing a Domain Name

You must purchase a fully qualified domain name (FQDN) for the BBSM Hotspot server before you can purchase a Secure Server Digital ID (certificate). A domain name that is purchased for a server other than BBSM Hotspot will not work.

Use the following steps to purchase the domain name.

Step 1 Go to http://www.verisign.com, or the website of your choice, to access their online enrollment form to purchase a domain name.

Note Domain names can be purchased from other companies. Cisco does not endorse any particular company.

Step 2 Follow the online instructions.

Step 3 Proceed with registration and payment to complete your order. Be sure to print a receipt before closing your browser.

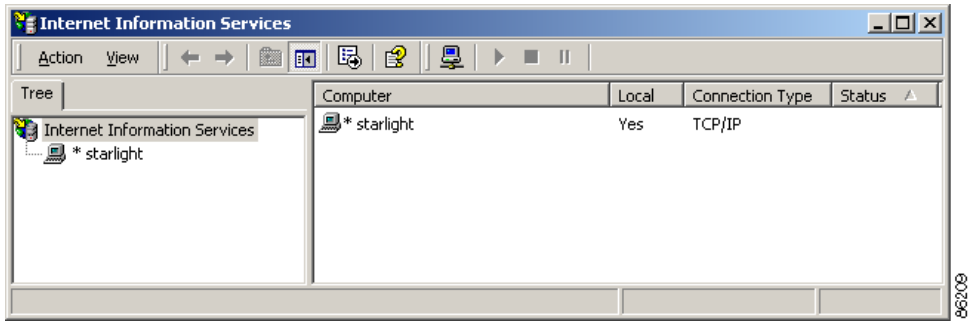
Generating a Certificate Signing Request

Use the following procedure to generate a Certificate Signing Request for your web server certificate. The BBSM Hotspot administrator should perform this procedure.

Note BBSM Hotspot servers use Microsoft IIS 5.0.

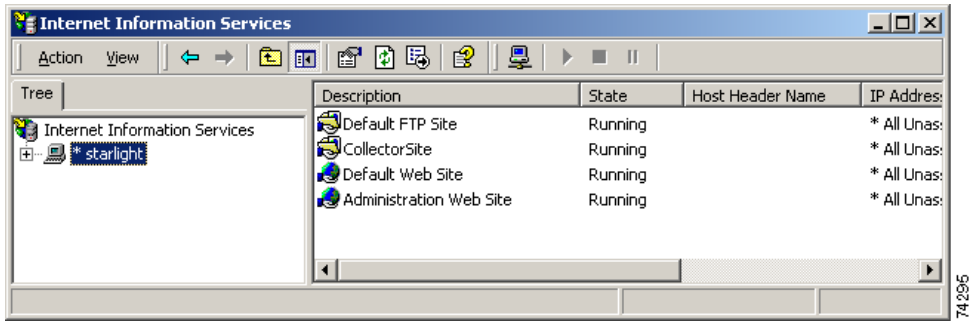
Step 1 From the BBSM Hotspot desktop, choose **Start > Programs > Administrative Tools > Internet Services Manager**. The Internet Information Services window appears. (See Figure B-1.)

Figure B-1 Internet Information Services Window



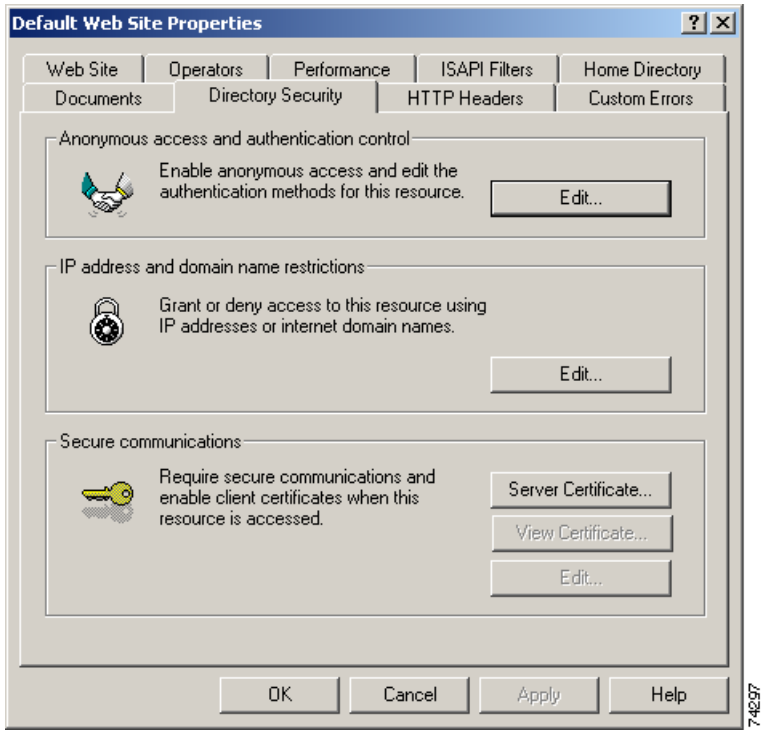
Step 2 In the left pane, click the server name. (The example server name is "starlight" in Figure B-2.) The server folders appear in the right pane.

Figure B-2 Internet Information Services Description Window



Step 3 In the right pane, right-click **Default Web Site**, and select **Properties**. The Default Web Site Properties dialog box appears. (See Figure B-3.)

Figure B-3 Default Web Site Properties Dialog Box



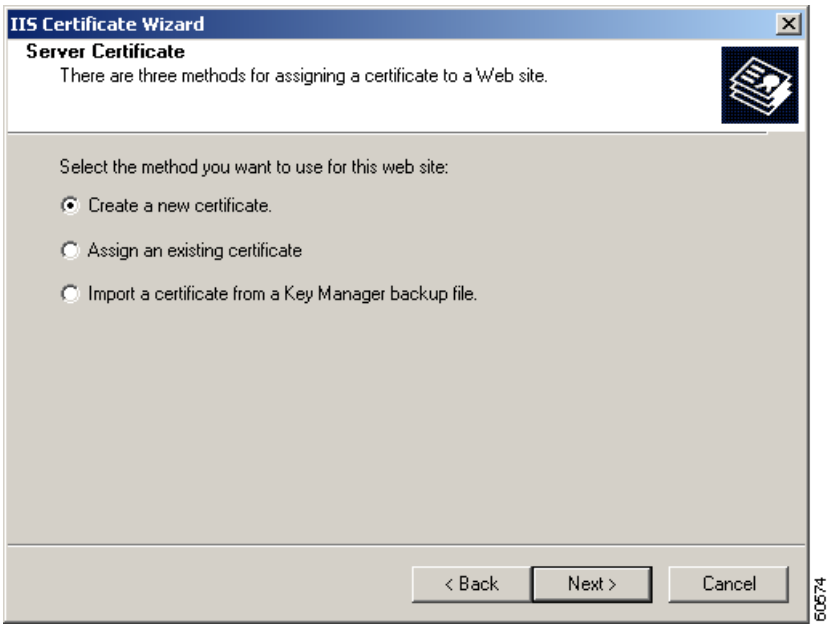
Step 4 Click the **Directory Security** tab.

Step 5 In the Secure communications section, click **Server Certificate**. The Welcome to the Web Server Certificate Wizard dialog box appears. (See Figure B-4.)

Figure B-4 Welcome to the Web Server Certificate Wizard Dialog Box

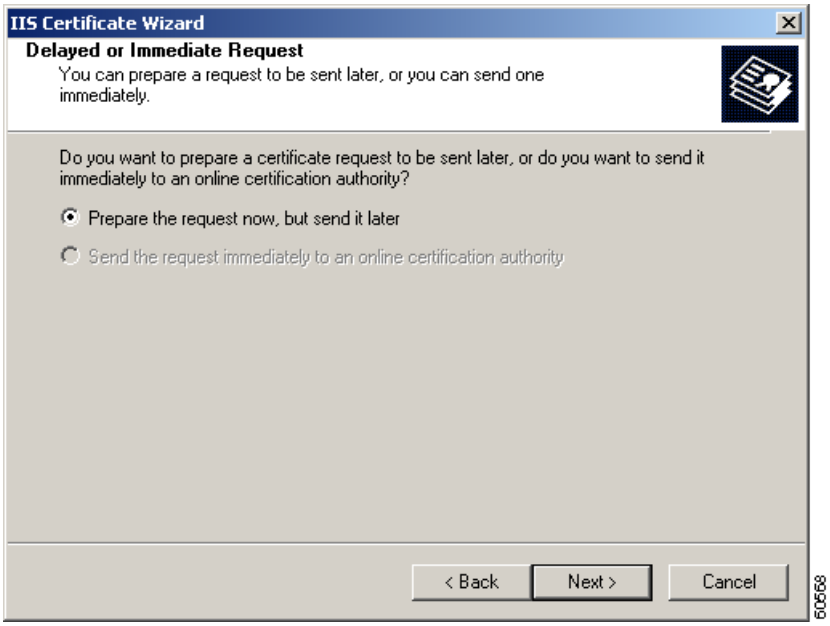
Step 6 Click **Next**. The Server Certificate dialog box appears. (See Figure B-5.)

Figure B-5 Server Certificate Dialog Box



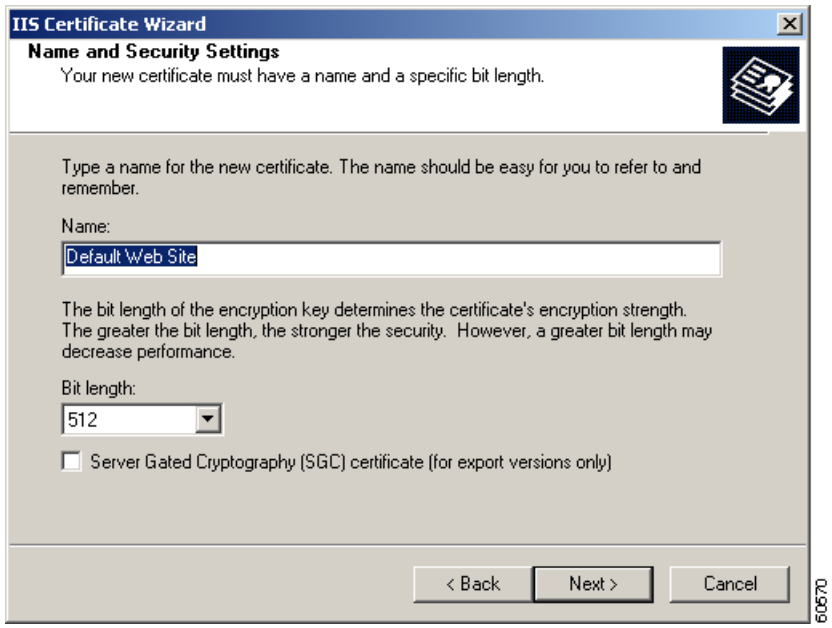
Step 7 Verify that the **Create a new certificate** radio button is selected. If it is not, select it. Then click **Next**. The Delayed or Immediate Request dialog box appears. (See Figure B-6.)

Figure B-6 Delayed or Immediate Request Dialog Box



Step 8 Verify that the **Prepare the request now, but send it later** radio button is selected. If it is not, select it, and then click **Next**. The Name and Security Settings dialog box appears. (See Figure B-7.)

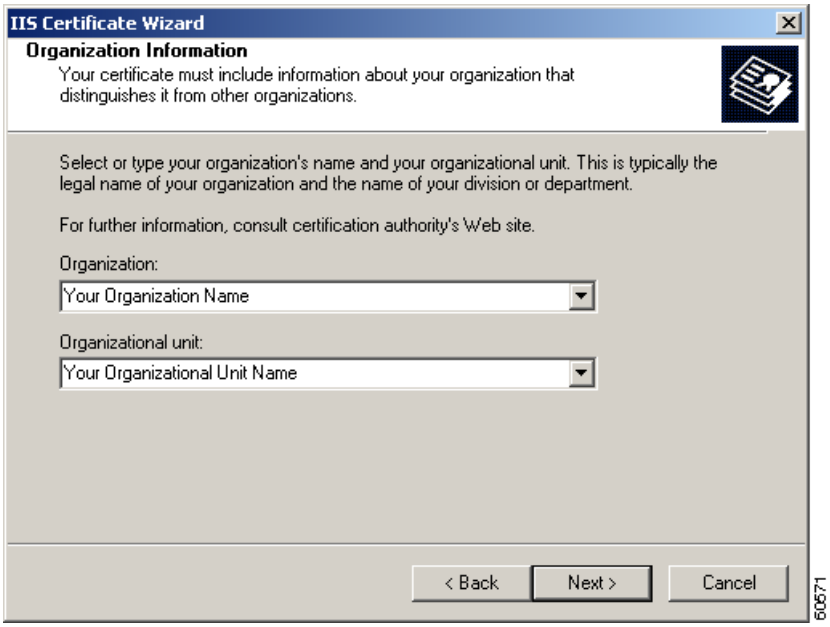
Figure B-7 Name and Security Settings Dialog Box



Step 9 Type a descriptive name for the new certificate, such as "SDPacificPlazaBBSM Hotspot."

Step 10 In the Bit length drop-down menu, keep the default setting, and then click **Next**. The Organization Information dialog box appears. (See Figure B-8.)

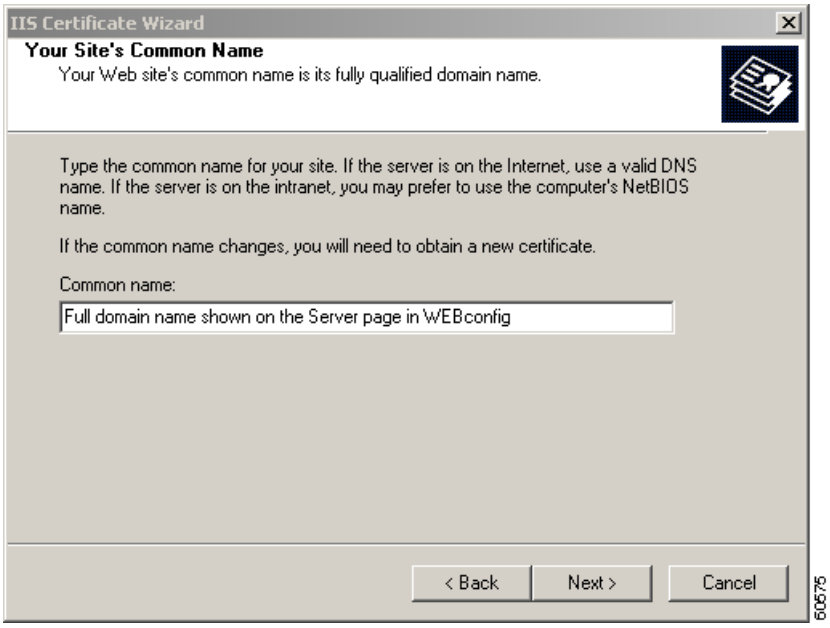
Figure B-8 Organization Information Dialog Box



Step 11 In the Organization and Organizational unit fields, enter your organization and organizational unit names. (You cannot use commas in these fields.)

Step 12 Click **Next**. The Your Site's Common Name dialog box appears. (See Figure B-9.)

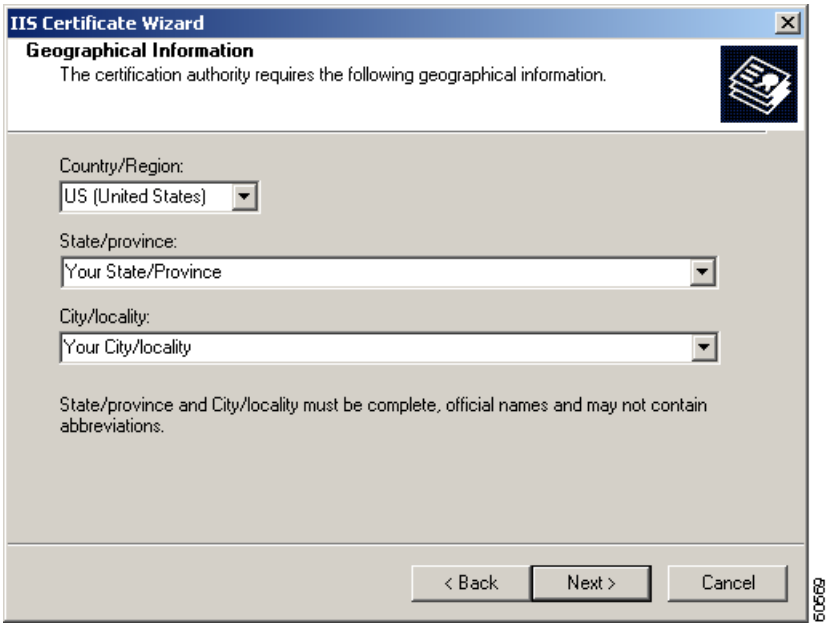
Figure B-9 Your Site's Common Name Dialog Box



Step 13 In the Common name field, enter your website's common name, and then click **Next**. The Geographical Information dialog box appears. (See Figure B-10.) This is the name that is entered on the Security/SSL page in WEBconfig. Refer to the "Configuring Security/SSL" section on page 3-22, Step 3.

Note Do not include "www" when you enter your website's common name. For example, enter **cisco.com**, not www.cisco.com. If the common name changes, you must obtain a new certificate. If you are using SSL page sets, go to the Security/SSL web page in WEBconfig, check the **Enable Domain Name for SSL Page Sets** check box, enter the same common name in the Full Domain Name field, and click **Save**.

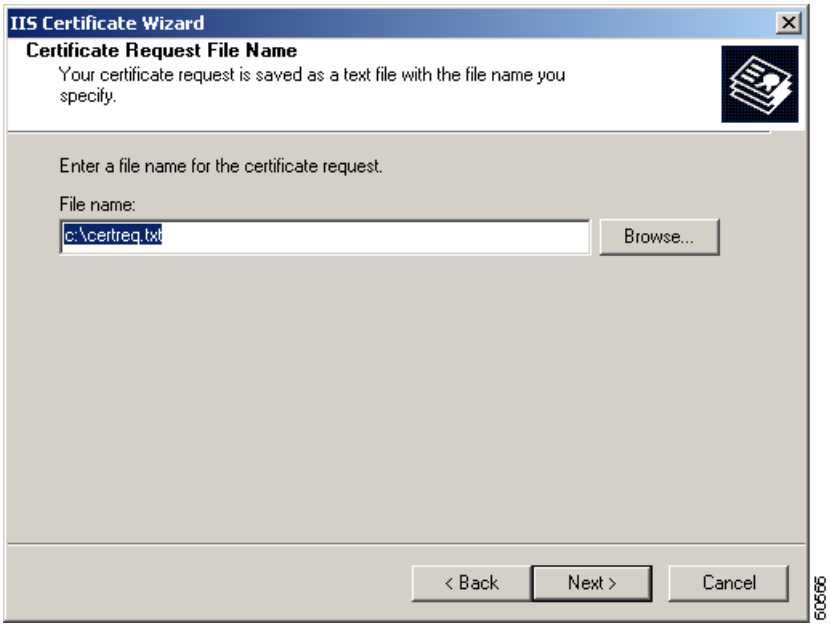
Figure B-10 Geographical Information Dialog Box



Step 14 Enter the requested information in the geographical fields, and click **Next**. The Certificate Request File Name dialog box appears. (See Figure B-11.)

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.

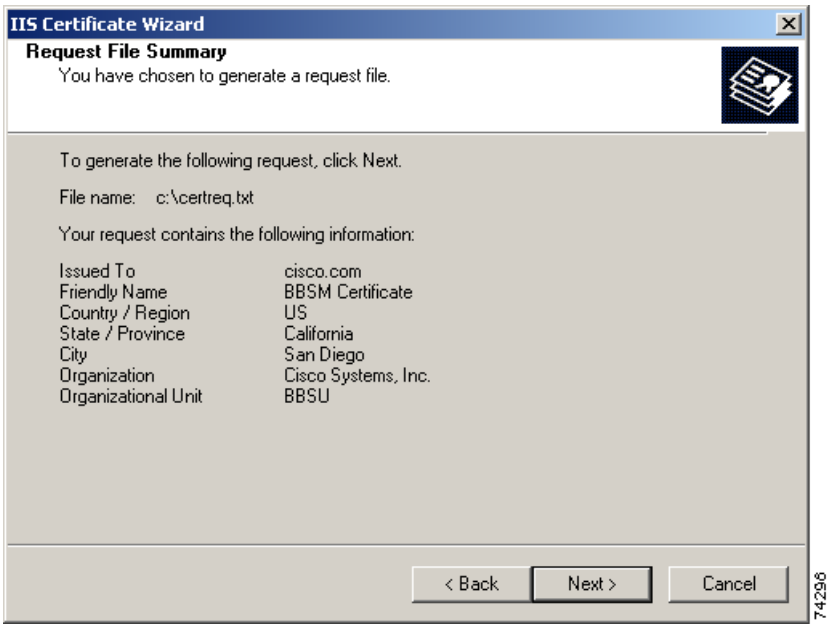
Figure B-11 Certificate Request File Name Dialog Box



Step 15 Use the default file name, or enter a new name for the certificate request. (Your certificate request is saved as a text file with the file name that you specify. We recommend that you make a backup copy of this file and store it in a secure location.)

Step 16 Click **Next**. The Request File Summary dialog box appears. (See Figure B-12.)

Figure B-12 Request File Summary Dialog Box



Step 17 Verify that the information is correct, and click **Next**. The Completing the Web Server Certificate Wizard dialog box appears. (See Figure B-13.)

Figure B-13 Completing the Web Server Certificate Wizard Dialog Box

Step 18 To close the dialog box, click **Finish**.

Step 19 To close the Default Web Site Properties dialog box, click **OK**.

Step 20 Close the Internet Information Services window.

You have now generated a Certificate Signing Request. Continue with the following sections to purchase a certificate and install it on the BBSM Hotspot server.

Purchasing a Secure Server ID from a Certificate Authority

After generating the Certificate Signing Request on your BBSM Hotspot server, you must purchase a Secure Server Digital ID (certificate) from a certificate authority (CA), such as VeriSign. This will authenticate your website and enable SSL encryption technology.

Note Secure Server Digital ID's can be purchased from other companies, as well. 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 must have a DUNS number to enroll. If you don't, contact Dun & Bradstreet.

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-----
```

Step 5 Complete the rest of the online application, making sure that the information you enter is correct.

Installing the Granted Certificate

After submitting your completed application, your domain's Technical and Organizational Contacts will receive an e-mail message confirming enrollment within a few hours of submitting the order. It usually takes at least 3 to 5 working days to issue your certificate.

Note You cannot perform this procedure until you have received your certificate from the certificate authority and copied it onto your BBSM Hotspot server.

Use the following procedure to install the granted certificate onto your BBSM Hotspot 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**, and select **Properties**. The Default Web Site Properties dialog box appears.

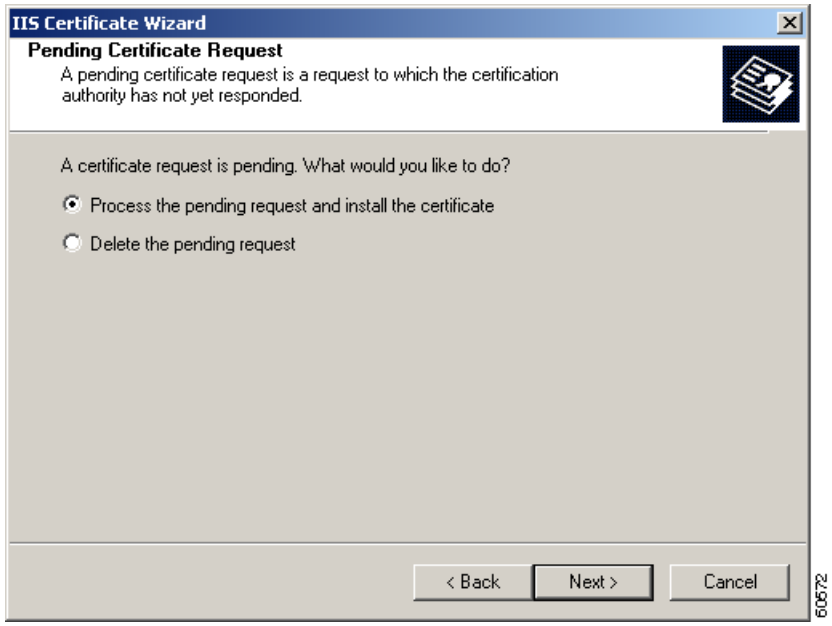
Step 4 Click the **Directory Security** tab. The Directory Security window appears.

Step 5 In the Secure Communications pane, click **Server Certificate**. The Welcome to the Web Server Certificate Wizard window appears. (See Figure B-14.)

Figure B-14 Welcome to the Web Server Certificate Wizard Dialog Box

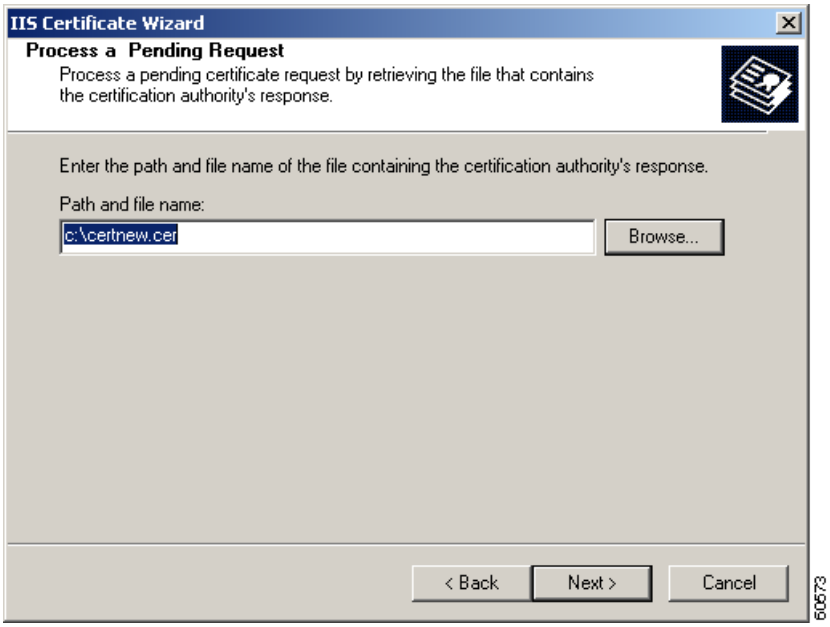
Step 6 Click **Next**. The Pending Certificate Request dialog box appears. (See Figure B-15.)

Figure B-15 Pending Certificate Request Dialog Box



Step 7 Verify that the **Process the pending request and install the certificate** radio button is selected. If it is not, select it, and then click **Next**. The Process a Pending Request dialog box appears. (See Figure B-16.)

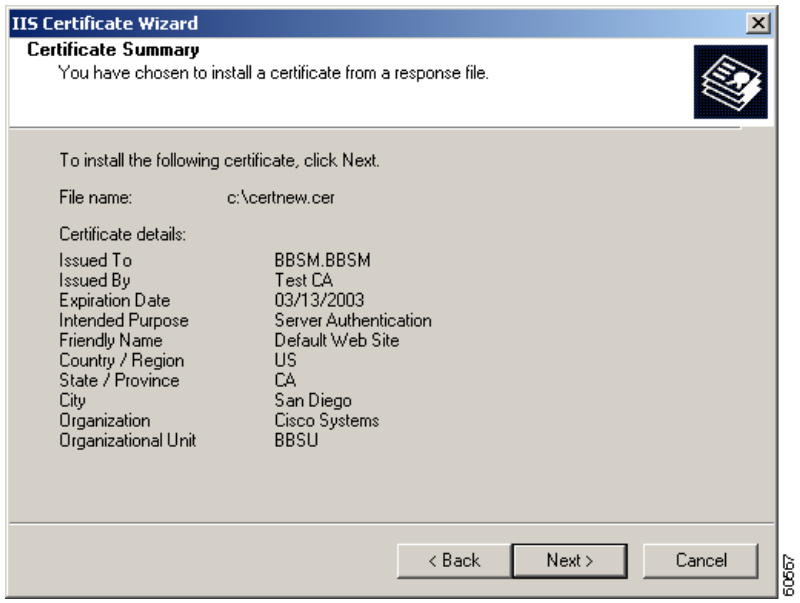
Figure B-16 Process a Pending Request Dialog Box



Step 8 In the Path and file name field, browse to or type the path and file name of the signed certificate that you copied to the BBSM Hotspot server at the beginning of this procedure. Then click **Next**. The Certificate Summary dialog box appears. (See Figure B-17.)

Note You cannot reinstall this certificate on a different machine.

Figure B-17 Certificate Summary Dialog Box



Step 9 Click **Next**. The Completing the Web Server Certificate Wizard dialog box appears, indicating that the installation is complete. (See Figure B-18.)

Figure B-18 Completing the Web Server Certificate Wizard Dialog Box

Step 10 Click **Finish** to close the dialog box. You return to the Default Web Site Properties dialog box.

Step 11 Click **OK** to close the Default Web Site Properties dialog box.

Step 12 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 a Windows-based application that provides a graphical user interface (GUI) and a programming framework in which *consoles*, which are collections of administrative tools, can be created, saved, and opened. The MMC also provides an environment for running management applications and administrative tools called *snap-ins* whose primary purpose is to perform management tasks and to allow administrators and other users with the ability to create custom management tools. These tools can be created for later use, or for sharing with other administrators and users.

Snap-ins can be created in various development environments such as Microsoft Visual Basic 6.0 and Microsoft Visual C++ 5.0 and 6.0. MMC is included in the Windows 2000 operating system and also runs on Windows 95, Windows 98, and Windows NT 4.0 operating systems. The MMC GUI allows snap-ins to integrate with the console, which has no management functionality. Snap-ins always reside in a console. They do not run by themselves. MMC is part of the Microsoft Platform Software Development Kit and is available for general use.

If your BBSM Hotspot server becomes damaged or needs to be rebuilt, you will need to reinstall a backup of your server certificate onto your BBSM Hotspot server. The following procedures explain how to create MMC snap-ins for managing certificates, exporting the certificates (creating a backup), and importing the certificates (reinstalling them) at a later time, if necessary.

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 From the BBSM Hotspot desktop, choose **Start > Run**. The Run window appears.

Step 2 Enter **mmc.exe**, and click **OK**. The Console1 and Console Root windows appear.

Step 3 From the Console1 window, click **Console**.

Step 4 Click **Add/Remove Snap-in**. The Add/Remove Snap-in window appears.

Step 5 Click **Add**. The Add Standalone window appears.

Step 6 Select **Certificates**, and click **Add**. The Certificates snap-in window appears.

Step 7 Click the **Computer account** radio button, and click **Next**. The Select Computer window appears.

Step 8 Verify that the **Local computer** radio button is selected, and click **Finish**. The Add Standalone Snap-in window appears.

Step 9 Click **Close**.

Step 10 From the Add/Remove Snap-in window, click **OK**. The Console1 and Console Root windows appear.

Note You have now added the Certificates snap-in, which will allow you to work with any certificates in your computer's certificate store.

Step 11 Save this MMC for later use.

Continue to the next section.

Exporting a Certificate

Exporting a certificate is the same as creating a backup copy of the server certificate in case you need to reinstall it onto a damaged or rebuilt BBSM Hotspot server at a later time. 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 From the Console Root window, open the Certificates (Local Computer) snap-in that 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, 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**, and click **Next**. This will create a PFX file.

Step 6 Choose a password to protect the PFX file, and click **Next**.

Step 7 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 8 Click **Next**.

Step 9 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 in a secure location.

Importing a Server Certificate in IIS 5.0

The following procedures explain how to reinstall a copy of the server certificate onto a BBSM Hotspot server. To complete this operation, you must have the backup copy of the server certificate, which is contained in the PFX file that you created in the previous procedure.

Caution Do not use the following procedures unless you have to reinstall a backup copy of the server certificate onto a new or rebuilt BBSM Hotspot server at a later time.

Creating MMC Snap-in for Managing Certificates

Use the same procedure that is described in the "Creating MMC Snap-in for Managing Certificates" section on page B-14. After you complete this procedure, continue to the next section.

Importing the Certificate

After you create a new MMC and add the Certificates snap-in, you can import the server certificate into your computer's certificate store by using the following procedure.

Step 1 From the Console Root window, open the Certificates (Local Computer) snap-in, 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 by following this procedure.

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 the contents of your computer's personal certificate store. Select 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 now have an SSL-enabled Web server. Be sure to protect your PFX files from any unwanted personnel.

Changing Server Bandwidth Parameter Settings

This appendix describes how to change the default server bandwidth parameter settings. If you accept the server settings shown in Table C-1, you do not need to make any changes. However, if necessary, you can change these settings by editing the Windows 2000 registry.

Determine the need to change the default bandwidth parameters based on the peak number of users expected on the BBSM Hotspot server, while considering that even if the maximum number of users is exceeded occasionally and performance is impacted, BBSM Hotspot continues to operate correctly.

Note Note that you can only make these changes locally, not from a remote server.

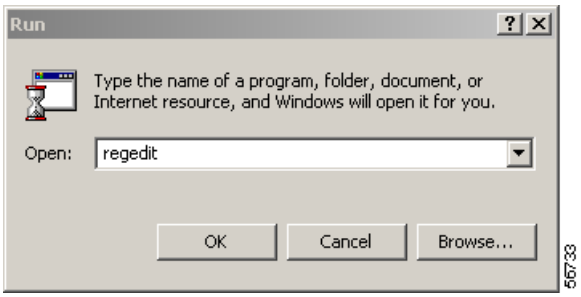
Caution Incorrect registry settings can render your BBSM Hotspot server unusable. Alter only the parameters listed in Table C-1. Always backup the registry before making any changes.

Table C-1 BBSM Hotspot 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. The default is 151,400 bytes.
PacketPoolSize	The number of packet descriptors. The default is 50 descriptors.
LookaheadPoolSize	The number of look-ahead buffer descriptors, which is indicated by the packet descriptor. Set PacketPoolSize and LookaheadPoolSize greater than the anticipated maximum number of packets queued for bandwidth management. The default is 50 descriptors. • For TCP clients, this number is the TCP window divided by the packet size. For example, a typical Windows TCP client uses a window of 8192 bytes, and an Ethernet interface has a maximum packet size of 1514 bytes. Divide the window size (8192 bytes) by the packet size (1514 bytes) to allocate six packets per TCP client. • For UDP clients, this number is the BTWQueueSize divided by the packet size. Calculate both and select the larger of the two values. For example, assume that the BWTQueueSize is 15140 Kb. Because the Ethernet packet size is 1514 bytes, divide the BWTQueueSize (15140) by 1514 bytes to establish 10 packets per client. Because 10 is greater than 6, 10 packets per client would be used.

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

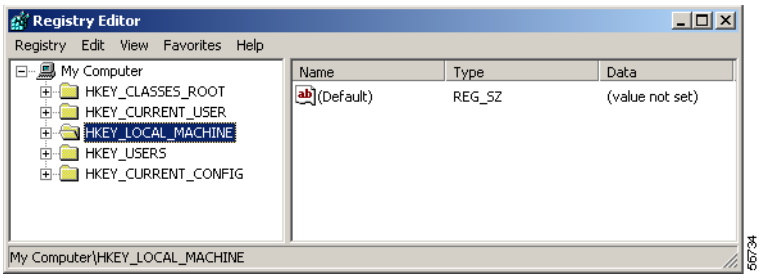
Figure C-1 Run Window



Step 2 Enter **regedit**.

Step 3 Click **OK**. The Registry Editor window appears. (See Figure C-2.)

Figure C-2 Registry Editor Window



Step 4 Double-click **HKEY_LOCAL_MACHINE**.

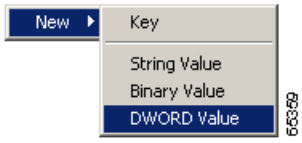
Step 5 Navigate to **System > CurrentControlSet > Services > ATNAT > Parameters.**

Step 6 Right-click anywhere in the right pane of the Registry Editor window.

Step 7 To back up the file before making any changes, choose **Registry > Export Registry File** and follow the instructions.

Step 8 From the New > drop-down menu, select **DWORD Value**. (See Figure C-3.)

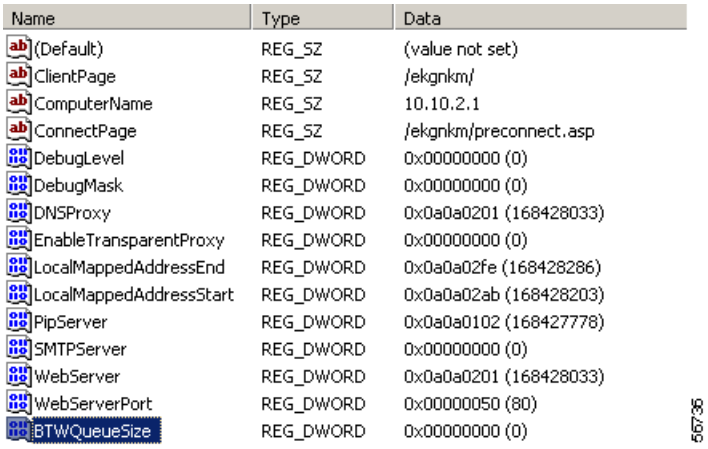
Figure C-3 Registry Editor New Drop-Down Menu



Step 9 Rename the entry to the parameter name you want to change. For applicable parameter names, see Table C-1 on page C-2.

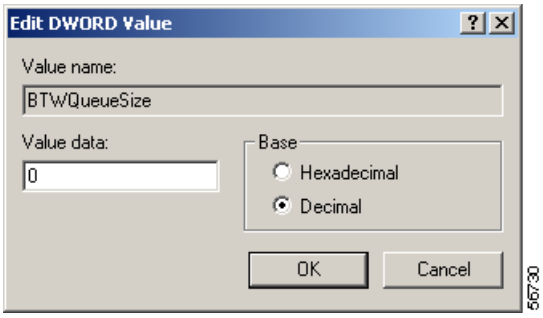
Step 10 Double-click the new parameter name. (See Figure C-4. Note that BTWQueueSize is shown here only as an example.)

Figure C-4 New Parameter Name



The **Edit DWORD Value** dialog box appears. (See Figure C-5.)

Figure C-5 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 C-1 on page C-2 for a list of parameters.

Step 13 Click **OK.**

Step 14 If you want to add another parameter, repeat Steps 6 through 13 for each new parameter.

Step 15 If you want to change other parameters, repeat Steps 10 through 13 for each parameter.

Step 16 When done, close the Registry Editor window.

Step 17 For the new changes to take effect, reboot the server.

A

access code A five-digit number that the BBSM Hotspot software generates for access to the Internet.

access point *See AP.*

access policy An access policy defines how an end user gains access to the Internet through BBSM Hotspot. For example, the end user can access the Internet by the day, the minute, or a block of time.

accounting policy An accounting policy authorizes and posts charges for access to the Internet. An accounting policy is the BBSM Hotspot logic that controls how the end user is charged for Internet access.

activate (session) Activating a session is the process by which BBSM Hotspot grants Internet access to an authenticated end user.

Active Server Page *See ASP.*

Administrator A user who has authentication rights on the BBSM Hotspot server as an Administrator.

AP access point. An AP is a wireless network device that provides physical layer access to a mobile node.

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 Hotspot configuration and logging data.

2. The BBSM Hotspot SQL server database that contains BBSM Hotspot configuration and logging data.

authentication The process by which BBSM Hotspot 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 Hotspot 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

BBSM Hotspot (Cisco) Building Broadband Service Manager Hotspot. BBSM Hotspot 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 A bridged network is a network in which all devices are in the same broadcast domain.

C

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 Hotspot. *See end user.*

client search The process used to search network devices in a BBSM Hotspot network to locate the cluster, switch, and port to which a client is physically connected.

cluster A group of network devices that function as a single device.

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.

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.

CPE customer premise equipment.

CSR certificate signing request.

customer An individual or organization who purchased BBSM Hotspot.

D

dashboard A central location for similar features or links related to a specific feature or feature set. The BBSM Hotspot Dashboard is the BBSM Hotspot-hosted web page that contains links to all BBSM Hotspot management and reporting web applications.

deactivate (session) Deactivating a session is the process by which BBSM Hotspot denies access to the Internet to a formerly authorized end user.

default gateway The IP address configured on the router that is used as the interface for the BBSM Hotspot network to the Internet. This IP address is routable.

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 Hotspot network, the BBSM Hotspot server is a DHCP server, and a guest computer may be a DHCP client.

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.

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

e-mail relay server Email relay servers are used by your ISP to forward non-web based e-mail, such as Microsoft Outlook or Eudora e-mail programs, from public locations. An example FQDN is www.ispemail.com. Typical e-mail servers block traffic from unknown sources for security purposes. Our server, as with any public location, is considered an unknown source that requires an e-mail relay server to forward end-user mail.

end user A user who uses a hardware device, such as a laptop, PDA, or web-enabled cell phone, to access the Internet through the BBSM Hotspot server. The term is used interchangeably with user. *See user.*

external network BBSM Hotspot acts as a router connecting two networks: the external network and the internal network. The external network is “closer” to the Internet and contains the external NIC on the BBSM Hotspot server and the default gateway on the router. BBSM Hotspot does not allow an end user to transmit packets to the external network until the end user has an active session.

F

forced redirect A forced redirect occurs when an end user attempts to view one URL, and BBSM Hotspot forces the user to a different URL. BBSM Hotspot performs a forced redirect when it detects an unauthenticated client.

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 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.

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 Hotspot Access Policy ActiveX server components run.

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 devices, end-user clients, and the BBSM Hotspot internal NIC.

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.

IRB integrated routed and bridged. An IRB network includes a bridged network and one or more routed networks.

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.

ISP Internet service provider.

J

JavaScript An interpreted client-side programming script language that is used in HTML programs and ASP files.

JScript An interpreted server-side programming script language that is used in HTML programs and ASP files.

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 Hotspot administrator to generate a certificate request and install a signed certificate.

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 Hotspot uses the MAC address to identify the location (or port) of a client. Once BBSM Hotspot knows the port that a client is using, BBSM Hotspot applies the per-port policy to the client's session.

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.

MHU multiple hospitality unit.

MIB management information base.

mixed network BBSM Hotspot 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 Hotspot 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 Hotspot system. BBSM Hotspot supports access policy modules, accounting policy 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

NAS network access server. NAS is a RADIUS term that denotes a RADIUS client that is trying to access a RADIUS server. BBSM Hotspot acts as a RADIUS client, or an NAS, when authenticating users that are using a RADIUS page set.

NAT network address translation. NAT is an Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. It is used to translate nonroutable, private network IP addresses to routable, public IP addresses that can be used on the Internet. The router performs the translation of private to public IP addresses in a BBSM Hotspot network.

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 Hotspot server. The network is configured with routers, switches, and other network hardware. BBSM Hotspot 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 device A device connected to the internal network, such as access points (APs) and switches. An end user connects his or her computer to the network device, then BBSM Hotspot queries the device to determine the end user's location.

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

outage The duration that the client cannot fully use the BBSM Hotspot server. The outage can be caused either by an AtDial service restart or by a server reboot. *See service restart* and *server reboot*.

P

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.

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.

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 an Aironet access point, the port is a virtual jack. BBSM Hotspot 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 device 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.

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.

private IP address An Internet Protocol address that is available for us on any network; however, it is not routable on the Internet. Private IP addresses are used extensively in networking due to a shortage of public IP addresses. Network address translation (NAT) is used to connect and route private IP addresses onto the Internet. A private IP address can be referred to as a "fake" or "foreign" IP address.

public IP address An Internet Protocol address that is globally unique and used for addressing over the Internet. This is referred to as a routable IP address.

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 Hotspot server from the external network.

Reports A BBSM Hotspot web application used to display BBSM Hotspot configuration and logged data.

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 Hotspot 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.

routable IP address *See public IP address.*

router A router is used to direct and route traffic (data) to and from the BBSM Hotspot network and the Internet.

S

SDK software developer's kit. An SDK is a set of routines and utilities used to help programmers write an application.

server reboot In the BBSM Hotspot system, the situation in which the BBSM Hotspot 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 Hotspot server is shut down, clients lose access to the Internet and BBSM Hotspot services, and active sessions are disrupted. End users are not able to connect to the BBSM Hotspot 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 Hotspot 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 Hotspot system, a set of interactions between an end user and BBSM Hotspot. The session starts when BBSM Hotspot 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 Hotspot 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.

SMTP Simple Mail Transfer Protocol. SMTP is a TCP/IP protocol used for sending e-mail messages over the Internet.

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 Hotspot 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.

switch A switch is a network device that selects a path for sending a packet of data to its next destination.

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.

TFTP Trivial File Transfer Protocol. TFTP is a simple form of File Transfer Protocol (FTP) that uses the User Datagram Protocol (UDP) and provides no security features.

testing session A set of interactions that a remote user has with a Remote Page Set Test feature on a BBSM Hotspot 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.

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 *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 Hotspot clients. It allows BBSM Hotspot 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 Hotspot that allows remote updates to the BBSM Hotspot server.

web page 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. These web pages control Internet access.

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

R

S

T

U

V

W