CONTENTS

Preface vii

Conventions viii

Related Publications ix

Obtaining Documentation ix

Cisco.com ix

Ordering Documentation ix

Documentation Feedback ix

Obtaining Technical Assistance x

Cisco Technical Support Website x

Submitting a Service Request x

Definitions of Service Request Severity xi

Obtaining Additional Publications and Information xi

CHAPTER 1

Overview 1-1

New in Software Release 5.3 1-2

Transmission and Networking Options 1-3

Understanding the BBSM Dashboard 1-6

Dashboard 1-7

Administration 1-8

Operations 1-11

Reports 1-11

Using Navigation Buttons 1-12

Connecting a Client to BBSM 1-12

CHAPTER 2

Advanced Topics 2-1

VLANs 2-1

What is a VLAN? 2-1

Incorporating Wireless Devices into VLANs 2-3

VLANs and BBSM 2-4

VPN 2-5

BBSM is VPN Neutral 2-5

Public-Private Addressing with VPN 2-5
### Adding and Configuring CMTSs
- 12-7

### Configuring Switches
- 12-13

### Configuring PMS or Print Billing
- **Overview** 13-1
- **Two-Way PMS Interface** 13-2
- **Supported PMS Protocols** 13-2
- **Configuring PMS or Print Billing** 13-4
- **Configuring PMS Call Types** 13-6
- **Configuring a Laptop for Mapping Rooms** 13-7
  - **Configuring the Laptop** 13-7
  - **Configuring Windows** 13-8
  - **Configuring the Browser** 13-9
- **Mapping Rooms** 13-9
  - **Basic Room Mapping** 13-10
  - **Dynamic Port-Room Configuration for CMTSs** 13-13

### Configuring RADIUS Billing
- **Overview** 14-1
  - **RADIUS Authentication and Authorization** 14-1
  - **RADIUS Accounting** 14-2
  - **User-Provisioned Bandwidth** 14-2
  - **Using Prepaid RADIUS** 14-2
  - **RADIUS Attributes** 14-4
- **Configuring the RADIUS Server Options** 14-6
- **Configuring RADIUS for Multiple Sessions** 14-9

### Configuring Credit Card Billing
- **Configuring the Credit Card Server Options** 15-2
- **Entering the Merchant ID** 15-3
- **Testing the Credit Card Interface** 15-4

### Configuring Security and SSL
- **Security Overview** 16-1
- **Installing an SSL Certificate** 16-2
  - **Before You Start** 16-3
  - **Generating a Certificate Signing Request** 16-3
Preface

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

The term customer refers to the BBSM purchaser, including individuals or organizations. The term end user refers to the customer of the service provider or property owner and the end user who accesses the Internet through the BBSM system.

This guide is organized into the following chapters and appendixes:

- **Chapter 1, “Overview,”** provides an overview of the BBSM system, including media and deployment options, network interfaces, and system features.
- **Chapter 2, “Advanced Topics,”** provides detailed discussions of topics pertinent to the BBSM system, such as VLANs and VPN client.
- **Chapter 3, “Getting Started,”** describes the initial steps to setting up the BBSM server.
- **Chapter 4, “Configuring Dual VLANs,”** describes how to configure two VLANs.
- **Chapter 5, “Running the BBSM Wizards,”** describes how to use the Address Change Wizard to configure BBSM IP addresses and the Switch Discovery Wizard to discover the access points and switches on your network.
- **Chapter 6, “Configuring DNS Forwarding,”** provides the procedure for configuring DNS forwarding after running the Address Change and the Switch Discovery wizards during the initial setup.
- **Chapter 7, “Connecting the PMS or Local Printer,”** provides the procedure to connect a PMS or local printer using serial or IP connections. Use the procedure only when you are using PMS billing or local print billing.
- **Chapter 8, “Configuring the Network and Bandwidth Management Settings,”** describes how to configure the basic network and bandwidth management settings in WEBconfig. (You must complete the procedures in Chapter 3, “Getting Started,” before beginning the initial system configuration.)
- **Chapter 9, “Changing the Internal Network IP Address Ranges,”** describes the BBSM IP address ranges that you need to configure and an overview of public and private IP addresses (multinets). Provides the procedure to configure the IP addresses in WEBconfig.
- **Chapter 10, “Configuring BBSM Sites,”** describes how to configure sites in WEBconfig. You can add sites, change site information, and delete sites and their related clusters using this web page.
Conventions

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

- Commands and data that you type are shown in bold.
- Variables or parameters for which you supply values are shown in angle brackets (< >). The > angle bracket is also used to indicate cascading menu choices, such as Billing > RADIUS > Site x.
- Terminal sessions and screen displays are shown in screen font.
- Optional elements are shown in square brackets ([ ]).
Related Publications

These documents provide complete information about BBSM:

- *Cisco BBSM 5.3 Operations Guide* (order number DOC-7816161=)
- *Cisco BBSM 5.3 Software Installation Guide* (order number DOC-7815714=)
- *Cisco BBSM 5.3 SDK Developer Guide* (available on Cisco.com)

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

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:


Ordering Documentation

You can find instructions for ordering documentation at this URL:


You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.
You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:
Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883
We appreciate your comments.

**Obtaining Technical Assistance**

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

**Cisco Technical Support Website**

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:


**Submitting a Service Request**

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553 2447
For a complete list of Cisco TAC contacts, go to this URL:
http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
  http://www.cisco.com/go/marketplace/

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
  http://cisco.com/univercd/cc/td/doc/pcat/

- Cisco Press publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
  http://www.ciscopress.com

- Packet magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
  http://www.cisco.com/packet
• *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
  http://www.cisco.com/go/iqmagazine

• *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
  http://www.cisco.com/ipj

• World-class networking training is available from Cisco. You can view current offerings at this URL:
Overview

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

This chapter includes these sections:

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

The BBSM server integrates and manages these key functions:

- Connection—Enables you to provide Internet access to end users regardless of the client’s network interface configurations. Network deployment options include Ethernet, long-reach Ethernet (LRE), wireless, and cable.
- Authentication—Supports multiple authentication methods, such as port-based authentication, RADIUS, and access codes.
- Accounting—Supports accounting and payment methods including credit cards, RADIUS, and the property management system (PMS). The PMS and credit card billing can also allow impulse charges for additional bandwidth or future value-added services.
- Portal—Includes a forced portal, walled garden free access, and Connect (start) pages that you can customize.
- Bandwidth options—Supports options such as bandwidth throttling and bandwidth reservation.
- Network deployment and configuration—Includes multiple features to support network installation, configuration, and testing.
- SDK—A comprehensive software developer’s kit (SDK) can help you develop custom access or accounting policies or a PMS module for a new PMS interface.
BBSM is available as a preloaded server appliance, or you can purchase the software separately and install it yourself. If you are installing the BBSM software, refer to the Cisco BBSM 5.3 Installation Guide for instructions on installing BBSM and for the minimum hardware and software requirements. For information on obtaining the installation guide and other documentation, refer to the “Obtaining Documentation” section in the preface to this user guide.

New in Software Release 5.3

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

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

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

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

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

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

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

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

**Security hardening**
As of BBSM 5.3, the BBSM appliances ship with security hardening. Hardening BBSM involves disabling unnecessary services, removing and modifying registry key entries, and applying appropriate restrictive permissions to files and services to prevent exploitation. In addition to the BBSM server being...
hardened, other devices on the network should also configured to ensure proper security. Examples include filtering on firewalls, access control lists, and intrusion detection systems. A BBSM white paper describes the procedure for hardening a BBSM server:


Transmission and Networking Options

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

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

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

Figure 1-1  Typical BBSM Building Network

![Diagram of BBSM Network](image-url)
The BBSM system supports the following types of networks:

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

![Figure 1-2 Basic Bridged BBSM Network](image)

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

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

Central location

Internet

External router

BBSM server (router = 0)

Base switch

POP router (router = A)

Remote property = Site 1

POP router (router = 1)

Switch

Switch

Client

Client

Remote property = Site 2

POP router (router = 2)

Switch

Switch

Client

Client

RADIUS server

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

Figure 1-4 Basic Mixed and Routed BBSM Network

Understanding the BBSM Dashboard

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

- Administrator—Can perform all system functions
- Reports user—Can view reports

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

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

- To access the Dashboard locally, double-click the Dashboard icon on the desktop. The Dashboard appears. (You can also choose Start > BBSM Dashboard to access the Dashboard.)

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

These usernames and passwords are created when a site is created. A site can be created in switch discovery or in WEBconfig during site configuration. (Refer to the “Running the Switch Discovery Wizard” section on page 5-6.)
Figure 1-5  Dashboard for Single Sites

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

Administration

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

- **WEBconfig**—WEBconfig is the primary tool for configuring BBSM. Clicking WEBconfig displays the BBSM Server Settings web page and the navigation bar (NavBar) for selecting all of the web pages used to configure the system. (See Figure 1-6.) To close WEBconfig and return to the Dashboard, click the Dashboard link in the upper right-hand corner of the web page.

- **WEB PMS Test**—WEB PMS Test is used to test the physical connection and transfer of data between BBSM and the PMS.

- **WEBpatch**—WEBpatch is used to transfer and install service packs or patches for the BBSM software. With WEBpatch, you can update the BBSM server software remotely and obtain a list of details about the installed BBSM service packs, patches, and upgrades.

- **Page Set Wizard**—The Page Set Wizard enables you to create your own custom DailyHotel page set using a web-based wizard.
Figure 1-6  BBSM WEBconfig Default Web Page and Navigation Bar

Building Broadband Service Manager
WEBconfig

BBSM Software Information
Version: "5.2.1"
Updates: "New"

Network Configuration
Enable Maximum Active Sessions
Maximum Active Sessions: 23
Enable Transparent Proxy
Enable Duplicate IP Addresses
(Requires local DHCP Server to be enabled)
SMTP Forwarding Server
Currency Type

Bandwidth Management
Enable Bandwidth Throttle
Access Code Bandwidth

BBSM Server Settings
IP Addresses
Sites
Routers
Network Elements
Port Test Settings
Billing
Security/SSL
Bandwidth Reservation
Custom Page Sets
Walled Garden
Port Hopping
WEB Printing
Alerts

Latest Update:
The last update applied to this server.
Note: For a complete list of the Updates applied to the server, see WEBConfig.
Enable Duplicate IP Addresses:
Check the box if you want to allow Static clients with duplicate IP addresses to authenticate. Enabling this feature requires the local DHCP server to be enabled and protected-port configuration on network devices.
SMTP Forwarding Server:
To properly relay e-mail, you must enter the IP address or fully qualified domain name of the SMTP server.
Currency Type:
The selected currency type will be the type used for all transactions on this server. The default is US dollars (USD).
Enable Bandwidth Throttle:
Check the box if you plan to offer users the option to choose a bandwidth when connecting.
Table 1-1 describes the WEBconfig web page options.

**Table 1-1 WEBconfig Web Page NavBar Options**

<table>
<thead>
<tr>
<th>Web Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BBSM Server Settings</td>
<td>Configures server-wide settings such as bandwidth management, transparent proxy, and the SMTP forwarding IP address.</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>Configures the IP address ranges for the BBSM server and the network equipment.</td>
</tr>
<tr>
<td>Sites</td>
<td>Manages site data and locations.</td>
</tr>
<tr>
<td>Routers</td>
<td>Sets router interface parameters. Enables you to configure routes to the switches and to the client computers attached to these switches. (This feature is for routed networks and is not related to WAN activities.)</td>
</tr>
<tr>
<td>Network Elements</td>
<td>Expands to the Access Points, CMTS (cable modem termination system), and Switches web pages for each site:</td>
</tr>
<tr>
<td></td>
<td>• Access Points—For a particular site, sets access point parameters, such as the access point IP address and type.</td>
</tr>
<tr>
<td></td>
<td>• CMTS—For a specific site and CMTS, sets the CMTS mode, parameters, and cable modem IP address ranges and DHCP options.</td>
</tr>
<tr>
<td></td>
<td>• Switches—For a particular site, cluster, and switch number, sets the switch parameters, such as number of client ports, cluster IP address, router IP address, and Cisco switch type. Each site can support multiple clusters, and each cluster can support up to 16 cluster-capable switches.</td>
</tr>
<tr>
<td>Port Test Settings</td>
<td>For each site, expands to the Port Test Settings web page, which enables you to select the port test parameters, including switch mode.</td>
</tr>
<tr>
<td>Billing</td>
<td>Expands to the PMS/Print, RADIUS, and Credit Card web pages, which define the billing features for the site:</td>
</tr>
<tr>
<td></td>
<td>• PMS/Print—Expands to enable you to configure the PMS settings and call types.</td>
</tr>
<tr>
<td></td>
<td>• RADIUS—Enables you to configure the RADIUS server parameters and the multiple concurrent RADIUS sessions for each site.</td>
</tr>
<tr>
<td></td>
<td>• Credit Card—Enables you to configure the credit card server parameters and the merchant ID number for each site.</td>
</tr>
<tr>
<td>Security/SSL</td>
<td>Configures the domain name for SSL page sets, changes the MSDE sa password, and changes the BBSD and Web API accounts.</td>
</tr>
<tr>
<td>Bandwidth Reservation</td>
<td>Expands to the External Router, Total Bandwidth, and Classes of Service web pages:</td>
</tr>
<tr>
<td></td>
<td>• External Router—Configures the IP address and the Telnet terminal and IOS enable passwords.</td>
</tr>
<tr>
<td></td>
<td>• Total Bandwidth—Sets the router bandwidth parameters for total property and unreserved users.</td>
</tr>
<tr>
<td></td>
<td>• Classes of Service—For the router, sets the class of service parameters. If you are entering the external router information in WEBconfig remotely, Cisco recommends using SSL to connect to the Dashboard. This will protect the sensitive data that is entered on this page.</td>
</tr>
<tr>
<td>Custom Page Sets</td>
<td>Adds your new custom page sets and sets the associated Start page. The page set then appears in the Page Set drop-down menu when you are configuring port settings from your Network Elements web page.</td>
</tr>
<tr>
<td>Walled Garden</td>
<td>Enables you to configure walled garden web sites, which let the end user view the web sites that you specify as free of charge.</td>
</tr>
</tbody>
</table>
Chapter 1      Overview

Understanding the BBSM Dashboard

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

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

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

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

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

<table>
<thead>
<tr>
<th>Web Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Hopping</td>
<td>Configures the port hop delay.</td>
</tr>
<tr>
<td>Alerts</td>
<td>Enables or disables SNMP alerts. When alerts are enabled, you can enter parameters such as what level of alerts to send and where to send them.</td>
</tr>
</tbody>
</table>

**Operations**

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

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

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

**Reports**
Using Navigation Buttons

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

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

Table 1-2 Navigation Button Descriptions

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;&lt;</td>
<td>Returns the user to the first record or page.</td>
</tr>
<tr>
<td>&lt;</td>
<td>Returns the user to the previous record or page.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Takes the user to the next record or page.</td>
</tr>
<tr>
<td>&gt;&gt;&gt;</td>
<td>Takes the user to the last record or page.</td>
</tr>
</tbody>
</table>

Connecting a Client to BBSM

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

Table 1-3 Minimum End-User Client Connection Requirements

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

The page set that the BBSM administrator selects in the Switch Discovery Wizard or from the Page Set drop-down menu in the WEBconfig Network Element Port Settings pop-up window determines which Connect page the end user uses to connect to the Internet.
The following example demonstrates a general connection sequence for an end user.
A hotel has purchased a BBSM server, set it up, and selected the DailyHotel page set. After checking into a hotel room, an end user with a laptop computer might do the following:

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

The following sections provide detailed information about topics that pertain to the BBSM system:

- **VLANs**, page 2-1
- **VPN**, page 2-5
- **Web Proxies**, page 2-7
- **Web Servers**, page 2-8

Many features are described in detail in the overview of the configuration chapters. For example, the RADIUS overview and attributes are presented in Chapter 14, “Configuring RADIUS Billing.”

**VLANs**

As of BBSM 5.3, the BBSM server supports two VLANs on the internal interface. This feature enables you to put the management traffic and equipment on one VLAN and end-user clients on the other VLAN.

**What is a VLAN?**

A switched network can be logically segmented into virtual local area networks (VLANs) by functions, project teams, or applications on a physical or geographical basis. For example, a workgroup team can connect all of their workstations and servers to the same VLAN regardless of their physical network connections or intermingling with devices for other teams. VLANs can be reconfigured through software rather than physically unplugging and moving devices or wires.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. It consists of end systems, either hosts or network equipment such as bridges and routers, connected by one bridging domain. This bridging domain is supported on various network equipment, such as LAN switches that operate bridging protocols between them with a separate group for each VLAN.

VLANs are created to provide the segmentation services that routers traditionally provide in LAN configurations. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic-flow management. None of the network devices within the defined group bridge any frames, not even broadcast frames, between two VLANs.

Several key issues must be considered when designing and building switched LAN networks.

- LAN segmentation
- Security
- Broadcast control
• Performance
• Network management
• Communication between VLANs

VLANs are extended into the wireless realm by adding IEEE 802.1Q tag awareness to the access point. The access point wirelessly transmits frames destined for WLAN clients on different VLANs on different SSIDs with different Wired Equivalent Privacy (WEP) keys. (WEP is an 802.11 security protocol for wireless network WEP keys.) The only clients that can receive and process packets are those with the correct WEP keys. Conversely, packets coming from a client associated with a certain VLAN are 802.1Q tagged before they are forwarded onto the wired network.

Figure 2-1 shows the difference between traditional physical LAN segmentation and logical VLAN segmentation with wireless devices connected.

Figure 2-1  LAN and VLAN Segmentation with Wireless Components
Incorporating Wireless Devices into VLANs

A wireless LAN (WLAN) is generally deployed in an enterprise campus or branch office for increased efficiency and flexibility. WLANs are one of the most effective methods for connecting to an enterprise network. With Cisco IOS Release 12.01T, you can configure your wireless devices to operate in a VLAN.

The basic wireless components of a VLAN consist of an access point and a set of clients associated with it using wireless technology. The access point is connected physically through a trunk port to the network switch on which the VLAN is configured. The physical connection to the VLAN switch is through the Ethernet port of the access point.

In fundamental terms, the key to configuring an access point to connect to a specific VLAN is to configure an SSID to map to that VLAN. Because VLANs are identified by a VLAN ID, if an SSID on an access point is configured to map to a specific VLAN ID, a connection to the VLAN is established, and clients can access the VLAN through the access point. The VLAN processes data to and from the clients the same way that it processes data to and from wired connections. The fact that the client is wireless has no impact on the VLAN.

The VLAN feature enables users to deploy access points with greater efficiency and flexibility. For example, one access point can handle the specific requirements of multiple users having widely varied network access options and permissions. Without VLAN capability, multiple access points (one for each VLAN) would have to be used to serve user classes based on the access options and permissions that they were assigned.

The following simplified example shows how access points can be used effectively in a VLAN environment on a college campus. In this example, three levels of access are available through VLANs configured on the physical network:

- Student access—Lowest level of access; ability to access school’s intranet, obtain class schedules and grades, make appointments, and perform other student-related activities
- Faculty access—Medium level of access; ability to access internal files, read to and write from student databases, access the intranet and Internet, and access internal information such as human resources and payroll information
- Management access—Highest level of access; ability to access all internal drives and files, and perform management activities

In this scenario, a minimum of three VLANs are required—one for each of the above access levels. Because the access point can handle up to 16 service set identifiers (SSIDs), the following basic design can be used. (See Table 2-1.)

<table>
<thead>
<tr>
<th>Access Level</th>
<th>SSID</th>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student</td>
<td>Student</td>
<td>01</td>
</tr>
<tr>
<td>Faculty</td>
<td>Faculty</td>
<td>02</td>
</tr>
<tr>
<td>Management</td>
<td>Management</td>
<td>03</td>
</tr>
</tbody>
</table>

Using this design, setting up the clients is based on the access level that each user requires. Figure 2-2 shows a typical network diagram using this design.
VLANs and BBSM

With BBSM, you can choose any VLAN IDs, such as VLAN 1 for the management VLAN and VLAN 100 for the client VLAN. The VLANs on most equipment defaults to VLAN1. Cisco recommends that you change these defaults for security reasons.

Configure the network device port that BBSM is connected to as a trunk port to allow packets from both VLANs to reach the BBSM server. In a daisy-chained network topology, the network device must have at least two ports—one for upstream and one for downstream. The trunk port transmits packets that are tagged with the VLAN number to the BBSM server.

Caution: In a multi-VLAN configuration, VLANs associated with the trunk port should not be native. The reason is that packets on a native VLAN are sent untagged to the BBSM server, and BBSM rejects them (when the internal NIC is enabled for the IEEE 802.1Q, which specifies formatting for dual VLANs).

If you want to use non-default VLANs for the management and client VLANs, you must change the VLAN number. The network device's SNMP password configured in WEBconfig has to be appended with @<management VLAN #> for the management VLAN or @<client VLAN #> for the client VLAN, which enables BBSM to discover ports in the VLAN, as in this example:

If the device's SNMP read-write community string is private and its management VLAN # is 100, change the BBSM SNMP password for the network device to private@100.
Or, you can use Switch Discovery Wizard to specify the management and client VLANs when adding switches or access points to BBSM. (CMTSs must be configured using WEBconfig.) Refer to the following documentation about VLANs:

- Chapter 4, “Configuring Dual VLANs”
- “Running the Switch Discovery Wizard”

**Note**
Access points are not automatically configured with a default VLAN. If you add or remove a default VLAN from an access point, you must reconfigure your port settings using WEBconfig. Refer to the “Configuring Access Points” section on page 12-2.

**VPN**

One advantage of the public and private IP addressing feature is that it eliminates the IP Security (IPSec) VPN problems that occur with the use of private IP addressing. All VPN clients are supported. For an overview of public and private addressing, refer to the “Public and Private IP Addresses (Multinets)” section on page 9-2.

If the VPN client requires routable addresses, the end user can choose this option from the Connect page. The client has to be configured for DHCP. If the VPN client can work with network address translation (NAT), BBSM can use either routable or nonroutable addresses and the client can be DHCP or static. Cisco VPN 3000 works with NAT.

**Note**
When you finish the session, close the VPN client before disconnecting.

**BBSM is VPN Neutral**

Technically, BBSM does not support or reject VPN clients. The topology of the in-building network is the parameter than affects the use of VPN clients:

- If the in-building network is deployed with all public IP addresses, the router does not need to perform any NAT or port address translation (PAT) and no problems occur when VPN is used. However, this situation would be unusual and expensive if the operator did not already have a large block of IP addresses.
- More often, the in-building network is configured with private IP addresses, which causes the router to perform PAT to connect various sessions to the Internet. This router PAT activity interferes with certain types of non-Cisco VPN clients. Cisco routers that have the Cisco IOS Release 12.1.4T or later firmware patch installed also support Microsoft PPTP VPNs regardless of PAT activity.

You may experience problems if you use another VPN vendor’s product that uses IPSec with authentication headers (AHs). Although BBSM may support these VPN products, they have not been tested with BBSM.

**Public-Private Addressing with VPN**

Public-private IP addressing eliminates the following problems that relate to VPN:

- NAT after IPSec
Applying NAT after IPSec encryption to hide IP addresses provides no benefit because the actual IP addresses of the transport devices are hidden by the encryption. Only the public IP addresses of the IPSec peers are visible, and hiding the public IP addresses provides no additional security. NAT is applied after IPSec encapsulation when IP addresses are being conserved. This conservation application is common in hotels, cable or DSL residential deployments, and enterprise networks. In these cases, using NAT after IPSec encryption can interfere with establishing the IPSec tunnel (depending on the type of NAT).

When IPSec uses the authentication header (AH) mode for signature integrity, one-to-one NAT can invalidate the signature checksum. Because the signature checksum is partially derived from the AH packet’s IP header contents, the signature checksum becomes invalid when the IP header changes. The packet then appears to have been modified in transit and is discarded when the remote peer receives it.

However, when IPSec incorporates the encapsulating security payload (ESP), devices can send packets successfully over the VPN, even with one-to-one NAT after encapsulation. This scenario is possible because ESP does not use the IP header contents to validate packet integrity. In cases in which many-to-one NAT occurs (also known as PAT), the IP address and the source Internet Key Exchange (IKE) port (normally User Datagram Protocol [UDP] port 500) changes. Some VPN devices do not support IKE requests sourced on ports other than UDP 500, and some devices performing many-to-one NAT do not handle ESP or AH correctly. Remember that ESP and AH are higher layer protocols than IP and do not use ports.

Because many-to-one NAT is common in environments that include remote access clients, a special mechanism called NAT transparency is used to overcome these NAT problems. NAT transparency re-encapsulates the IKE and ESP packets into another transport layer protocol, such as UDP or TCP, that address-translating devices can translate correctly. This mechanism also allows the client to bypass access control in the network that allows TCP or UDP but blocks encrypted traffic. This feature does not affect transport security in any way. NAT transparency takes packets that IPSec has already secured and encapsulates them again in TCP or UDP.

The Internet Engineering Task Force (IETF) IPSec working group has not endorsed IPSec over UDP. Although the problems of using IPSec through a device performing many-to-one translations are discussed frequently, no standard approach to solving these problems exists at this time. Therefore, Cisco is implementing support for IPSec over UDP as a short-term solution until a standards-based workaround is available. As a result, IPSec over UDP is compatible only with the Cisco VPN 3000 clients and concentrators.

- Using Cisco VPN 3000 Concentrators and the Cisco VPN 3000 Client with IPSec over UDP
  No user intervention is required to perform IPSec over UDP with Cisco VPN 3000 concentrators. An administrator can centrally control when a user should use IPSec or IPSec over UDP through a group-user configuration policy within the Cisco VPN 3000 series concentrator product. If IPSec over UDP is enabled for a particular user, the client and the Cisco VPN 3000 concentrator automatically negotiate using IKE. The setup includes basic information such as the UDP port number and the IPSec-over-UDP requirement. Data will be transmitted successfully through NAT.

- IPSec over UDP through a NAT firewall performing filtering
  Although any device that can perform outgoing NAT on UDP packets allows IPSec or UDP to be used, the network administrator needs to ensure that no specific rules exist that block access to the UDP port that the remote network’s administrator defines. If the administrator is not blocking the packets, the user can successfully access the remote network in a secure manner.

- NAT before IPSec
  When two sites are connected through IPSec, the tunnel does not establish whether or not any of the site network address ranges overlap because the VPN termination devices cannot determine the site to forward the packets to. Using NAT before IPSec overcomes this restriction by translating one set
of the overlapping networks into a unique network address range that does not interfere with establishing the IPSec tunnel. The NAT application is recommended only in this scenario. However, some protocols embed IP addresses in packet data segments. As a general practice, verify that a protocol-aware device carries out the NAT when addresses are translated, not only in the IP header but also in the packet’s data segment.

If the packet address was not correctly translated because of embedded addresses before being transmitted, the remote application does not receive the correct IP address embedded in the data segment when it receives the packet and probably does not function properly. Many remote access VPN clients now support a virtual address that the VPN concentrator assigns. Devices at the remote site can connect to the remote access client using this virtual address by one-to-one addressing that translates all transmitted and received packets. If the VPN client does not address-translate packets correctly or if a new application arrives that is not yet supported, the application may not function.

In summary, follow these guidelines:

- Use address ranges at your sites and remote access VPN client virtual address pools that do not overlap with the addresses of other devices that you connect through IPSec. If this is not possible, use NAT in this scenario to allow only for connectivity. (This option is not configured on the BBSM server.)

- Do not hide the public IP addresses of the VPN devices because hiding them does not add security and can cause connectivity problems.

- When you believe that NAT is involved and a remote access client cannot establish a tunnel successfully or send packets over an established tunnel, consider enabling the NAT transparency mode. Do not try to use the NAT transparency mode to resolve connection problems associated with client applications that are not NAT friendly. (The NAT transparency mode option is not configured on the BBSM server. It is not related to the BBSM transparent proxy feature.)

Web Proxies

BBSM can function as a web proxy server in several different ways:

- As shipped, BBSM works as a proxy server for end users whose browsers are configured for a web proxy server. (BBSM uses Microsoft Industry Standard Architecture [ISA] for this function.) In other words, BBSM selectively proxies only the users that require it (those with proxy settings).

- BBSM also has a transparent proxy feature that can be enabled:
  - Enabling transparent proxy forces all users, regardless of browser settings, through the BBSM proxy engine. Refer to Chapter 9, “Changing the Internal Network IP Address Ranges.”
  - If your router is configured properly, transparent proxy does not need to be enabled for BBSM to operate correctly. Problems occur when the client is using a private IP address and the router is not configured with a static route to the BBSM internal network. In this case, the router cannot route packets to the client and the client cannot browse the Internet.
  - With web proxy enabled globally, you can use Microsoft ISA to monitor the Internet sites that the web browser has visited. (You must turn on ISA logging manually.) The resulting data appears in the ISA log files. This feature is used to gather statistics for marketing purposes and is not recommended for most deployments because using it affects performance.
Refer to Chapter 9, “Changing the Internal Network IP Address Ranges,” to enable transparent proxy in WEBconfig and log subsequent entries.

**Note**

BBSM has no provision for directing client traffic through a remote proxy server. BBSM supports use of the proxy server only on the BBSM server. However, you can use a Cisco router between BBSM and the Internet to intercept packets using the Web Cache Communication Protocol (WCCP) and then send the requests to a content engine. The content engine can be configured to use the proxy for outbound data. (Cisco IOS supports both versions of WCCP.)

**Caution**

Do not modify the ISA settings to ensure that the BBSM server supports web proxy.

**Web Servers**

A web server can be hosted on a client machine inside the BBSM network. Although this situation is not common, you can accomplish it by using the following information. Hosting a web server on an internal BBSM network client allows unrestricted access from the external side.

Check the Transparent Proxy check box in WEBconfig and do the following:

- To keep the billing intact, reserve a DHCP address for the client and then set up one-to-one static mapping to that address (if you are using private addresses). (The client is still required to connect to BBSM.) After the client session is enabled, the client can host a web server. The client should not run services such as DHCP and DNS to avoid conflicts with these services running on BBSM.

- You can configure the web server with a BBSM management range IP address if these addresses are not needed for billing. Perform one-to-one NAT of the address in the router (if you are using private addresses). Internet access to the web server is then available.
Getting Started

This chapter describes the information and procedures that you need to configure your BBSM server:

- **Before You Start, page 3-1**
- **Setting Up the BBSM Server, page 3-2**

Be sure to read the “Before You Start” section before continuing.

Before You Start

Before you begin configuring BBSM, complete the following tasks:

1. Read the ReadMeFirst web page that launches when you start your BBSM server.
2. Read the applicable sections in the configuration guide and the cautions below to avoid costly problems.
3. From your BBSM server desktop, open the BBSM Checklist and complete it to ensure that you have all of the networking information that you need to configure your server. This includes configuration information for your network topology and information for the routers, clusters, and network devices (access points, CMTSs, and switches) that you will use with the server.
4. If you are using secured (https) pages, obtain and install a Certificate Authority (third-party SSL). Refer to the “Installing an SSL Certificate” section on page 16-2.

Read the cautions below before proceeding.

**Caution**

Do not change the Windows 2000 computer name of your factory-installed BBSM appliance because the BBSM MSDE database has the name embedded in the application. Changing the name breaks MSDE functionality, and SQL server errors will be reported on your BBSM server. The only solution in this situation is to reformat the hard drive and reinstall all software so that the MSDE database is reinstalled. Because this situation is a Microsoft problem, the Cisco software team cannot resolve it. If you want a different computer name for your BBSM server, you must install the software on a clean Windows 2000 server that already has the correct computer name configured.
Caution
We do not recommend changing any of the Windows 2000 server component settings on your
BBSM server, because changing the operating system can cause problems and leave your server in
an unsupported state. These components include, but are not limited to, the DHCP Server,
Microsoft ISA, DNS Server, IIS Server, RRAS, and Local Security Policy. If you must modify
component settings, test your server in a lab environment before going to production.

Caution
Cisco recommends using the latest version of Internet Explorer to perform functions accessed through
the BBSM Dashboard.

Caution
If you change the system clock on the server while clients are connected, you must reboot the BBSM
server.

Caution
To avoid disrupting end-user sessions, make changes only when no sessions are active because all
active services stop when you save changes on the Webconfig web pages. Services restart
automatically after the settings are updated.

Setting Up the BBSM Server

This section explains how to set up the BBSM server:

- Entering Security Passwords, page 3-2
- Installing Service Packs or Patches, page 3-4
- Configuring Windows for Public and Private IP Addressing, page 3-4

Entering Security Passwords

If you purchased a BBSM appliance (rather than BBSM software on CD), you are prompted to enter the
following information in the Set BBSM Security Passwords window (Figure 3-1) when you turn on the
BBSM server for the first time:

- Windows Administrator username and password
- MSDE System Administrator sa account password

Note
The MSDE System Administrator sa login username cannot be changed or removed.
If you are installing the BBSM software from a CD, the Windows Administrator password is entered during the operating system installation and the MSDE System Administrator sa password is entered during BBSM installation.

If you want to change the MSDE System Administrator sa password or change the BBSD or Web API account usernames or passwords, refer to Chapter 16, “Configuring Security and SSL.”

Do not change any other account information, including system generated accounts such as TsInternetUser and accounts prefaced with IWAM_ and IUSR_. If you change them, BBSM may not function properly. In addition, restoring these accounts to their previous states can be very difficult.

When the Set BBSM Security Passwords window appears, you must enter the required username and passwords. To ensure that passwords are entered, the set passwords window does not contain a Close button and clicking the escape key does not close the window. In addition, if any other applications are opened while the set passwords window is displayed, they will appear in the background and the Set Passwords window will appear in the foreground.
Follow this procedure to set the Windows Administrator username and password and the MSDE System Administrator sa password.

**Step 1** Turn on the BBSM server for the first time. The Set BBSM Security Passwords window appears.

**Step 2** Enter the Windows Administrator username and password.

Passwords must be between 6 and 15 characters long, blank passwords are not permitted, and passwords are case sensitive. The two password fields must be identical for each account.

**Step 3** Enter the MSDE System Administrator sa account password twice and then click **OK**. The SetPasswords configuration dialog box appears.

**Step 4** Click **OK** to confirm the passwords.

### Installing Service Packs or Patches

Before beginning the basic configuration of your BBSM server, determine if any service packs or patches need to be installed. Cisco recommends that you install all available service packs and patches. For instructions on performing these installations, refer to the *Cisco BBSM 5.3 Operations Guide*.

### Configuring Windows for Public and Private IP Addressing

This section describes how to reconfigure Windows to support public and private IP addressing, which requires configuring multiple networks called *multinets*. It reconfigures the internal network interface card (NIC) on your BBSM server. You need to perform this procedure only if you will be using multiple networks. Factory-installed BBSM servers are initially configured as single networks called *singlenets*.

**Note**

For more information, refer to the “Public and Private IP Addresses (Multinets)” section on page 9-2.

**Caution**

Although you use the Network and Dial-up Connections window to add multinets, do not delete multinets through this window. Instead, use the Address Change Wizard to remove multinet 2 so BBSM can update its internal database with this information. Refer to the “Running the Address Change Wizard” section on page 5-1.

**Step 1** Right-click **My Network Places** and select **Properties**. The Network and Dial-up Connections window appears.
Step 2  To add the IP address, follow these steps:

- If you are adding a second multinet IP in a single VLAN configuration, right-click AtNatMP and select Properties. The AtNatMP Properties window appears.
- If you are adding a second multinet IP address in a dual-VLAN configuration, right-click the client VLAN and select Properties. The client VLAN Properties window appears.

Note  In a dual-VLAN configuration, you cannot add the multinet IP address until you configure the dual VLAN because the second IP address is added to the client VLAN. Refer to Chapter 4, “Configuring Dual VLANs.”

Step 3  Choose Internet Protocol (TCP/IP) and click Properties. The Internet Protocol (TCP/IP) Properties window appears.

Step 4  Click Advanced. The Advanced TCP/IP Settings window appears, showing the IP addresses tab. (See Figure 3-2.)

Figure 3-2  Advanced TCP/IP Settings

Step 5  Add the second multinet IP address and subnet mask.

a. In the IP addresses area, click Add. The TCP/IP Address window appears. (See Figure 3-3.)
b. Enter the second IP address and subnet mask and click Add. You are returned to the Advanced TCP/IP Settings window, which now shows both multinets, and you are finished with the configuration. No gateways are configured for the internal NIC.

**Step 6** To close all three windows, click OK in each window and then close the Network and Dial-up Connections window.
Configuring Dual VLANs

This chapter describes how to configure BBSM to support two VLANs on its internal network. The procedure in this chapter assumes that you have already configured your network devices to support the VLANs. For additional information, refer to the product manual for your network device. You must also use the Intel PRO family of NICs for dual VLANs to be supported on the BBSM server.

**Note**
If the internal NIC link speed on the BBSM 5.3 Hotspot appliance is set to auto-detect and/or auto-negotiate, no clients can connect in the dual VLAN configuration. The internal NIC model of the D530 server is Intel Pro/1000 MT Desktop, and it does not forward packets with its link speed set to auto-negotiate after dual VLANs are configured. For it to forward packets in the dual VLAN configuration, its link speed must be set to either 100 or 1000 Mbps full duplex, depending on the speed of the switch port that it is connected to. To set the link speed of the internal NIC on D530, launch the PROset application and click *Intel Pro/1000 MT Desktop Adapter* from the left-hand panel. Click the *Speed* tab on the right-hand panel and then click *100 Mbps* full duplex or *1000 mbps* full duplex radio button.

**Caution**
In a multi-VLAN configuration, the VLANs associated with the trunk port should not be native because packets on a native VLAN are sent untagged to the BBSM server and the server rejects them when the internal NIC is enabled for Institute of Electrical and Electronics Engineers (IEEE) protocol 802.1Q (specifies formatting for dual VLANs).

**Caution**
If you need to install the restore image on a BBSM 5.3 rack-mounted server, you must have the Intel PRO/1000 MT Dual Port Server Adapter, part number PWLA8492MT, installed in the lower slot or the image installation will fail. Refer to the *Cisco BBSM 5.3 Quick Start Guide* for details.
Figure 4-1 shows a BBSM configuration with dual VLANs. In this figure, network device 1 has to tag the VLAN 1 packets. BBSM will drop untagged packets.

**Figure 4-1  Dual-VLAN Configuration in a Bridged Network**

For additional information on VLANs, refer to the “VLANs” section on page 2-1.

**Step 1**  Uncheck the Adaptive Network Address Translation Service component on the AtNatMP NIC interface:


b. Right-click AtNatMP and select Properties. The AtNatMP Properties window appears.

c. Uncheck the Adaptive Network Address Translation Service check box and click OK to close the window.

d. Close the Network and Dial-up Connections window.
Caution

If you forget to uncheck this component and your server starts to reboot continuously, unplug the internal NIC. This will stop the continuous reboot and allow you to uncheck the component.

Step 2

Install the Intel PROset utility that is used to create the management and client VLANs:

- If you purchased a BBSM appliance, go to Step 3.
- If you are installing BBSM from the installation CD, go to Step 4.

Note

The PROSet pack includes 10, 100, and gigabit adapter base drivers and the PROSet utility for Intel PRO network adapters for Windows 2000 and XP.

Step 3

Cisco ships the BBSM appliance with the PROset utility installed on it. You can launch it from a small PROset icon in the right-hand corner of the task bar at the bottom of the window. You can also launch it by using the executable file at this location: c:\Program Files\Intel\NCS\ProSet\Proset.exe.

Step 4

To install the PROset utility from the BBSM Version 5.3 Software CD, follow the steps below. (If the BBSM Installation window appears, click Exit in the bottom-right corner of the window.)

a. Choose Start > Run.
b. Type e:\Drivers\PRO2KXP8.2.1.exe and press Enter to start the PROset installation.
c. Click I accept the terms of the license agreement and click Next.
d. Verify that the files are being saved in the folder c:\IntelPRO and click Next.
e. From the Intel PRO Network Connections window, click Install Software.
f. After the files have been installed, click Exit.
g. As in Step 3, you can run PROset from a small PROset icon in the right-hand corner of the task bar at the bottom of the window. You can also launch it by using the executable file at this location: c:\Program Files\Intel\NCS\ProSet\Proset.exe.

Figure 4-2 shows the main window on the PROset utility.
Step 5  To select the appropriate internal NIC from the two menu items in the Network Components area of the PROset window, follow one of the steps below:

a. If you purchased an appliance, select Intel(R) 82559 Fast Ethernet LAN on Motherboard #2 for the internal NIC from the Network Components.

b. If you installed the BBSM software from a CD, select the internal NIC by examining which network component matches the internal NIC IP address shown in the IP Address line on the right-hand side of the window.

Step 6  To add the VLANs, follow these steps for the management and client VLAN:

a. From the Action menu, click Add Vlan. (See Figure 4-3.)

b. For the first VLAN, enter the appropriate VLAN ID and name the VLAN, such as MgmtVLAN and then click Apply.

c. Repeat these steps for the second VLAN and then close the PROset window.
Step 7  To configure the IP addresses for the management and client VLANs, follow these steps:

Note  These steps describe how to configure the IP address for the client VLAN.


b. Verify that the two VLANs appear in the window. (See Figure 4-4.)

Figure 4-4  Network and Dial-up Connections Window Showing Two VLANs

c. Double-click the first VLAN. (When you finish these steps, you will double-click the second VLAN to configure its IP address.) The VLAN is named VLAN <VLAN name>, ID: <VLAN ID>, such as VLAN ClientsVLAN, ID: 100. This is one of the VLANs that you named in Step 6. The VLAN Status dialog box appears. (See Figure 4-5.)
d. Click Properties. The VLAN Properties window appears.

e. Specify the properties for the VLAN, as shown below:
   - For the client VLAN, uncheck all boxes except TCP/IP and Adaptive Network Translation Service.
   - For the management VLAN, uncheck all boxes except TCP/IP.

f. Select Internet Protocol (TCP/IP) and click Properties. The Internet Protocol (TCP/IP) Properties window appears.

g. Click Use the following IP address and enter a client IP address for the client VLAN you just created (or if applicable a management IP address for the management VLAN).

h. Leave the default gateway and preferred DNS server entries blank.

i. Click OK. A dialog box appears, stating that you have left the DNS field blank. Click OK to acknowledge the message and then click OK to close the window.

j. Repeat these steps for the second VLAN listed in the Network and Dial-up Connections window and then close this window.

Step 8 Use the Address Change Wizard to configure the management and client VLANs and to delete dual-VLAN configurations. Refer to the “Running the Address Change Wizard” section on page 5-1.
Running the BBSM Wizards

This chapter describes how to use the Address Change Wizard to configure BBSM IP addresses. Use the Switch Discovery Wizard to discover the access points and switches on your network.

Running the Address Change Wizard

This procedure describes how to run the Address Change Wizard to enter BBSM IP addresses for singlenet, multinet, and/or dual-VLAN configurations. (The default configuration for BBSM is singlenet.) If you are planning to use public and private IP addressing, be sure to configure Windows for multinetns before running the Address Change Wizard. Refer to the “Configuring Windows for Public and Private IP Addressing” section on page 3-4.

Before you begin using the Address Change Wizard, review the following information to verify that you are using the correct BBSM tool to enter or change addresses.

• For the initial configuration, use the BBSM tools as follows to enter IP addresses:
  – If you purchased a BBSM appliance (rather than BBSM software on CD), use the Address Change Wizard to enter all BBSM IP addresses:
    – The internal and external NIC IP addresses and subnet masks
    – The BBSM internal network address ranges (DHCP, Management, Foreign, and Temp DHCP)
  – If you purchased BBSM software on CD (rather than a BBSM appliance), you should have configured the internal and external NIC IP addresses when you installed the Windows 2000 operating system. In this case, you can use either the Address Change Wizard or the IP Addresses page in WEBconfig to enter the BBSM internal network address ranges. Refer to the “Configuring BBSM Sites” section on page 10-1.

• To change IP addresses after the initial configuration, use the BBSM tools as follows:
  – You can change all BBSM IP addresses by using the Address Change Wizard. You must use the Address Change Wizard to change the TCP/IP internal and external NIC addresses and subnet masks. They cannot be changed on the IP Addresses web page in WEBconfig.
  – You can use the IP Addresses web page in WEBconfig to change the BBSM internal network address ranges (DHCP, Management, Foreign, and Temp DHCP).
  – If you are using multinetns and/or dual VLANs, you must use the Address Change Wizard to delete the second multinet and/or the dual-VLAN configuration.
Caution

If you do not enter the TCP/IP internal and external IP addresses and subnet masks correctly, BBSM will not function properly. If you are performing the initial configuration, be sure to install any service packs or patches before beginning the configuration.

Step 1

Choose **Start > BBSM Configuration Wizards > Address Change Wizard**:

- If your configuration is a single VLAN, the IP Addresses window appears. Go to **Step 4**.
- If your configuration is a dual VLAN, a window appears to map VLAN IDs to the client and management VLANs. This window contains two drop-down menus for mapping VLANs and a check box for deleting the dual-VLAN configuration. (See **Figure 5-1**.) Go to **Step 2**.

![Figure 5-1 Address Change Wizard VLAN Window](image)

Step 2

Verify that the correct VLAN type is associated with the VLAN ID. If the VLAN type does not match the VLAN ID, choose the other VLAN type from the drop-down menu. Notice that the second VLAN type changes to the correct type. When you click **Next**, the IP Addresses window appears, showing the new IP address fields for the client and management VLANs. Go to **Step 4**.
Step 3 If you want to delete the dual-VLAN configuration, follow these steps:

a. In the VLAN window, click **Delete Dual VLAN Configuration** and perform Steps 8 through 12. (You have completed the steps you must follow in the Address Change Wizard.)

Step 4 Verify that the information in the BBSM TCP/IP Properties area is accurate. Figures 5-2 through 5-4 show the IP Addresses window for a singlenet, single-VLAN configuration and a multinet, dual-VLAN configuration. (If you installed BBSM from the CD, only the TCP/IP addresses were automatically entered.)

Caution Do not use the Windows Network and Dial-up Connections window to change IP addresses. This window should only be used to set up multinets and dual VLANs.

Figure 5-2  Address Change Wizard IP Addresses Window (Singlenet, Dual VLAN)
### Figure 5-3  Address Change Wizard IP Addresses Window (Multinet, Single VLAN)

<table>
<thead>
<tr>
<th>BBSM Internal Network Address Ranges</th>
<th>Multinet 1</th>
<th>Multinet 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DHCP Start</strong></td>
<td>192.168.100.21</td>
<td>192.168.100.2</td>
</tr>
<tr>
<td><strong>DHCP End</strong></td>
<td>192.168.100.170</td>
<td>192.168.100.102</td>
</tr>
<tr>
<td><strong>Management Start</strong></td>
<td>192.168.100.2</td>
<td>192.168.100.103</td>
</tr>
<tr>
<td><strong>Management End</strong></td>
<td>192.168.100.20</td>
<td>192.168.100.254</td>
</tr>
<tr>
<td><strong>Foreign (Static) Start</strong></td>
<td>192.168.100.171</td>
<td></td>
</tr>
<tr>
<td><strong>Foreign (Static) End</strong></td>
<td>192.168.100.180</td>
<td></td>
</tr>
<tr>
<td><strong>Temp DHCP Start</strong></td>
<td>192.168.100.163</td>
<td></td>
</tr>
<tr>
<td><strong>Temp DHCP End</strong></td>
<td>192.168.100.254</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BBSM TCP/IP Properties</th>
<th>Multinet 1</th>
<th>Multinet 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal NIC IP</strong></td>
<td>192.168.100.1</td>
<td>192.168.100.1</td>
</tr>
<tr>
<td><strong>Internal NIC Subnet Mask</strong></td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td><strong>External NIC IP</strong></td>
<td>10.10.1.2</td>
<td></td>
</tr>
<tr>
<td><strong>External NIC Subnet Mask</strong></td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td><strong>Default Gateway</strong></td>
<td>10.10.1.1</td>
<td></td>
</tr>
</tbody>
</table>

- Temp DHCP Lease Duration
- Delete Second Multinet
**Step 5**  In the BBSM Internal Network Address Ranges area, enter the DHCP, Management, Foreign (static), and, if applicable, Temp DHCP IP address ranges. Note the following about entering the addresses:

- If you are entering temporary DHCP IP addresses, the minimum number of addresses in the range must be at least 20 percent of the total permanent DHCP IP addresses in multinets 1 and 2.
- If you are using dual VLANs, you must change the IP addresses in the management range to the appropriate addresses for the management VLAN. Refer to Chapter 4, “Configuring Dual VLANs.”
- For field descriptions and important notes, refer to Table 9-2 on page 9-5.

**Step 6**  For a multinet configuration, enter the number of seconds in the Temp DHCP Lease Duration field. (Refer to Table 9-3 on page 9-6.)

**Step 7**  To delete multinet 2 after the initial configuration, check the **Delete Second Multinet** check box in the Multinet section.

**Caution**  You must delete multinet 2 by using the Address Change Wizard for BBSM to function properly. Although you used the Windows Network and Dial-up Connections window to add multinet functionality, do not delete multinets using this window.

**Step 8**  Click **OK**. A dialog box appears, stating that you must stop BBSM services to make the change and asking you to verify this action.

**Step 9**  To stop BBSM services, click **OK**. A second dialog box appears, stating that you have altered the IP addresses and must reboot for the changes to take effect.
Running the Switch Discovery Wizard

After you run the Address Change Wizard, run the Switch Discovery Wizard to discover the switches and access points connected to the BBSM network. The wizard determines the network device type and creates records for the network devices in the BBSM database. Note the following about running the wizard:

- The wizard discovers switches and access points that were configured with an IP address in the Management range (as specified in the Address Change Wizard) and that have the same SNMP read-write community string (password).
- It discovers switches and access points at a single site or multiple sites (one site at a time).
- It discovers network devices in bridged network configurations, not in routed or mixed (bridged and routed) configurations.
- It does not discover CMTSs. Refer to the “Adding and Configuring CMTSs” section on page 12-7.
- The wizard only discovers cluster members and then adds them to the BBSM database; it does not create or enable them. You can cluster up to 16 switches, which use a single IP address. Because clustered Cisco switches do not all have the same SNMP read-write community string (password), specify the password of the master switch, and the wizard will discover all of the switches in the cluster.

⚠️ **Caution**

If you want to cluster your switches, you must first create the Cisco switch clusters before running the Switch Discovery Wizard.

For information on clustering, go to these Cisco websites:

For information on debugging switch connectivity problems, go to this website:

Follow this procedure to run the Switch Discovery Wizard:

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

**Figure 5-5 Site Information**

![Site Information dialog box](image)

**Step 2** Verify that the site number is correct.

**Step 3** Enter the site name and description and click Next:

- If this is a new site, the Enter Site Account Information dialog box appears. Go to Step 4. (See Figure 5-6.)
- If this is an existing site, the The Network Elements Information dialog box appears. Go to Step 5. (Figures 5-7 and 5-8 show singlenet and multinet configurations.)
Step 4 Enter the new Operator and Report account names and passwords and then click OK. The Network Elements Information dialog box appears. (Figures 5-7 and 5-8 show a single-net, single VLAN configuration and a multinet, dual-VLAN configuration.)

Note Operator and Report permissions are specified for each site. The same Operator and Report names and passwords can be used for multiple sites.
Figure 5-7  Network Elements Information Window (Singlenet)
Step 5 Verify that the information is correct and make any needed changes by using the information in Table 5-1.

Table 5-1 Network Elements Information Window Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address Range</strong></td>
<td></td>
</tr>
<tr>
<td>Site</td>
<td>Displays the site number that is being configured.</td>
</tr>
<tr>
<td>Management Start</td>
<td>Displays the beginning and ending IP addresses of the Management range. These IP addresses are obtained from the Address Change Wizard. Click <strong>Change</strong> to edit the management IP addresses.</td>
</tr>
<tr>
<td>Management End Change</td>
<td></td>
</tr>
<tr>
<td>Add Cluster Members</td>
<td>Check this check box if you want the wizard to automatically add all cluster members to the BBSM internal network.</td>
</tr>
<tr>
<td>Mgmt Vlan ID</td>
<td>If you are using a single-VLAN configuration, displays the default VLAN ID. 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.</td>
</tr>
<tr>
<td>Clients VLAN ID (dual VLANs only)</td>
<td>If you are using a dual-VLAN configuration, displays the configured management VLAN ID.</td>
</tr>
</tbody>
</table>
Table 5-1  Network Elements Information Window Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Switch Password</td>
<td>Displays the default name <em>private</em>, which can be changed.</td>
</tr>
<tr>
<td>Discovery Protocol</td>
<td>Click this option to use the Cisco Discovery Protocol. If you are using Cisco switches or access points exclusively, this option is more efficient than the By MAC protocol for discovering network devices.</td>
</tr>
<tr>
<td>CDP</td>
<td>Click this option to use the network device’s MAC address to discover network devices. You can use this protocol if you are using Cisco switches or a combination of Cisco and non-Cisco switches.</td>
</tr>
<tr>
<td>By MAC</td>
<td></td>
</tr>
<tr>
<td>Server TCP/IP Properties</td>
<td></td>
</tr>
<tr>
<td>Internal NIC</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the internal NIC IP address and subnet mask for multinet 1 (and multinet 2 if applicable), which are obtained from the Address Change Wizard.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td></td>
</tr>
<tr>
<td>(single VLAN only)</td>
<td></td>
</tr>
<tr>
<td>Clients VLAN IP Address</td>
<td>Note</td>
</tr>
<tr>
<td>Clients VLAN Subnet Mask</td>
<td>When dual VLANs are being used, these fields are displayed instead of the Internal NIC IP Address and Subnet Mask fields above.</td>
</tr>
<tr>
<td>Mgmt VLAN IP Address</td>
<td>Displays the client VLAN and management IP addresses and subnet masks. If you are using multinet, the Clients VLAN fields show the IP addresses and subnet masks for multinet 1 and 2.</td>
</tr>
<tr>
<td>Mgmt VLAN Subnet Mask</td>
<td>These fields can also be changed by using the Address Change Wizard.</td>
</tr>
<tr>
<td>(dual VLANs only)</td>
<td></td>
</tr>
<tr>
<td>Buttons</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>Changes the range of IP addresses that the Switch Discovery Wizard searches.</td>
</tr>
<tr>
<td>Back</td>
<td>Returns you to the previous page.</td>
</tr>
<tr>
<td>Next</td>
<td>Takes you to the next page.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Exits the wizard.</td>
</tr>
<tr>
<td>Help</td>
<td>Accesses the Switch Discovery Wizard online help.</td>
</tr>
</tbody>
</table>

Step 6  Click **Next**. The Locating Network Elements dialog box appears. It shows a ping being sent to each IP address in the Management range to find the network devices. When this process is complete, the Next button is enabled. (Figures 5-9 and 5-10 show the dialog box for singlenet and multinet configurations.)

If more than one BBSM switch type with the same device type identifier from the SNMP MIB II database (sysObjectID) is discovered during the discovery process, the Select Switch Type dialog box appears. (See Figure 5-11.) In this case, select the actual switch type and click **OK**. The SwitchDiscovery dialog box appears, asking you to verify the selected switch type. Click **Yes** to confirm your selection.
Running the Switch Discovery Wizard

**Figure 5-9  Locating Network Elements Window (Singlenet)**

![Image of Locating Network Elements Window (Singlenet)](image)

**Figure 5-10  Locating Network Elements Window (Multinet)**

![Image of Locating Network Elements Window (Multinet)](image)
**Step 7** From the Locating Network Elements dialog box, click **Next**. The Port Settings dialog box appears. (Figure 5-12 shows multinet configuration.)
Step 8  Configure the port settings by using the information shown in Table 5-2.

### Table 5-2  Port Settings Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Mapping</td>
<td></td>
</tr>
<tr>
<td>Site</td>
<td>Displays the site number that is being configured.</td>
</tr>
<tr>
<td>Page Set</td>
<td>From the drop-down menu, select the appropriate page set for the site that</td>
</tr>
<tr>
<td></td>
<td>you are configuring.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you will be using SSL and have not yet installed your SSL certificate,</td>
</tr>
<tr>
<td></td>
<td>you will not be allowed to select SSL page sets. Choose the Clear version</td>
</tr>
<tr>
<td></td>
<td>of the RADIUS or credit card page set until you install the certificate and</td>
</tr>
<tr>
<td></td>
<td>then change your page set to the SSL page set. For example, choose RADIUSClear</td>
</tr>
<tr>
<td></td>
<td>until the certificate is installed. After installing the certificate, change</td>
</tr>
<tr>
<td></td>
<td>the page set to RADIUS.</td>
</tr>
<tr>
<td>Start Page</td>
<td>The Start Page field automatically populates with the URL that corresponds</td>
</tr>
<tr>
<td></td>
<td>with the page set that you just selected.</td>
</tr>
<tr>
<td>Enable Port Hopping</td>
<td>Check this check box to enable the BBSM port-hopping feature, which enables</td>
</tr>
<tr>
<td></td>
<td>all switches for port hopping and enables the end user to move between</td>
</tr>
<tr>
<td></td>
<td>network hardware such as wireless access points, switch ports, or cable</td>
</tr>
<tr>
<td></td>
<td>modems in a BBSM network without interrupting service. If you want to</td>
</tr>
<tr>
<td></td>
<td>enable port hopping on specific ports, use the Network Elements Port Settings</td>
</tr>
<tr>
<td></td>
<td>pop-up window in WEBconfig. For additional information, refer to Chapter</td>
</tr>
<tr>
<td></td>
<td>13, “Configuring PMS or Print Billing.”</td>
</tr>
<tr>
<td>Delete Existing Port Map</td>
<td>Check this check box if you want to clear the existing port settings.</td>
</tr>
<tr>
<td><strong>Caution</strong></td>
<td>This will erase any previous room mapping.</td>
</tr>
<tr>
<td>Client IP Address Range</td>
<td>Note  This field appears only in a multinet configuration.</td>
</tr>
<tr>
<td>(DHCP)</td>
<td>DHCP assigns leases to clients from either the Multinet 1 or Multinet 2</td>
</tr>
<tr>
<td></td>
<td>IP address ranges. Select the appropriate multinet. (The page set overrides</td>
</tr>
<tr>
<td></td>
<td>this setting if the page set specifies which multinet to use.)</td>
</tr>
<tr>
<td>Buttons</td>
<td></td>
</tr>
<tr>
<td>Back</td>
<td>Returns you to the previous page.</td>
</tr>
<tr>
<td>Finish</td>
<td>Completes the last step of the Switch Discovery Wizard.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Exits from the Switch Discovery Wizard.</td>
</tr>
<tr>
<td>Help</td>
<td>Opens the Switch Discovery Wizard online help.</td>
</tr>
</tbody>
</table>

Step 9  Click Finish. The SwitchDiscovery completion dialog box appears, stating that switch discovery is complete.

Step 10 Click OK. Windows Notepad opens, displaying a log of Switch Discovery activities. (See Figure 5-13.)
Figure 5-13 Switch Discovery Activities

<table>
<thead>
<tr>
<th>Time</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003/04/20 23:04:37</td>
<td>Stopping AtDial service...</td>
</tr>
<tr>
<td>2003/04/20 23:04:37</td>
<td>AtDial service stopped</td>
</tr>
<tr>
<td>2003/04/20 23:04:38</td>
<td>Using existing Site 1 record</td>
</tr>
<tr>
<td>2003/04/20 23:05:30</td>
<td>Site 1 Multinet 1</td>
</tr>
<tr>
<td>2003/04/20 23:05:30</td>
<td>Searching for switches from 192.168.255.2 to 192.168.255.20</td>
</tr>
<tr>
<td>2003/04/20 23:05:30</td>
<td>Ping 192.168.255.2...</td>
</tr>
<tr>
<td>2003/04/20 23:05:34</td>
<td>192.168.255.2: no response</td>
</tr>
<tr>
<td>2003/04/20 23:05:34</td>
<td>Ping 192.168.255.3...</td>
</tr>
<tr>
<td>2003/04/20 23:05:38</td>
<td>192.168.255.3: no response</td>
</tr>
<tr>
<td>2003/04/20 23:05:38</td>
<td>Ping 192.168.255.4...</td>
</tr>
<tr>
<td>2003/04/20 23:05:42</td>
<td>192.168.255.4: no response</td>
</tr>
<tr>
<td>2003/04/20 23:05:42</td>
<td>Ping 192.168.255.5...</td>
</tr>
<tr>
<td>2003/04/20 23:05:46</td>
<td>192.168.255.5: no response</td>
</tr>
<tr>
<td>2003/04/20 23:05:46</td>
<td>Ping 192.168.255.6...</td>
</tr>
<tr>
<td>2003/04/20 23:05:50</td>
<td>192.168.255.6: no response</td>
</tr>
<tr>
<td>2003/04/20 23:05:50</td>
<td>Ping 192.168.255.7...</td>
</tr>
<tr>
<td>2003/04/20 23:05:54</td>
<td>192.168.255.7: no response</td>
</tr>
</tbody>
</table>

**Step 11** After reviewing the log, close the window.

**Note** After running the Address Change Wizard and the Switch Discovery Wizard during the initial configuration, you must configure the DNS forwarding. Refer to Chapter 6, “Configuring DNS Forwarding.”
Configuring DNS Forwarding

After running the Address Change and the Switch Discovery wizards during the initial setup, follow this procedure to enable Domain Name System (DNS) forwarding on BBSM. DNS forwarding allows DNS requests to be relayed to a remote DNS server. (You must obtain the IP addresses for your DNS servers from your ISP before you can perform this procedure.)

BBSM 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 a request for www.cisco.com, are resolved into IP addresses so the Internet routers can locate the web server with the content.

If BBSM cannot resolve an IP address, it responds with its own Internal IP address when the server is pinged. If the IP address that the browser requests cannot be resolved, BBSM displays a Network Error page or the browser displays a DNS fail page.

---

**Step 1** Choose Start > Programs > Administrative Tools > DNS. The DNS window appears.

**Step 2** From the left pane, right-click your BBSM server name and choose Properties. The BBSM Properties dialog box appears, showing the Interfaces tab. (See Figure 6-1.)

**Note** The name of this window depends on your server name. For example, if your server name is BBSM53, the window appears as BBSM53 Properties.
Step 3  Click the Forwarders tab. (See Figure 6-2.)

Figure 6-1  <BBSM Server Name> Properties, Interfaces Tab

Figure 6-2  <BBSM Server Name> Properties, 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**. If you have more than one DNS server IP address, continue to enter them and click **Add** until they are all in the list. Enter the primary DNS server first. It will appear first in the list. Enter the secondary DNS server second.

Step 6  Click **OK** and close the DNS window.
Connecting the PMS or Local Printer

This chapter describes how to connect the PMS or local printer and test the PMS interface.

Connecting BBSM to a PMS or Printer

Follow these procedures to connect a PMS or local printer using serial or IP connections. Follow the procedure only when you are using PMS billing or local print billing. (See Figure 7-1.)

Note
For information on configuring the BBSM server for PMS or local print billing, refer to Chapter 13, “Configuring PMS or Print Billing.”

Figure 7-1 PMS or Local Printer Connection

Follow this procedure to connect the BBSM server to a PMS using an IP connection.

Step 1
Use an Ethernet cable to connect the PMS to the external network.

Step 2
Assign the PMS an IP address that the BBSM server can access.

Step 3
Verify connectivity by pinging the PMS from BBSM and pinging BBSM from the PMS.

Follow this procedure to connect the BBSM server to a PMS using a serial connection.

Step 1
Use a null modem cable (not a straight-through cable) to connect the serial port on the PMS to the BBSM server. Check with the hotel property PMS vendor to determine specific cabling and pin-out requirements.
A null modem cable is one that swaps transmit and receive lines. It is a serial cable with a DB9-to-DB25 connector. A female DB9 connector is required for the BBSM server side, and a male DB25 connector is usually required for the PMS, although a DB9 or DB25 with a male or female connector can sometimes be required.

If the distance between the BBSM server and the PMS is greater than 50 feet, use a short-haul modem. For example, the RAD SRM-3D short-haul modem has been used successfully with previous BBSM installations. (See Figure 7-2.)

**Figure 7-2  Modem Connection Using RAD SRM-3D Connection**

The short-haul modem connects the BBSM server or Site Controller to the PMS using a crossover cable from pins 3 (Receive –) to 4 (Transmit –) and pins 5 (Receive +) to 6 (Transmit +). To have a good connection, verify that Transmit + on one modem connects to Receive + on the other modem and Transmit – from the first modem connects to Receive – on the other modem.

**Step 2**  Test the physical connection from the BBSM server to the PMS using WEB PMS Test feature. Refer to the following section.
Testing the PMS Interface (WEB PMS Test)

This section describes how to test the physical connection from the BBSM server to the PMS using WEB PMS Test. Run this test before BBSM is operational to verify that the PMS is communicating with the BBSM server.

For information on configuring the PMS connection and a list of the PMS protocols, refer to Chapter 13, “Configuring PMS or Print Billing.”

Follow this procedure to set up the test parameters, send a simulated charge posting from BBSM to the PMS, and verify that the charges are posting correctly.

Step 1 From the Dashboard, click WEB PMS Test. The WEB PMS Test web page appears. (Figure 7-3 shows the page with Bell Hobic output.)

Figure 7-3  WEB PMS Test Web Page

Step 2 From the PMS Protocol drop-down menu, select a PMS protocol.
- If you selected a serial protocol, click Config Serial. The COM Port Data area of the web page appears.
- If you selected a TCP protocol, click Config TCP. The TCP Settings area of the web page appears.

Step 3 Configure the communication parameters according to the PMS vendor’s hotel specifications. Refer to Table 7-1 for the WEB PMS Test web page options.

Step 4 To view the changes, click Update.

Step 5 Click Config Data. The Hotel Data area of the web page appears. (See Figure 7-3.)

Step 6 Configure the test charge posting data to be sent to the PMS and click Update.
Testing the PMS Interface (WEB PMS Test)

Chapter 7      Connecting the PMS or Local Printer

Step 7    Send a test charge to the PMS:
   a. Confirm that the selected PMS protocol is correct and click **Send**. If the charge posts successfully, PMS protocol data specific to each kind of protocol appears in the data area of the web page.
   b. To erase the contents of the Dir, Time (UTC), and Data columns, click **Clear**.
   c. Close the browser to exit the program.

**Note**    The WEB PMS Test application must be closed before continuing. The BBSM PMS interface software and WEB PMS Test cannot use the serial COM port at the same time. If WEB PMS Test is left running, BBSM will not be able to communicate with the PMS and the next step to verify charges from client in a guest room will fail.

Step 8    Verify that the charges are posting to the PMS by posting an actual charge:
   a. Connect a guest-room client that is configured with an appropriate page set, such as DailyHotel.
   b. Map the client port by going to the Port Control web page and entering a test location designator for the client port. Unmapped ports will not post charges to the PMS. For information on using the Port Control option, refer to the *Cisco BBSM 5.3 Operations Guide*.
   c. Open the browser and connect to the Internet.
   d. Disconnect the client. Because there is no disconnect button for DailyHotel, enter this URL address in the browser to disconnect:

   http://<internal IP address>/disconnect.asp

   e. Verify that charges were sent to the PMS.

After you have verified that the physical connection to the PMS is working, you can configure PMS billing.

For additional information, refer to Chapter 13, “Configuring PMS or Print Billing.”
### Table 7-1 WEB PMS Test Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send</td>
<td>Posts a test charge to the PMS.</td>
</tr>
<tr>
<td>Clear</td>
<td>Clears the contents of the Dir, Time UTC, and Data columns.</td>
</tr>
<tr>
<td>Config Data</td>
<td>Makes the Hotel Data area of the web page visible, which enables you to specify the data for a charge that you want to send to the PMS.</td>
</tr>
<tr>
<td>Config Proto</td>
<td><strong>Note</strong> This feature is for internal use only. For additional information, contact the Cisco TAC. Refer to the “Obtaining Technical Assistance” section in the preface to this user guide.</td>
</tr>
<tr>
<td>Config Serial</td>
<td>Makes the COM Port Data of the web page visible, which enables you to specify the serial communication settings for the selected PMS protocol.</td>
</tr>
<tr>
<td>Config TCP</td>
<td>Makes the TCP Settings part of the web page visible, which enables you to specify the TCP/IP settings for the selected PMS protocol.</td>
</tr>
<tr>
<td>PMS Protocol</td>
<td>Selects the protocol used by your PMS. Possible drop-down menu selection values are BellHobic, Hilton, Xiox, MicrosFidelioSerial, and MicrosFidelioTCP_IP.</td>
</tr>
<tr>
<td>Update</td>
<td>Commits the changes made to Config Data, Config Proto, or Config COM.</td>
</tr>
</tbody>
</table>
Configuring the Network and Bandwidth Management Settings

Follow this procedure to configure the basic network and bandwidth management settings. You must complete the procedures in Chapter 3, “Getting Started” before beginning the initial system configuration.

**Step 1**

From the Dashboard, click WEBconfig. The BBSM Server Settings web page appears. (See Figure 8-1.)

*Figure 8-1  BBSM Server Settings Web Page*
Step 2  Configure the network configuration and bandwidth management options using the information shown in Table 8-1 and click Save.

### Table 8-1  BBSM Server Settings Web Page Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BBSM Software Information</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Version</td>
<td>Displays the BBSM version number and any updates since the release.</td>
</tr>
<tr>
<td>Updates</td>
<td><strong>Network Configuration</strong></td>
</tr>
<tr>
<td>Enable Maximum Active Sessions</td>
<td>Check this check box so the administrator can set the maximum number of active sessions.</td>
</tr>
<tr>
<td>Maximum Active Sessions</td>
<td>If the Enable Maximum Active Sessions check box is checked, this option sets the maximum number of allowable active sessions. The default of zero indicates that no maximum exists. This option controls the maximum number of simultaneous users.</td>
</tr>
<tr>
<td>Enable Transparent Proxy</td>
<td>Check this box to allow BBSM to force all clients to use a proxy even if they are not configured to do so. With web proxy enabled globally, you can use Microsoft ISA to monitor the Internet sites that the end users have visited. This information appears in the ISA log files. If your router is configured properly, transparent proxy does not need to be enabled for BBSM to operate correctly. Problems occur when the client is using a private IP address and the router is not configured with a static route to the BBSM internal network. In this case, the router cannot route packets to the client and the client cannot browse the Internet. For additional information on proxies, refer to the “Web Proxies” section on page 2-7. To log the transparent proxy entries, refer to the procedure following this table.</td>
</tr>
<tr>
<td>Enable Duplicate IP Address Support</td>
<td>Check this box to allow static clients with duplicate IP addresses to authenticate. This feature allows a client with a duplicate IP address to be redirected to the appropriate Connect page and prompted to authenticate. If the feature is disabled, no client with a duplicate IP address can gain access to the BBSM network. (Before configuring this feature, be sure that no clients are connected to the internal network.) Note For the Duplicate IP feature to work, the local DHCP server must be enabled and inter-client communication must be blocked on network devices. Inter-client communication on Cisco switches is blocked by enabling the protected port feature on client ports and enabling Publicly Secure Port Forwarding (PSPF) on Cisco access points. If you are using Cisco Aironet 1100 or 1200 Series access points with configured VLANs, you must use Cisco IOS Release 12.2(13)JA or later. Note This feature is not supported with routed, combination bridged and routed, or CMTS networks. This field is disabled if these networks are configured.</td>
</tr>
<tr>
<td>SMTP Forwarding Server</td>
<td>Specifies the IP address or fully qualified domain name (FQDN) for SMTP forwarding of all emails. To enable the BBSM server to transmit emails, contact your ISP to register the internal BBSM IP network. Then enter an SMTP server relay IP address or FQDN in this field, which enables BBSM to forward emails to that SMTP server and then to the appropriate mail server. If this field is left blank, the server does not change the SMTP destination for emails being sent.</td>
</tr>
<tr>
<td>Currency Type</td>
<td>From the drop-down menu, choose the local currency type for BBSM transactions. (When designated, this currency type is used in all BBSM options and reports.) The default type is USD.</td>
</tr>
</tbody>
</table>
Chapter 8  Configuring the Network and Bandwidth Management Settings

To log the transparent proxy entries, follow this procedure.

Step 1  Check Enable Transparent Proxy.

Step 2  Choose Start > Programs > Microsoft ISA Server > ISA Management.

Step 3  Open the Servers and Arrays folder and then open the Monitoring Configuration folder.

Step 4  Click Logs.

Step 5  Right-click ISA Server Web Proxy Service.

Step 6  Choose Properties and then the Log tab.

Step 7  Check Enable logging for this service and click OK.

### Table 8-1  BBSM Server Settings Web Page Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bandwidth Management</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Bandwidth Throttle</td>
<td>Check this box if you plan to offer end users the option to choose a bandwidth when they connect. Bandwidth throttling enables the administrator to control the maximum bandwidth allocated to end users per IP address. If you are using the AccessCode and MeetingRoom page sets, you can control bandwidth by using the Access Codes Bandwidth option below.</td>
</tr>
</tbody>
</table>
| Access Code Bandwidth  | From the drop-down menu, choose the desired bandwidth option. The option that you choose determines the bandwidth options that are available on the Access Code Management web page:  
  - None (default)—Disables bandwidth management for access codes.  
  - Throttle—Enables bandwidth throttling for access codes.  
  - Reservation—Enables bandwidth reservation for access codes. |
| **Buttons**            |                                                                             |
| Defaults               | Displays the default parameter settings.                                    |
| Requery                | Refreshes the web page (click before saving changes).                       |
| Save                   | Saves the changes made to the web page.                                     |
Changing the Internal Network IP Address Ranges

This chapter describes public and private IP addresses (multinets) and how to configure the BBSM IP address ranges. Refer to these sections:

- Public and Private IP Addresses (Multinets), page 9-2
- Configuring Internal Network IP Address Ranges in WEBconfig, page 9-3

Use this chapter to change the BBSM internal network IP address ranges:

- End-user clients (DHCP and Foreign addresses)
- Network equipment (Management addresses)
- Multinet temporary DHCP addresses

These are the IP addresses for the entire BBSM server; that is, only one IP configuration exists for each server.

Before using the IP Addresses web page, review the information below to ensure that you are using the correct BBSM tool to enter or change IP addresses.

- For the initial configuration, use the BBSM tools as follows to enter IP addresses:
  - If you purchased a BBSM appliance (rather than BBSM software on CD), use the Address Change Wizard to enter all BBSM IP addresses:
    - The TCP/IP properties (internal and external NIC IP addresses and subnet masks)
    - The BBSM internal network address ranges (DHCP, Management, Foreign, and Temp DHCP)
  - If you purchased BBSM software on CD (rather than a BBSM appliance), you should have configured the internal and external NIC IP addresses when you installed the Windows 2000 operating system. In this case, you can use either the Address Change Wizard or the IP Addresses in WEBconfig to enter the BBSM internal network address ranges.
- To change IP addresses after the initial configuration, use the BBSM tools as follows:
  - You can change all BBSM IP addresses using the Address Change Wizard. You must use the Address Change Wizard to change the TCP/IP internal and external NIC addresses and subnet masks. They cannot be changed on the IP Addresses web page in WEBconfig.
  - You can use the IP Addresses web page in WEBconfig to change the BBSM internal network address ranges (DHCP, Management, Foreign, and Temp DHCP).
  - If you are using multinets, you must use the Address Change Wizard if you want to delete multinet 2.
Caution
Do not use the Windows Network and Dial-up Connections window to change IP addresses. This window should only be used to set up multinets and dual VLANs.

Public and Private IP Addresses (Multinets)

As of BBSM 5.2, you can offer end users a choice of individually assigned private or public DHCP IP addresses.

- **Public IP addresses**—These IP addresses can be accessed by other devices on the Internet. You benefit significantly in several ways by offering public IP addresses to your end users:
  - One key advantage to you is that you can charge a little more for public IP addresses than for private ones. You can offer these addresses to end users who need them and pass along some of your cost to the user. You can specify the prices for the public and private IP addresses on the Connect page, and the end user can decide which one meets his or her needs.
  - Another advantage to offering public IP addresses is that some VPN systems require their clients to have public IP addresses to operate correctly.

- **Private IP addresses**—These IP addresses cannot be accessed by other Internet devices. An advantage of using private IP addresses is that you do not have to take the steps to thwart security threats as you do when you use public 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 cannot be seen on the Internet. Private IP addresses are also less expensive than public IP addresses.

A BBSM server can be configured as follows:

- **Multinet**—A BBSM server that is configured to support both private and public IP addresses is classified as multinet because the internal NIC is configured with two distinct logical subnets.

- **Singlenet**—A BBSM server that is configured as a single logical subnet and supports only one subnet of IP addresses is classified as a singlenet.

Table 9-1 shows the singlenets and multinets with subnets.

<table>
<thead>
<tr>
<th>Network</th>
<th>Routed</th>
<th>Not Routed</th>
<th>Subnets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Singlenet</td>
<td>X</td>
<td></td>
<td>One bridged internal subnet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X</td>
<td>One bridged internal subnet and one internal subnet per router</td>
</tr>
<tr>
<td>Multinet</td>
<td>X</td>
<td></td>
<td>Two bridged internal subnets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X</td>
<td>Two bridged internal subnets and two internal subnets per router</td>
</tr>
</tbody>
</table>

For the initial configuration, BBSM can be configured in two ways for multinet based on whether BBSM is customer installed or factory installed:

- Customer-installed BBSM servers can be configured as multinets or singlenets when the Windows 2000 operating system is being installed. For additional information, refer to the *Cisco BBSM 5.3 Installation Guide*. 
Factory-installed BBSM servers are configured initially as a singlenet and must be reconfigured for multinets. To change your BBSM server to a multinet configuration, you must configure Windows for multinets. Refer to the “Configuring Windows for Public and Private IP Addressing” section on page 3-4.

For additional information about multinet use, refer to the following sections:

- To configure the public or private IP addresses, refer to the “Running the Address Change Wizard” section on page 5-1.
- To see which page sets support multinet provisioning by an administrator or self-provisioning by the end user, refer to the “Page Set Overview” section on page 18-2.

### Configuring Internal Network IP Address Ranges in WEBconfig

Follow this procedure to configure the IP address ranges for the internal BBSM network. If you are configuring your system for the first time, refer to the “Running the Address Change Wizard” section on page 5-1.

Note that these IP address configurations are possible:

- Singlenet or multinet with dual VLANs
- Singlenet or multinet without dual VLANs

---

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

**Step 2**  In the NavBar, click IP Addresses. The IP Addresses web page appears. Figures 9-1 and 9-2 show the web pages for a single network (singlenet) and for multinets.
Chapter 9  Changing the Internal Network IP Address Ranges

Figure 9-1  IP Addresses Web Page (Singlenet, Single VLAN)

![IP Addresses Web Page](image)

**Building Broadband Service Manager**

**WEBconfig**

**IP Addresses**

**BB3M Internal Network Address Ranges**
- DHCP Start: 192.168.255.21
- DHCP End: 192.168.255.230
- Management Start: 192.168.255.1
- Management End: 192.168.255.20
- Foreign (Static) Start: 192.168.255.231
- Foreign (Static) End: 192.168.255.254

**BB3M TCP/IP Properties**
- **Internal NIC**
  - IP Address: 192.168.255.1
  - Subnet Mask: 255.255.255.0

- **External NIC**
  - IP Address: 10.10.1.2
  - Subnet Mask: 255.255.255.0
  - Default Gateway: 10.10.1.1

---

**CAUTION:**
Do not use the Network and Dial-up Connections feature in Windows to change IP addresses.

---

The BB3M TCP/IP properties cannot be changed or updated in the IP Addresses web page. Use the BB3M Address Change Wizard to make any changes.
Step 3  Enter the IP configuration data based on the information shown in Tables 9-2 and 9-3. Table 9-2 shows the IP address ranges that are used for singlenet and multinet configurations.

Table 9-2  IP Addresses Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Singlenet</th>
<th>Multinet 1</th>
<th>Multinet 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP and Management IP ranges</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Foreign IP address ranges</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temp DHCP IP addresses</td>
<td>—</td>
<td>Multinet 1 or 2, whichever address range is higher</td>
<td></td>
</tr>
</tbody>
</table>

Step 4  Verify that the TCP/IP IP addresses are correct. They must be accurate for BBSM to function properly. If they are incorrect, refer to the “Running the Address Change Wizard” section on page 5-1 to change them.
Table 9-3  IP Addresses Web Page Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Start</td>
<td>Enter the starting and ending IP addresses for network equipment such as switches, base switches, access points, CMTSs, and network-addressable UPS systems.</td>
</tr>
<tr>
<td>Management End</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>When Dual VLAN is configured on BBSM server, the management range should be on the management VLAN.</td>
</tr>
<tr>
<td>If you are using multinets,</td>
<td>Note: Multinet 1—Usually the private multinet.</td>
</tr>
<tr>
<td>note the following:</td>
<td>Multinet 2—Usually the public multinet used for remote management. It is also used to assign static addresses to clients that need this configuration, such as for a meeting room in which the client needs routable addresses for its own servers.</td>
</tr>
<tr>
<td>Caution</td>
<td>All IP addresses in the management range are granted unchallenged access to the Internet. For security reasons, Cisco recommends that you use an address range only large enough for your network devices.</td>
</tr>
<tr>
<td>DHCP Start</td>
<td>Enter the starting and ending IP addresses to be assigned to end-user DHCP clients.</td>
</tr>
<tr>
<td>DHCP End</td>
<td></td>
</tr>
<tr>
<td>Foreign (Static) Start</td>
<td>Enter the starting and ending Foreign IP addresses for end-user clients that are configured with static IP addresses. This address range enables BBSM to perform adaptive network address translation (NAT) for statically configured devices in a bridged environment.</td>
</tr>
<tr>
<td>Foreign (Static) End</td>
<td>Note: All other NAT and PAT functionality is handled by the external router.</td>
</tr>
<tr>
<td>Temp DHCP Start</td>
<td>Enter the starting and ending IP addresses for the DHCP leases received by clients when they initially connect to the network. The minimum number of addresses in the range must be at least 20 percent of the total permanent DHCP IP addresses in multinets 1 and 2. Cisco recommends 20 to 30 percent.</td>
</tr>
<tr>
<td>Temp DHCP End (multinets only)</td>
<td>Note: This range must belong to the numerically higher multinet on the internal network.</td>
</tr>
</tbody>
</table>

**Multiple VLANs**                                                                                              |

(dual VLANs only)                                                                                                                                                        |
| Client VLAN ID               | Displays the client VLAN ID.                                                                                                                                                                                                                                                                 |
| Mgmt VLAN ID                 | Displays the management VLAN ID.                                                                                                                                                                                                 |

Caution: All IP addresses in the management range are granted unchallenged access to the Internet. For security reasons, Cisco recommends that you use an address range only large enough for your network devices.
### Table 9-3  IP Addresses Web Page Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **BBSM TCP/IP Properties**  
(These fields are read only on this web page. To change these IP addresses, you must use the Address Change Wizard.) | |
| **Internal NIC** | Displays the IP address and subnet mask of the internal NIC that connects to the internal BBSM network. If you are using multinets, this field displays the IP address and subnet mask for multinets 1 and 2.  
Cisco recommends that you set the number of IP addresses (rooms or clients) only to the needed size and no larger. Because BBSM initializes each address at startup, configuring a larger range of IP addresses than necessary can greatly increase the initialization time and degrade performance. The following list shows the number of IP addresses available for the subnet sizes that you will probably use:  
- 255.255.255.0 subnet mask = /24 subnet code = 254 users  
- 255.255.254.0 subnet mask = /23 subnet code = 510 users  
- 255.255.252.0 subnet mask = /22 subnet code = 1022 users | |
| **Client VLAN IP Address** | Note When dual VLANs are being used, these fields are displayed instead of the internal NIC IP Address and Subnet Mask fields above.  
Displays the client VLAN and management IP addresses and subnet masks. If you are using multinets, the Clients VLAN fields show the IP addresses and subnet masks for multinets 1 and 2.  
These fields can also be changed by using the Address Change Wizard. | |
| **External NIC** | Displays the IP address and subnet mask of the external NIC that connects to the external router. | |
| **BBSM DHCP Properties**  
(multinets only) | Enter the lease time for the temporary DHCP lease that a client receives when it connects to the BBSM network. Set this time low so that when the client chooses its IP preference, it receives its final IP address in a short amount of time. The longer it takes for the client to receive its final IP address, the more likely it is that the Temp DHCP range will fill up, which will prevent additional clients from connecting. The default is 60 seconds.  
Note Some cable modems are unable to receive an IP address if the lease time is less than 180 seconds. When cable modems are being used, the Temp DHCP Lease Duration may need to be adjusted for them to come online. After all of the modems have come online and the port settings are configured for each port, you can re-adjust the Temp DHCP Lease Duration to a lower value again. | |
| **Buttons** | Refreshes the web page (click before saving any changes).  
Saves the changes made to the web page. | |
Configuring BBSM Sites

Follow this procedure to configure one or more BBSM sites using the Sites web page in WEBconfig. You can add sites, change site information, and delete sites and their related network devices using this web page. (Before adding and configuring new sites in WEBconfig, verify that the necessary BBSM network cabling, hardware, routers, switches, and clusters are attached to the new site.)

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

**Step 2** In the NavBar, click **Sites**. If the first site has been configured, the Sites web page appears, showing the site number, name, and description. (See Figure 10-1 and Table 10-1.) If the first site has not been configured, the New Site web page appears, requesting the new site information. (See Figure 10-2 and Table 10-2.)

**Step 3** Go to these steps to add a new site:

- To configure a site if site 1 does not exist, go to **Step 4**.
- To configure a site if site 1 already exists, go to **Step 5**.
Figure 10-1 Sites Web Page

Figure 10-2 New Site Web Page
Step 4 Enter the new site information based on the information in Table 10-2 and click Save. You have completed this procedure.

Step 5 Click New on the Sites web page (Table 10-1). The New Site web page appears, requesting the new site information.

Note Operator and Report permissions are specified for each site. The same Operator and Report names and passwords can be used for multiple sites.

Step 6 If you need to change the site name or description, enter the correct information and click Save.

Table 10-1 Sites Web Page Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Number</td>
<td>From the drop-down menu, choose the number of the site you want to modify. The default is 1.</td>
</tr>
<tr>
<td>Site Name</td>
<td>Enter the name of the site.</td>
</tr>
<tr>
<td>Site Description</td>
<td>Enter a site description, such as San Diego or Building One.</td>
</tr>
</tbody>
</table>

Buttons

| New               | Adds a new site. The new site web page appears, showing a new site number. Enter the site information and click Save. |
| Requery           | Refreshes the web page (click before saving changes).                      |
| Save              | Saves the changes made to the web page.                                   |
| Delete            | Deletes the site, including all network elements and port settings for the site. |

Note Be cautious about deleting site records because rooms or locations must be mapped manually again.
Table 10-2  New Site Web Page Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Site Information</strong></td>
<td></td>
</tr>
<tr>
<td>Site Number</td>
<td>Displays the new site number.</td>
</tr>
<tr>
<td>Site Name</td>
<td>Enter the name of the site. The name can contain a maximum of 30 characters, including letters, numbers, special characters, and spaces. (The web page does not enable you to type more than 30 characters, so you do not need to count characters.)</td>
</tr>
<tr>
<td>Site Description</td>
<td>Enter the site description, such as <em>Building One</em>.</td>
</tr>
<tr>
<td><strong>Set New Site Permissions</strong></td>
<td></td>
</tr>
<tr>
<td>Operator Account Name</td>
<td>Enter the site operator account name and password. Retype the password to confirm it.</td>
</tr>
<tr>
<td>Operator Account Password</td>
<td></td>
</tr>
<tr>
<td>Confirm Password</td>
<td></td>
</tr>
<tr>
<td>Report Account Name</td>
<td>Enter the site report account name and password. Retype the password to confirm it.</td>
</tr>
<tr>
<td>Report Account Password</td>
<td></td>
</tr>
<tr>
<td>Confirm Password</td>
<td></td>
</tr>
<tr>
<td><strong>Buttons</strong></td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>Creates a new site.</td>
</tr>
<tr>
<td>Requery</td>
<td>Refreshes the web page (click before saving changes).</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the changes made to the web page.</td>
</tr>
</tbody>
</table>
Configuring Routers

Follow the procedure in this chapter to configure a router on the BBSM internal network. (Refer to your network configuration information to configure the router fields.)

In BBSM, all network devices are associated with a router. This association tells BBSM how to build routes to the network internal to the router. For additional information about networking options, including routed networks, refer to the “Transmission and Networking Options” section on page 1-3.

Note

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

Step 1
From the Dashboard, click WEBconfig. The BBSM Server Settings web page appears.

Step 2
In the NavBar, click Routers. The Routers web page appears. (Figure 11-1 shows the Routers web page for a multinet, dual-VLAN configuration.)
Step 3  Enter the router data based on the information shown in Table 11-1 and click Save. (For router number 0, which is the BBSM server, all fields except Router Number and SNMP Password are disabled. These fields are enabled only if the router number is greater than 0.)

Table 11-1  Routers Web Page Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Router Number Go          | Displays the router number of the router being configured. (BBSM degenerates this number.)  
|                           | Click Go to advance to the router number entered in the text field to the left of the Go button. Use this field to conveniently retrieve any router record without having to use the > or < buttons to advance through each router. |
| Gateway to Router         | Enter the IP address of the first hop from the BBSM server to the router. This address should be on the BBSM server’s internal network and is the router’s external address if the router is connected directly to the BBSM server’s network. |
| Router IP Address         | Displays the client-side IP address of the router. On clients, this IP address is the default gateway. For clients connected to the BBSM server internal network, the gateway is the BBSM server’s internal NIC address. The default is 127.0.0.1. (This loopback IP address refers to the BBSM server and cannot be changed for router 0.) |
| Client Start Client End   | Enter the starting and ending IP addresses and the subnet mask for the clients connecting to this router. This subnet mask value must be configured on the clients and is set automatically for DHCP clients. |
| Client Subnet Mask        |                                                                              |
| Temp DHCP Start Temp DHCP End (multinet only) | Enter the starting and ending IP addresses for the temporary DHCP address range. |
### Table 11-1  Routers Web Page Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router Dual VLAN Support</td>
<td>Check this check box to enable dual VLANs on the router. This feature is disabled by default.</td>
</tr>
<tr>
<td>Mgmt Router IP</td>
<td><strong>Note</strong> These fields apply only when two VLANs are configured.</td>
</tr>
<tr>
<td>Mgmt Start</td>
<td>Enter the IP address of the router for the management VLAN and the starting and ending IP address and subnet mask of the network devices in the management VLAN.</td>
</tr>
<tr>
<td>Mgmt End</td>
<td></td>
</tr>
<tr>
<td>Mgmt Subnet Mask</td>
<td></td>
</tr>
<tr>
<td>Router Supports SNMP</td>
<td>If you are using a router that supports SNMP, check this check box:</td>
</tr>
<tr>
<td></td>
<td>• For router 0 (the BBSM server), the check box is checked and disabled. The SNMP password field is enabled.</td>
</tr>
<tr>
<td></td>
<td>• For routers other than router 0, the field is enabled. If you check the check box, the SNMP password field is enabled. Otherwise, the SNMP password is disabled.</td>
</tr>
<tr>
<td>Caution</td>
<td>Restrictions exist to disabling Router Supports SNMP. Because BBSM does not know the client’s MAC address, it cannot use a network device (switch DLL) to determine if the session is still active (the administrator must configure the null switch). This inability to identify the client affects many BBSM operations, including reporting, the Daily access policy Welcome Back feature, and any per-port policy.</td>
</tr>
<tr>
<td>SNMP Password</td>
<td>Enter the SNMP read-write community string (password) that is used when communicating with routers. The default is <em>public</em>.</td>
</tr>
<tr>
<td>Create Client DHCP Scope</td>
<td>Check this check box if BBSM is your DHCP server. A DHCP scope is created on the BBSM server for the router subnet, as determined by the IP addresses in the Client Start and Client End fields. Leave the check box unchecked if you are using a DHCP server other than BBSM.</td>
</tr>
<tr>
<td><strong>Multiple VLANs</strong></td>
<td><em>(dual VLANs only)</em></td>
</tr>
<tr>
<td>Clients VLAN ID</td>
<td>Displays the client VLAN ID.</td>
</tr>
<tr>
<td>Mgmt VLAN ID</td>
<td>Displays the management VLAN ID.</td>
</tr>
</tbody>
</table>

**Buttons**

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Adds a new router web page with a router number. (When you add routers, physically install them before trying to configure them.)</td>
</tr>
<tr>
<td>Requery</td>
<td>Refreshes the web page (click before saving changes).</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the changes made to the web page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the router from the site.</td>
</tr>
</tbody>
</table>
Configuring Network Elements

This chapter describes how to configure the BBSM-supported network device types: access points, switches, and CMTSs. To configure the network devices, you must first configure at least one site. Refer to Chapter 11, “Configuring Routers.”

These sections describe the network types and how to configure them:

- Switch Clustering, page 12-2
- Configuring Access Points, page 12-2
- Adding and Configuring CMTSs, page 12-7
- Configuring Switches, page 12-12

**Caution**
The SNMP password located in WEBconfig under Network Elements must match the SNMP read-write community string that is configured in the network device software. If the BBSM password does not match the community string (password), BBSM cannot communicate with or locate end users connected to the network device. To change the network device SNMP read-write community string, follow the manufacturer’s instructions.

**Note**
When BBSM is trying to locate the port to which a client is connected, BBSM sequentially queries each configured network device, looking for the client's MAC address. When BBSM locates the client, it stops querying the network devices and displays the appropriate page set Connect page on the client's browser.

If a configured network device does not respond to the BBSM query, BBSM times out on the query after a while and then retries the query and times out again. As a result, nonresponsive network devices greatly increase the time BBSM takes to locate clients on network devices that follow the nonresponsive network devices in the BBSM search order.

To prevent this unnecessary delay in client search logic, simply disable each nonresponsive network device using the Webconfig Network Elements web pages. When the nonresponsive network devices are connected and functioning correctly, enable them again on the Webconfig Network Elements pages.
Switch Clustering

Cisco switch clustering technology is supported as of BBSM 5.2. A switch cluster comprises up to 16 switches that are managed using just one IP address. The administrator can update the WEBconfig Switches page using only the master switch IP address and a unique SNMP read-write community string (password) for each switch in the cluster.

Some of the switches that support switch clustering are the Catalyst 1900, 2900 XL, 2950, 3500, and 3550 XL switches. The list changes frequently as Cisco releases new switches that are added to BBSM.

Note
Before running the Switch Discovery Wizard or configuring clustered switches in WEBconfig, you must enable the switch clustering capability for all cluster-capable switches. For detailed information, refer to your switch documentation.

Configuring Access Points

This section provides basic information about using access points, including authentication, and the procedure to configure them in WEBconfig.

Overview

Cisco Aironet access points are wireless LAN transceivers that serve as the center point of a stand-alone wireless network or as the connection point between wireless and wired networks. The port-hopping feature in BBSM enables a user to move among access points in a LAN if the user moves within the configurable period of the hop timer. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network. The roaming functionality is based on signal quality, not proximity. When a client’s signal quality drops, the client roams to another access point.

To make the access point work with BBSM, the access point must be online and able to receive a ping from the BBSM server. Then you configure the access point in WEBconfig. (For BBSM 5.0, choose Generic without Link Status for the access point. The access point appears as two ports—the uplink port and a client port. If the access point appears as 30 ports, you have the newer access point firmware.)

To handle several client connections in a wireless LAN, BBSM polls the bridge MIB on the access point to detect client MAC addresses just as it polls the MIB on a switch.

The following are common topics of interest about using access points:

- **EAP and LEAP**—Entering the IP addresses of the wireless access points and switches allows the full Extensible Authentication Protocol (EAP) and Light EAP (LEAP) authentication traffic to pass through the BBSM server. (Refer to the bulleted section below on wireless hotspots.)

- **Roaming**—If a client’s signal to a distant access point remains strong, the client does not roam to a closer access point. If client devices checked continuously for closer access points, the extra radio traffic would slow throughput on the wireless LAN.

- **Segmenting users**—Wireless meeting room users can be segmented from public space users. These are the options:
  - **No wireless cell overlay**—Dedicate access points with meeting room page sets and public space access points with the RADIUS, credit card, or other page sets.
Wireless cell overlay—Account for overlap and use the Mega page set. Meeting room clients use access codes while public space clients use RADIUS and credit cards, for example. This configuration allows for overlapping wireless cells to be used by both meeting room and public space clients. At the same time, bandwidth is being controlled.

Depending on the firmware version of the Cisco access point, the association of service set identifiers (SSIDs) and VLANs is supported. For example, different types of users can be assigned to different VLANs; the visitor VLAN can go to BBSM, and the enterprise user VLAN can bypass BBSM.

- Wireless hotspots—Use Cisco Aironet access points to deploy wireless hotspots. (These access points support open authentication through the use of an SSL certificate.)

- Security with LEAP and Wired Equivalent Privacy (WEP)—When access points at a hotspot have an open-air link to clients, eavesdroppers can tap into the traffic being transmitted very easily. Using IPSec 3DES VPN connections to the enterprise typically addresses these security concerns. However, mobile end user must first authenticate with BBSM through the unprotected link. For this reason, you can choose whether or not to use SSL-protected BBSM page sets to secure the connection between the end user and the server.

- Disabling inter-client communication with PSPF—Inter-client communication on Cisco switches is blocked by enabling the protected port feature on client ports and enabling Publicly Secure Port Forwarding (PSPF) on Cisco Aironet access points. For additional information, refer to the Cisco documentation for the applicable access point.

- Disconnecting—When the user ends a wireless session without disconnecting and multiple users are connected to a single access point, the access point has a table of MAC addresses for each connected client and a corresponding timer. When there is no activity, a timer counts down to zero from a preconfigured time period. The next time BBSM polls the access point, the server finds that the MAC has timed out and marks the client as disconnected. The user gets charged only for the actual connected time.

For additional information about Cisco wireless LAN products, refer to this website:

Access Point Configuration Procedure

Follow this procedure to configure each access point in WEBconfig.

Step 1  From the Dashboard, click WEBconfig. The BBSM Server Settings web page appears.

Step 2  In the NavBar, navigate to the Access Points web page by choosing Network Elements > Site x > Access Points. The Access Points web page appears. (See Figure 12-1.)

![Figure 12-1 Access Points Web Page (Singlenet, Single VLAN)](image)

Step 3  Configure the access points based on the information shown in Table 12-1 and click Save. The Network Element Port Settings window pops up. (See Figure 12-2.)

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

Step 4  Enter the information in the Network Element Port Settings window based on the information in Table 12-2 and click Submit. A dialog box appears, asking you to verify your changes. Click OK and you are returned to the Access Points web page.

Note  If you add or remove a default VLAN for your access point, you must reconfigure the access point. To do this, click Submit in the Network Element Port Settings window. For more information on VLANs, refer to the “VLANs” section on page 2-1.
### Table 12-1 Access Points Web Page Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Information</td>
<td>Displays the site number, site name associated with the access points to be configured.</td>
</tr>
<tr>
<td>Cluster Number Go</td>
<td>Displays the cluster number associated with the access point to be configured. Click Go to advance to any cluster number that has been configured in WEBconfig. This is a more convenient way to access records than using the &lt; or &gt; buttons to advance one record at a time.</td>
</tr>
<tr>
<td>Access Point Type</td>
<td>From the drop-down menu, choose an access point type.</td>
</tr>
<tr>
<td>Access Point IP Address</td>
<td>Enter a unique IP address in the management range assigned to the access point.</td>
</tr>
<tr>
<td>SNMP Password</td>
<td>Enter the SNMP read-write community string (password) that is used when communicating with the access point. The default is private.</td>
</tr>
<tr>
<td>Caution</td>
<td>Cisco recommends that you change the default password on the access points because the default password is well known and could compromise network security.</td>
</tr>
<tr>
<td>Router</td>
<td>From the drop-down menu, choose the IP address of the router that this access point is connected to. If the site and cluster are directly connected to the BBSM server, use the default IP address for the BBSM server, which is 127.0.0.1.</td>
</tr>
<tr>
<td>Packet Inactivity Period</td>
<td><strong>Note</strong> This field is disabled unless your access point type supports packet inactivity. Enter the time, in seconds, that a user can be idle before being automatically signed off by BBSM. If needed, refer to the Cisco BBSM Products Network Device Compatibility Guide to verify the access points that monitor for packet inactivity.</td>
</tr>
<tr>
<td>Disable AP</td>
<td>Check this check box if you do not want BBSM to look for clients on the ports for the access point. Use when troubleshooting. <strong>Note</strong> Even 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.</td>
</tr>
<tr>
<td>VLANs</td>
<td><em>(These fields apply only when two VLANs are configured.)</em></td>
</tr>
<tr>
<td>Clients VLAN ID</td>
<td>Displays the client VLAN ID.</td>
</tr>
<tr>
<td>Mgmt VLAN ID</td>
<td>Displays the management VLAN ID.</td>
</tr>
<tr>
<td>Buttons</td>
<td></td>
</tr>
<tr>
<td>Port Settings</td>
<td>Configures the access point ports. The Network Element Port Settings window pops up. Enter the correct information, as described in Table 12-2 and click Submit.</td>
</tr>
<tr>
<td>New</td>
<td>Adds a new access point. The web page changes to reflect this new access point.</td>
</tr>
<tr>
<td>Defaults</td>
<td>Displays the default parameter settings.</td>
</tr>
<tr>
<td>Requery</td>
<td>Refreshes the web page (click before saving changes).</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the changes made to the web page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the access point.</td>
</tr>
</tbody>
</table>
### Figure 12-2 Network Element Port Settings Pop-up Window

![Network Element Port Settings Pop-up Window](image)

### Table 12-2 Port Settings Window Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Displays the network device type.</td>
</tr>
<tr>
<td>Location Prefix</td>
<td>Enter a location prefix. The prefix can contain a maximum of 40 characters. (This field is optional.)</td>
</tr>
<tr>
<td>Page Set</td>
<td>From the drop-down menu, choose a page set. For descriptions of the default page sets that ship with BBSM, refer to Table 18-1 on page 18-3.</td>
</tr>
<tr>
<td>Caution</td>
<td>If you will be using SSL and have not yet installed your SSL certificate, you will not be able to select an SSL page set. Choose the Clear version of the page set until you install the certificate 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 install the SSL page set before installing the certificate, the Start page will not display.</td>
</tr>
<tr>
<td>Note</td>
<td>For CMTSs, the page set that you choose is the default page set that will be applied to the CMTS dynamic port-room configuration. Refer to the “Dynamic Port-Room Configuration for CMTSs” section on page 13-13.</td>
</tr>
<tr>
<td>Start Page</td>
<td>BBSM automatically enters the Start page for the network device based on the page set. However, you can enter a different Start page.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Enter a bandwidth throttling value in kbps for clients connected to this network device. The bandwidth is effective only if bandwidth management is turned on. (Refer to Chapter 9, “Changing the Internal Network IP Address Ranges.”) If the end user selects a bandwidth from the Connect page, that selection overrides this default bandwidth.</td>
</tr>
</tbody>
</table>
Adding and Configuring CMTSs

If you are using a CMTS, you must add a CMTS record in WEBconfig as a network device for a site. Follow this procedure to add and configure the CMTS record.

**Note**

If you are using an external provisioning server for your cable modem, such as TFTP, ToD, or a log server, you must create a walled garden entry for the cable modems to come online properly. The entry must consist of only an IP address and subnet mask for the cable modems to access these servers. The walled garden hostname, which is usually used for clients using a proxy server setting, can be just a description.

**Step 1**

From the Dashboard, click WEBconfig. The BBSM Server Settings web page appears.

**Step 2**

In the NavBar, navigate to the CMTS web page by choosing Network Elements > Site 1 (or other applicable site) > CMTS. The initial CMTS configuration selection web page appears the first time you configure the CMTS. (See Figure 12-3.)
Step 3  Enter the CMTS IP address and select a CMTS configuration (IRB, Routed, or Bridged) based on the information shown in Table 12-3 and click Submit. The appropriate CMTS network configuration web page appears. (See Figures 12-4 through 12-6.) (The IRB and Bridged CMTS configuration web pages are the same for singlenet or multinet. Only the Routed configuration web pages are different for singlenet and multinet.)

Table 12-3  Initial CMTS Web Page Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the new CMTS IP address</td>
<td>Enter the IP address of the CMTS being added. This is the CMTS client-side IP address:</td>
</tr>
<tr>
<td></td>
<td>• In a Bridged or IRB configuration, this IP address is on the same subnet as the DHCP and Management ranges.</td>
</tr>
<tr>
<td></td>
<td>• In a Routed configuration, this IP address is not on the BBSM internal network but on a subnet internal to the router.</td>
</tr>
<tr>
<td>IRB</td>
<td>Click if the CMTS is configured for an integrated routed and bridged configuration, which means that the CMTS acts as both a router for cable modems and a bridge for end users.</td>
</tr>
<tr>
<td>Routed</td>
<td>Click if the CMTS is configured as a router. In this case, BBSM cannot support static clients (plug and play).</td>
</tr>
<tr>
<td>Bridged</td>
<td>Click if the CMTS is configured in a bridged configuration.</td>
</tr>
<tr>
<td>Button</td>
<td>Submit  Takes you to the CMTS configuration web page for the mode you selected.</td>
</tr>
</tbody>
</table>

Step 4  Configure the CMTSs based on the information shown in Table 12-4 and click Save. The Network Element Port Settings window pops up. (See Figure 12-2 on page 12-6.)
Chapter 12  Configuring Network Elements

Adding and Configuring CMTSs

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

Step 5
Enter the applicable information based on the information in Table 12-2 on page 12-6 and click Submit. A dialog box appears, asking you to verify your changes. Click OK and you are returned to the applicable CMTS web page.

Figure 12-4  IRB CMTS Web Page (Singlenet, Single VLAN)
Figure 12-5  Routed CMTS Web Page (Multinet, Dual VLAN)

Network Elements - CMTS

- **CMTS Type**: CMTS
- **Cluster Number**: 5
- **CMTS IP Address**: 192.10.255.255
- **Gateway to Router**
- **Gateway IP**
- **Client VLAN ID**: 100
- **Netw VLAN ID**: 2

**Top Menu**: Site | Site | CMTS | Switches | Port Test Settings | VLAN | Security/SSL | Bandwidth Reservation | Custom Page Sets | Web Access | Port Mirroring | Alerts

**Configuration Options**
- **Cable Modem DHCP Range and Options**
  - **Cable Modem DHCP End**
  - **Cable Modem Subnet Mask**
  - **(002) Time Offset**
  - **(003) Time Server**
  - **(004) Router**
  - **(005) DNS Server**
  - **(016) Boot File Name**

**Multiple VLANs**
- **Client VLAN ID**: 100
- **Netw VLAN ID**: 2

**Notes**
- If port configuration records already exist, the Network Element Fort Settings window does not pop up automatically when you click Save. Click Port Settings.
- Even if you disable a CMTS, its IP address remains reserved. If you need to reuse its IP address for a different network element, change the IP address of the disabled CMTS temporarily; otherwise, you will not be able to update WEBsyst.
- For bridged configuration, the DHCP IP address range must be on the same subnet as your internal NIC. For RB and routed configurations, the DHCP IP range must be on the same subnet as your internal NIC.
Table 12-4  IRB, Routed, and Bridged Configuration CMTS Web Page Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMTS Type</td>
<td>Based on the CMTS configuration and the CMTS IP address that you entered, the system automatically fills in the basic parameters and displays the CMTS type, cluster number, CMTS IP address, and router of the CMTS that you will be configuring.</td>
</tr>
<tr>
<td>Cluster Number</td>
<td>Displays the cluster number associated with the CMTS.</td>
</tr>
<tr>
<td>CMTS IP Address</td>
<td>Displays the router that the CMTS is connected to.</td>
</tr>
<tr>
<td>Router Number</td>
<td>Checks if you do not want BBSM to look for CMTS clients on the ports for the cluster.</td>
</tr>
<tr>
<td>Disable CMTS</td>
<td>If your CMTS configuration is disabled, its IP address remains reserved.</td>
</tr>
<tr>
<td>Aging Period (in seconds)</td>
<td>Enter the time period in seconds that the client can be idle before the end user is automatically signed off. The default is 300 (5 minutes).</td>
</tr>
<tr>
<td>SNMP Password</td>
<td>Enter the SNMP read-write community string (password) that is used when communicating with the CMTS. The default is public. (Cisco recommends that the default password on the switches and on BBSM be changed because the default password is well known and could compromise network security.)</td>
</tr>
<tr>
<td>Router Number (IRB or Routed configuration)</td>
<td>Displays the router number associated with the CMTS.</td>
</tr>
</tbody>
</table>
## Table 12-4  IRB, Routed, and Bridged Configuration CMTS Web Page Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Gateway to Router  
(IRB and Routed configurations) | Displays the IP address of the first hop from the BBSM server to the router. |
| Router IP Address  
(Routed configuration) | Displays the IP address of the router that you are connecting to. The router IP address is the same as the CMTS IP address when the CMTS is in the Routed configuration. |
| Client Start  
Client End  
Client Subnet Mask  
(Routed configuration) | Enter the starting and ending IP addresses and the subnet mask for the clients connecting to this CMTS. The BBSM server treats traffic from the Client Start through the Client End IP address range as coming from client computers. |
| Cable Modem DHCP Start  
Cable Modem DHCP End | Enter the starting and ending IP addresses to be assigned to the cable modems.  
- For Bridged configuration, the IP address range must be on the same subnet as your internal NIC.  
- For IRB and Routed configurations, the IP range must not be on the same subnet as your NIC. |
| Cable Modem Subnet Mask  
(IRB or Routed configuration) | Enter the cable modem subnet mask for the DHCP IP addresses. In a bridged configuration, the subnet mask is the same as your internal NIC subnet mask. |
| DHCP options | Because these options are standard DHCP options, they are not described here. An administrator configuring the CMTS will probably understanding these options.  
**Note** Refer to the Internet Engineering Task Force (IETF) Request for Comments (RFC) 2132 for details about these DHCP options. |
| **VLANs**  
(These fields apply only when two VLANs are configured.) |  |
| Clients VLAN ID | Displays the client VLAN ID. |
| Mgmt VLAN ID | Displays the management VLAN ID. |
| **Buttons** |  |
| New | Configures a new CMTS. The initial CMTS web page appears. |
| Requery | Refreshes the web page (click before saving changes). |
| Save | Saves the changes made to the web page. |
| Delete | Deletes the CMTS. |
| Port Settings | Configures the CMTS ports. The CMTS Port Settings window pops up. Enter the correct information, as described in Table 12-2 on page 12-6. |
Configuring Switches

Follow this procedure to configure each switch. Most BBSM installations use two types of switches:

- Client switches—Connect to end-user computers called clients.
- Base switches—Connect to base switches, also known as aggregation switches.

Unused ports on the base switch can be used as client ports if the base switch is added to the Switches web page. When the base switch is also being used as a client switch, the ports connected to client switches must be marked as uplink ports. For instructions on how to configure a port as an uplink port, refer to the Cisco BBSM 5.3 Operations Guide.

As of BBSM 5.2, Cisco supports switch clustering. For additional information about the clustering architecture, refer to the “Switch Clustering” section on page 12-2.

Step 1

From the Dashboard, click WEBconfig. The BBSM Server Settings web page appears.

Step 2

In the NavBar, navigate to the Switches web page by choosing Network Elements > Site x > Switches. The Switches web page appears. (Figure 12-7 shows a dual-VLAN configuration.)

Figure 12-7 Switches Web Page (Dual VLAN)
Step 3 Configure the switches based on the information shown in Table 12-5 and click Save. The Network Element Port Settings window pops up. (See Figure 12-2 on page 12-6.)

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

Step 4 Enter the applicable information in the Network Element Port Settings window based on the information in Table 12-2 on page 12-6 and click Submit. A dialog box appears, asking you to verify your changes. Click OK and you are returned to the Switches web page.

### Table 12-5 Switches Web Page Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Information</td>
<td>Displays the site number and name associated with the switch to be configured.</td>
</tr>
<tr>
<td>Cluster Number</td>
<td>Displays the cluster number and cluster member number associated with the switch to be configured.</td>
</tr>
<tr>
<td>Cluster Member No.</td>
<td>Click Go to advance to another previously configured switch. This is a convenient way to advance to another switch record without having to use the &lt; or &gt; buttons to advance one switch at a time.</td>
</tr>
<tr>
<td>Switch Type</td>
<td>From the drop-down menu, choose a switch type. Because the list of supported Cisco switch types continues to be updated, refer to the following document for the latest list of supported network devices: <a href="http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/devices.pdf">http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/devices.pdf</a></td>
</tr>
<tr>
<td>Cluster/Switch IP Address</td>
<td>Enter a unique IP address in the management range assigned to the cluster or switch. Check with the person installing your clusters and switches if you are unsure of this IP address.</td>
</tr>
<tr>
<td>SNMP Password</td>
<td>Enter the SNMP read-write community string (password) that is used when communicating with switches. (Non–Cisco stackable switches, which share the same stack, are installed with the same password.) The default is “public.”</td>
</tr>
<tr>
<td>Note</td>
<td>Cisco recommends that the default password on the switches and on BBSM be changed because the default password is well known and could compromise network security.</td>
</tr>
<tr>
<td>Router</td>
<td>From the drop-down menu, choose the router IP address of the router that this site and cluster are connected to. If the site and cluster are directly connected to the BBSM server, use the default IP address for the BBSM server, which is 127.0.0.1.</td>
</tr>
<tr>
<td>Disable Switch</td>
<td>Check this check box if you do not want BBSM to look for clients on the cluster ports. Use when troubleshooting. (Even 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. If you do not change the IP address, you will not be able to update WEBconfig.)</td>
</tr>
<tr>
<td>Aging Period (in seconds)</td>
<td>Enter a time period, in seconds, that the network device will wait before eliminating inactive clients from its internal tables, which causes BBSM to automatically sign off the client. The default time period is 300 (5 minutes).</td>
</tr>
<tr>
<td>Packet Inactivity Period (in seconds)</td>
<td>This field is disabled unless your switch type supports packet inactivity. Enter a time, in seconds, that a user can be idle before being automatically signed off by BBSM. If needed, refer to the <em>Cisco BBSM Products Network Device Compatibility Guide</em> to verify the switches that monitor for packet inactivity.</td>
</tr>
<tr>
<td>No. of Client Ports</td>
<td>Enter the number of ports that can be used as clients on switch 1 of the cluster. The default is 23.</td>
</tr>
<tr>
<td><strong>VLANs</strong></td>
<td><em>(These fields apply for dual VLANs only.)</em></td>
</tr>
<tr>
<td>Clients VLAN ID</td>
<td>Displays the client VLAN ID.</td>
</tr>
<tr>
<td>Mgmt VLAN ID</td>
<td>Displays the management VLAN ID.</td>
</tr>
</tbody>
</table>
### Table 12-5  Switches Web Page Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Buttons</strong></td>
<td></td>
</tr>
<tr>
<td>Port Settings</td>
<td>Click to configure the settings for all ports on this switch. The Network Element Port Settings window pops up. Enter the applicable information based on the parameters in Table 12-2 on page 12-6 and click <strong>Submit</strong>.</td>
</tr>
<tr>
<td>New Cluster/Switch</td>
<td>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. Use this option also to add a single, nonclustered switch.</td>
</tr>
<tr>
<td>New Cluster Member</td>
<td>Adds a new network device to an existing cluster. A new web page appears with blank fields so the associated parameters can be configured. (If a switch is not cluster capable or not configured as a cluster switch, BBSM considers the switch as a cluster of a single switch.)</td>
</tr>
<tr>
<td>Defaults</td>
<td>Displays the default parameter settings.</td>
</tr>
<tr>
<td>Requery</td>
<td>Refreshes the web page (click before saving changes).</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the changes made to the web page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the switch.</td>
</tr>
</tbody>
</table>
CHAPTER 13
Cisco BBSM 5.3 Configuration Guide

13-1

Configuring PMS or Print Billing

You must decide which billing option you want to use with BBSM—PMS or print billing, RADIUS, or credit cards—and configure the option in WEBconfig. This chapter describes PMS, including two-way PMS, and print billing (local non-PMS bill printing) and lists the PMS protocols that BBSM currently supports. Follow the procedures in this section to implement PMS or print billing for the site:

- Overview, page 13-1
- Two-Way PMS Interface, page 13-2
- Supported PMS Protocols, page 13-2
- Configuring PMS or Print Billing, page 13-4
- Configuring PMS Call Types, page 13-6
- Mapping Rooms, page 13-9

Overview

With PMS or print billing, the DailyHotel page set, which uses the Hotel accounting policy, sends the BBSM guest charges to the PMS or local printer. By default, charges are sent to the PMS or printer when the guest ends the session.

Caution
Verify that the physical connection to the PMS is working before continuing with this section. For details, refer to the “Testing the PMS Interface (WEB PMS Test)” section on page 7-3.

Refer also to the following:
- To clear any unwanted charges posted during the room mapping process, refer to the section on clearing charges in the Cisco BBSM 5.3 Operations Guide.
- To reconfigure page set parameters, such as when the guest charges are sent to the PMS or printer, refer to the “Creating Custom Page Sets Manually” section on page 18-12.
- To connect a BBSM server to a PMS, refer to Chapter 7, “Connecting the PMS or Local Printer.”

With PMS billing, the BBSM guest room is billed directly for the charges through the PMS. When charges are sent to the PMS, a one-letter call type is sent to the PMS as part of the billing record to classify the service that was used, such as Internet access charges or web printing. Although the PMS integrator determines the actual call types, you can modify the BBSM default call types and add, change, or delete custom call types.
With print billing, the BBSM charges are sent to a local printer. The printed bill consists of the date, time, room number, site number, port ID, and charge printed on a single line. The format and content of the print report cannot be changed.

**Two-Way PMS Interface**

With the two-way PMS feature, the PMS interface becomes bidirectional so you can pull data from the PMS for enhanced functionality. You can customize guest content and enable guests to view folios and check out from the room. BBSM provides a page set template that demonstrates how to use these features. The BiDirectional_DailyHotel page set template displays the following basic guest information: title, name, company, language, VIP status, arrival date, and departure date. You can customize the information with additional fields. For details, refer to the Cisco BBSM 5.3 SDK Developer Guide.

When the two-way PMS feature is enabled, BBSM monitors room status (checked-in/out). If no guest is checked into the room, BBSM prevents an unauthorized person from using the port. The PMS provides this room status during database swaps and through real-time check-in and check-out records. When a guest checks out of a room, port use is restricted until a new guest checks in. BBSM also restricts access if the checked-in guest is a cash-only guest and is not allowed to post charges to the room.

When multiple guests are registered to one hotel room, the two-way PMS interface behavior changes as described:

- Only basic Internet service is allowed, assuming that all guests in the room are allowed to post charges.
- The guest-based features—guest data, view folio, and remote checkout—are not available. BBSM cannot determine which guest is using the port in the hotel room, so guests receive basic Internet access, which is similar to using the DailyHotel page set.
- If at least one registered guest in the room is not allowed to post charges (cash only), then no Internet access is available.

The two-way PMS interface requires an active link to the PMS. However, BBSM maintains a local copy of guest information and enables a guest to connect to the Internet even if the PMS is unavailable. BBSM stores the incurred charges and sends them to the PMS when the link is re-established.

BBSM currently provides the two-way PMS interface only for the Micros-Fidelio protocol (both serial and TCP/IP connections). Using the BBSM SDK, you can extend any of the other existing protocols to take advantage of the bidirectional interface. You can also use the SDK to implement a new PMS protocol module that is not currently supported.

**Supported PMS Protocols**

BBSM provides interfaces for a number of standard PMS protocols. The currently supported PMS protocols include the following:

- Bell Hobic—Encore, GEAC/UX, GuestView, LanMark, LIBICA, Lodging Management System (LMS) from Inter-American Data (IAD), Logistics, Megasys Hospitality Systems, MSI, Promus 21, Protocol Technologies
Note

The BBSM Bell Hobic PMS interface posts the room number as five characters, with padding of spaces added on the right if the room number contains less than 5 digits; for example, room number changes from 20 to 20xxx with x indicating a space.

- Xiox
- Micros-Fidelio—6.x and 7.x, Fidelio Express and Opera
- Hilton—Hilton H1, Hilton H2
- Hotel Information Systems (HIS)—CLS by Hotel Information Systems (Product Code: CLSS380IB; call and request BBSM interface)
- Maestro (Bell Hobic, XIOX, Hilton)

BBSM is also compatible with and has been deployed by billing through the FCS call accounting package that is widely used in China and the Asia Pacific.

BBSM now supports IP connections and bidirectional links to PMS systems. Currently, BBSM supports only the Micros-Fidelio IP-based PMS protocol and the Micros-Fidelio bidirectional PMS interface. If you want to interface to another IP-based PMS protocol or want a bidirectional link to another PMS system, you need to create a custom PMS module using the BBSM SDK.

For additional information on the bidirectional PMS interface, refer to the “Two-Way PMS Interface” section on page 13-2.
Configuring PMS or Print Billing

As of BBSM 5.3, PMS or print billing is configured for each server, not each site. Follow the steps below to configure PMS billing or print billing.

**Note**

When using a TCP/IP connection to a PMS system from the BBSM internal network, the PMS IP address must be in the Management range on BBSM.

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

**Step 2**
In the NavBar, navigate to the Settings web page by choosing **Billing > PMS or Printer > Settings**. The Settings web page appears. (See **Figure 13-1**.)

**Figure 13-1 PMS or Printer Settings Web Page**

Configure the PMS billing or print billing options based on the information in **Table 13-1** and click **Save**.
Table 13-1  PMS or Printer Settings Web Page Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property Management System</td>
<td></td>
</tr>
<tr>
<td>Enable PMS Billing</td>
<td>Check if you are using PMS billing to send room charges to the hotel PMS.</td>
</tr>
<tr>
<td>PMS Protocol</td>
<td>From the drop-down menu, choose a PMS protocol:</td>
</tr>
<tr>
<td></td>
<td>• MicrosFidelio TCP/IP</td>
</tr>
<tr>
<td></td>
<td>• Bell Hobic</td>
</tr>
<tr>
<td></td>
<td>• Hilton</td>
</tr>
<tr>
<td></td>
<td>• MicrosFidelio Serial</td>
</tr>
<tr>
<td></td>
<td>• Xiox</td>
</tr>
<tr>
<td>PMS IP Address</td>
<td><strong>Note</strong> This field supports the IP-based PMS interface. You must choose the MicrosFidelio TCP/IP protocol. For an IP-based PMS, enter the IP address for the PMS.</td>
</tr>
<tr>
<td></td>
<td>PMS TCP/IP Port                                                              Enter the port to be used for the interface to the PMS. (You must choose the MicrosFidelio TCP/IP protocol.)</td>
</tr>
<tr>
<td>Enable Two-Way PMS</td>
<td>Check if you are using two-way communication between BBSM and the PMS. (For two-way PMS to work, you must choose one of the MicrosFidelio PMS protocols.)</td>
</tr>
<tr>
<td>Database Resync Time (per day)</td>
<td><strong>Note</strong> This field is enabled only if you chose Enable Two-Way PMS. Enter the time of day—hour and minute—that you want for synchronizing the PMS database with the BBSM database. Because resyncing the database can take several minutes or several hours, depending on the number of guest rooms on the property, the default time is 4 a.m. Because guests may not be able to connect during the resync, Cisco recommends that you set a time at which guests do not usually activate sessions.</td>
</tr>
<tr>
<td>Print</td>
<td></td>
</tr>
<tr>
<td>Print Billing Locally</td>
<td>Check if you will be printing bills to a local printer.</td>
</tr>
<tr>
<td>Local Billing Printer</td>
<td>Enter the name of the printer to be used for billing. This name must match exactly the default printer name as it is defined in the Printers folder for printing to work.</td>
</tr>
<tr>
<td>Buttons</td>
<td></td>
</tr>
<tr>
<td>Requery</td>
<td>Refreshes the web page (click before saving changes).</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the changes made to the web page.</td>
</tr>
</tbody>
</table>
Configuring PMS Call Types

If you are using PMS billing, you may want to add, change, or delete PMS call types. Follow the steps below to configure the call type options.

Note

The BBSM-supplied call types, Internet Session and Web Printing, cannot be deleted, and only the call type code can be modified. Custom call types, however, can be added, modified, or deleted.

Step 1
Contact the hotel or the PMS integrator to find out what call types are defined for the PMS.

Step 2
From the Dashboard, click WEBconfig. The BBSM Server Settings web page appears.

Step 3
In the NavBar, navigate to the Call Types web page by choosing Billing > PMS or Printer > Call Types. The Call Types web page appears. (See Figure 13-2.)

Figure 13-2  Call Types Web Page

Step 4
Configure the call types based on the information shown in Table 13-2 and click Save. The server can have multiple call types such as A for Internet charges and W for web printing.
Configuring a Laptop for Mapping Rooms

After running the Address Change and the Switch Discovery wizards and configuring DNS forwarding during the initial setup, you can map the rooms or locations.

You should map rooms if you plan to use location-based billing, such as in a hotel environment. If you are using RADIUS or credit card billing, you do not need to map rooms.

This section describes these procedures:

- Configuring the Laptop, page 13-7
- Configuring the Browser, page 13-9

Details of how to map the rooms are provided in the “Mapping Rooms” section on page 13-9.

Configuring the Laptop

Verify that your laptop meets the following requirements, then configure it as described in the sections that follow.

To map rooms, you need a laptop that meets the following specifications:

- Windows 95, 98, ME, 2000 Professional, or XP Professional operating system.
- A NIC that is configured to use TCP/IP with DHCP enabled and DNS disabled. (For Windows 2000 Professional, set it to obtain a DNS server address automatically.)
- One of these web browser releases: Internet Explorer 5.0 or later, or Netscape 4.7x or later
Configuring Windows

Follow this procedure to configure a laptop that is operating on a Windows 95, 98, or ME operating system.

**Step 1** From your desktop, right-click **Network Neighborhood**.

**Step 2** Click **Local Area Connection** and then click **Properties**.

**Step 3** Select the **Configuration** tab.

**Step 4** Choose the TCP/IP protocol for your network interface card (Windows 95, 98, or ME) and click **Properties**. The TCP/IP Properties dialog box appears.

**Step 5** Select the **IP Address** tab.

**Step 6** Click the **Obtain an IP address automatically** radio button.

**Step 7** Select the **Gateway** tab and remove all gateway addresses.

**Step 8** Select the **DNS Configuration** tab and click **Disable DNS**.

**Step 9** Click **OK** in each window to close the TCP/IP Properties and Network or General windows. (If you receive a request to copy files from your Windows CD, follow the instructions.)

**Step 10** If a dialog box appears, asking you if you want to restart, click **Yes**.

Follow this procedure for setting up a laptop that is operating on a Windows 2000 Professional or Windows XP Professional operating system.

**Step 1** Uncheck the Client for Microsoft Networks check box, as follows:

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

- **b.** Right-click **Local Area Connection**, and from the drop-down menu, choose **Properties**. The Local Area Connection Properties window appears.

- **c.** Uncheck the **Client for Microsoft Networks** check box.

**Note** If you do not uncheck the Client for Microsoft Networks check box, the ASP files will load very slowly.

**Step 2** Choose **Internet Protocol (TCP/IP)** and click **Properties**. The Internet Properties (TCP/IP) Properties window appears.

**Step 3** Verify that **Obtain an IP address automatically** and **Obtain a DNS server automatically** are both selected and click **OK**.

**Step 4** Click **OK** three times to close all windows.

**Note** You do not have to reboot.
Chapter 13  Configuring PMS or Print Billing  

Configuring the Browser  

Regardless of the type of browser that you are using, it must be set to connect directly to the Internet with all proxy server options turned off.  

Follow this procedure to configure Internet Explorer 5.0 or later.

**Step 1**  
Open Internet Explorer.

**Step 2**  
Choose **Tools > Internet Options**. The Internet Options window appears.

**Step 3**  
Select the **Connections** tab and click **LAN Settings**. The Local Area Network (LAN) Settings window appears.

**Step 4**  
Uncheck all check boxes and then click **OK**.

**Step 5**  
Close Internet Explorer.

Follow this procedure to configure Netscape 4.7x or later.

**Step 1**  
Open Netscape.

**Step 2**  
From the Edit menu, choose **Preferences**. The Preferences window appears.

**Step 3**  
Double-click **Advanced** and choose **Proxies**. The Proxies Preferences window appears.

**Step 4**  
Click the **Direct connection to the Internet** radio button and then click **OK**.

Mapping Rooms  

When ports are configured initially, room or location designators are created automatically for each port. This section describes how to replace these designators with actual designators. This process is called room mapping. This procedure also describes how to test the port. Note the following about how ports are configured:

- During the initial configuration, ports can be configured as follows:
  - Switches and access points—Ports can be configured initially using the Switch Discovery Wizard or WEBconfig.
  - CMTSs—Ports cannot be configured using the Switch Discovery Wizard. They can be configured using the Network Element Port Settings pop-up window in WEBconfig or mapped using the dynamic CMTS port-room configuration. For information on mapping ports and rooms dynamically for cable modems, refer to the “Dynamic Port-Room Configuration for CMTSs” section on page 13-13.
- If switches, access points, and/or CMTSs are being added after the initial configuration, they can all be configured using the Network Element Port Settings pop-up window in WEBconfig.
Caution

The only way to ensure that your port-room mapping is accurate is to use this Map Rooms option to map locations or rooms. If you enter port locations the first time using the Port Locations field in Port Control, there is no way to verify that ports have been mapped to the correct room numbers. After rooms have been mapped, you can update port locations using Port Control.

Basic Room Mapping

This section describes the basic procedure for mapping room and testing the network devices.

In addition, CMTS ports and rooms can be mapped dynamically. Refer to the “Dynamic Port-Room Configuration for CMTSs” section on page 13-13.

Before you begin mapping rooms, you may want to modify the DailyHotel page set so that a new charge will be incurred for each room that is mapped. By default, the DailyHotelPackage.asp file sets the bWelcomeBackMAC parameter to true, which means that the laptop that is being used to map the rooms only incurs a charge the first time it connects. To change this, navigate to the c:\atcom\ekgnkm\DailyHotelPackage.asp file on the BBSM server, open the file with Microsoft Notepad, and look for bWelcomeBackMAC. Change the value of this parameter from true to false. Remember to change this setting back to true after you map your rooms if you prefer that setting.

Refer to these sections for additional information that may help you:

- For detailed instructions on changing page set parameters, refer to the “Creating Custom Page Sets Manually” section on page 18-12.
- To clear any unwanted charges posted during the room mapping process, refer to the section on clearing pending hotel charges in the Cisco BBSM 5.3 Operations Guide.

Follow this procedure to map each room and test the port for switches, access points, and CTMSs.

### Step 1
At the location or room, connect the laptop to a jack (BBSM port).

### Step 2
Launch Internet Explorer. The BBSM Start page appears.

**Note** You must have an active BBSM session to map a room.

### Step 3
Click Connect. You now have an active BBSM session.

### Step 4
Enter the BBSM Dashboard’s URL: [http://<internal_IP_address>:9488/www](http://<internal_IP_address>:9488/www), where <internal_IP_address> is the internal IP address of the BBSM server you want to access; for example, type [http://10.10.2.1:9488/www](http://10.10.2.1:9488/www), and press Enter. The Enter Network Password dialog box appears.

### Step 5
Enter your username and password. The username was defined when the site was created. Leave the domain name blank. (You must have administrator or operator privileges to map the rooms.) Click OK.

**Note** If you leave the browser open, the login identification information is cached, and you do not need to enter it again. If you close your browser between rooms, you will be prompted to re-enter the password.

### Step 6
From the Dashboard, click Map Rooms. (For a BBSM server that has multiple sites, choose the appropriate site from the drop-down menu.) The Map Rooms web page appears. (See Figure 13-3.)
Enter location identifier (room name or number) below:

- Check here if this is a meeting room.

Step 7 Enter the appropriate guest room or location number. If you need to correct the room number, click Reset.

Step 8 If applicable, check the Check here if this is a meeting room check box. Checking this box sets the page set for that port to the MeetingRoom page set.

Step 9 To map the room to the port, click Submit. A confirmation web page appears, indicating that the room is mapped correctly. At this point, the connection between the port and the room has not been tested:

- In the “Time of last port test” field, the word never appears.
- In the Packet Loss field, the message 100% - (No packets transmitted) appears.

(Figure 13-4 shows the confirmation web page.)

Note If the port to room mapping failed, the port number will show ERROR rather than a valid port number. If this message appears, the actual room has not been mapped.
Step 10  To test the port connection, click **Port Test**. Wait several seconds for the test to complete. Again, the confirmation web page appears, this time showing the following:

- In the “Time of last port test” field, the time that the packet was transmitted appears.
- In the Packet Loss field, the message **0.00% - (Pass)** appears.

(Figure 13-5 shows the port test web page for basic room mapping.)

If the port test fails, repeat the test. If the test fails repeatedly, contact the Cisco TAC. Refer to the “Obtaining Technical Assistance” section in the preface to this user guide.
Step 11  When the port test is complete, enter this URL in the address line on the browser: http://<internal IP address>/disconnect.asp

Step 12  Disconnect from the room jack.

Dynamic Port-Room Configuration for CMTSs

In previous releases of BBSM, the CMTS ports had to be mapped to each cable modem before the rooms could be mapped. As of BBSM 5.2, the room mapping procedure has changed as follows:

- You do not need to generate a port map before mapping rooms for the cable modems.
- An active session is not required.
- BBSM assigns a default page set, DailyHotel, so you can map the rooms without having previously mapped the ports.

**Note**

If a port designator was already created automatically, the room is mapped just as it is described in the “Basic Room Mapping” section on page 13-10.

However, if you want to change the default page set, you must configure the CMTS port using the WEBconfig CMTS Network Element Port Settings pop-up window before performing the dynamic port-room configuration. Refer to the “Adding and Configuring CMTSs” section on page 12-7.
Caution

If you change network device port settings, including the page set, your existing port parameters will be reset.

Follow this procedure to map the cable modem ports and rooms in one step. This procedure assumes that the ports have not been mapped before this procedure.

Step 1
Connect a laptop and launch Internet Explorer. The Enter Network Password dialog box appears.

Step 2
Enter your username and password. The username was defined when the site was created. Leave the domain name blank. (You must have administrator or operator privileges to map rooms.) Click OK. The Map Rooms web page appears. (See Figure 13-6.)

Figure 13-6 Map Rooms Web Page

Note
If you leave the browser open, the login identification information is cached, and you do not need to enter it again. If you close your browser between rooms, you will be prompted to re-enter the password.

Step 3
Enter the appropriate guest room or location number. If you need to need to correct the room number, click Reset.

Step 4
If applicable, check the Check here if this is a meeting room check box. Checking this box sets the page set for that port to the MeetingRoom page set.

Step 5
To map the room to the port, click Submit. A confirmation web page appears, indicating that the room is mapped correctly. At this point, the connection between the port and the room has not been tested:
- In the “Time of last port test” field, the word Never appears.
- In the Packet Loss field, the message 100% - (No packets transmitted) appears.
(Figure 13-7 shows the confirmation web page.)
Step 6  To perform the optional port test, click Port Test. Wait several seconds for the test to complete. Again, the confirmation web page appears, this time showing the following:

- In the “Time of last port test” field, the time that the packet was transmitted appears.
- In the Packet Loss field, the message \textit{0.00\% - (Pass)} appears.

(Figure 13-8 shows the port test web page.)

If the port test fails, repeat the test. If the test fails repeatedly, contact the Cisco TAC. Refer to the “Obtaining Technical Assistance” section in the preface to this user guide.
Step 7  When the port test is complete, unplug the cable connected to the cable modem. The cable modem resets within 30 seconds. (If the cable modem does not reset, manually reset it.)

Step 8  To map additional modems in the same room, follow the steps below:

a. Repeat Steps 1 through 4. A web page appears, showing that you have already mapped this room. (See Figure 13-9.)

b. Click I want to have multiple ports in Room x and click Submit.

c. To perform the optional port test, repeat the test procedures previously described.
Step 9  When you are mapping the second or subsequent cable modem rooms, if you entered an incorrect room number and the *Room x is already mapped* web page appears (Figure 13-9), click **I typed the wrong room number. I want to cancel** and **Submit**. You are returned to the Map Rooms web page where you can enter the correct room number and continue with the procedure.

Step 10 If you want to replace an existing cable modem with another one, click **I want to replace one of the following modems in Room # x** and then click the cable modem to be replaced. Click **Submit**.
Configuring RADIUS Billing

This chapter describes the BBSM interface with the RADIUS server, including the RADIUS attributes that BBSM supports, user-provisioned bandwidth page sets, and prepaid RADIUS. The procedure to configure the RADIUS server billing options assumes that you have already run the Switch Discovery Wizard to configure the ports to use either the RADIUS page set or a custom page set. (Refer to the “Running the Switch Discovery Wizard” section on page 5-6.)

The chapter provides these sections:

- **Overview, page 14-1**
- **RADIUS Attributes, page 14-4**
- **Configuring the RADIUS Server Options, page 14-6**
- **Configuring RADIUS for Multiple Sessions, page 14-9**

Refer also to the RADIUS Session History Report section in the *Cisco BBSM 5.3 Operations Guide*.

**Overview**

The BBSM server has a built-in RADIUS client that complies with RADIUS standards, IETF RFCs 2865 and 2866, and is compatible with any compliant RADIUS server, although the officially supported servers are Cisco ACS, Microsoft IAS, and Navis.

**RADIUS Authentication and Authorization**

Each time the end user connects to the BBSM server using a page set configured for RADIUS, BBSM prompts for a username and password. BBSM then sends this information to a configured RADIUS authentication server in an access-request packet.

---

**Note**

The RADIUS authentication server does not have to be the same server as the RADIUS accounting server.

To provide redundancy in case the RADIUS server does not respond, you can configure multiple RADIUS servers in WEBconfig. This configuration includes the order in which these servers are contacted, with lowest ranked server being the first server contacted, the next highest ranked server being the second server contacted, and so on. For example, if two RADIUS servers are configured with rank 30
and 31, server 30 will be contacted first, then 31 will be contacted. (Refer to the “Configuring the RADIUS Server Options” section on page 14-6.) BBSM attempts to contact the servers until an access-accept packet is received:

- If a server does not respond within the specified time, BBSM attempts to contact that server up to three times before moving to the next server.
- If a server responds with an access-reject packet, BBSM immediately sends the access-request packet to the next server.

**RADIUS Accounting**

BBSM saves Internet session information and then sends it to a configured RADIUS accounting server in start and stop accounting-request packets and, if configured, in interim-update packets. BBSM sends this data in the same ranked order and manner that it uses for access-request packets. With this session data, administrators can perform independent billing on a flat-rate or per-minute basis.

**User-Provisioned Bandwidth**

The two user-provisioned bandwidth (UBand) page sets, RADIUSUBand and RADIUSUBandClear, enable administrators to define bandwidth offerings. The end user chooses a bandwidth on the Start page. These are examples:

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

BBSM throttles the session at the chosen bandwidth and sends the bandwidth VSA to the RADIUS accounting server in the start, stop, and interim-update accounting-request packets.

**Note**

The administrator must ensure that the RADIUS accounting server is configured to accept this bandwidth so the data can be retrieved for billing. The RADIUS provider is responsible for charging the end user.

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

**Using Prepaid RADIUS**

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

BBSM supports the prepaid functionality by supporting the RADIUS Session-Timeout attribute. This attribute is sent from the RADIUS server in the access-accept packet and indicates the number of seconds allowed for the end user’s session. Between sessions, the user account is maintained by the RADIUS server, not BBSM.
Chapter 14      Configuring RADIUS Billing

Overview

To set up BBSM for prepaid RADIUS, you need a RADIUS server that supports the following prepaid functionality:

- It can establish a user account that has a certain amount of time associated with it.
- When the user logs in, it sends the account time remaining in the Session-Timeout attribute in the access-accept packet.
- When the user disconnects, it reads the Acct-Session-Time attribute in the accounting stop packet.
  The RADIUS server must decrement the user's account by this amount.

Some RADIUS servers, such as the Cisco Access Registrar (CAR), have native support for the prepaid feature. Other servers can be extended to support this functionality. In some cases, a RADIUS server and a billing server combined can support the prepaid feature.

Although the BBSM prepaid RADIUS feature supports only time-based billing, volume-based billing is possible on a post-paid basis. Users can be charged based on packet volume when they log out of a session because BBSM sends the volume data to the RADIUS server in the accounting stop packet in the Acct-Input-Packets (47) and Acct-Output-Packets (48) attributes.

If you are using RADIUS for billing, you must configure BBSM to operate as a RADIUS client. This section describes how to configure BBSM for RADIUS billing and how to configure multiple concurrent RADIUS sessions. This configuration enables BBSM clients to be authenticated against a RADIUS server.
RADIUS Attributes

This section describes the RADIUS attributes that BBSM sends to and receives from the RADIUS server. Table 14-1 lists the access-request and accounting-request attributes by packet type, and Table 14-2 describes these attributes and several others that could be included in the access-accept packet from the RADIUS server.

Table 14-1  RADIUS Access-Request and Accounting-Request Packets

<table>
<thead>
<tr>
<th>Attribute</th>
<th>No.</th>
<th>Access-Request</th>
<th>Accounting-Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-Name</td>
<td>1</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>User-Password</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAS-IP-Address</td>
<td>4</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>NAS-Port</td>
<td>5</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Service-Type</td>
<td>6</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Framed-Protocol</td>
<td>7</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Framed-IP-Address</td>
<td>8</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Reply-Message</td>
<td>18</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Class</td>
<td>25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor-Specific</td>
<td>26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session-Timeout</td>
<td>27</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Called-Station-ID</td>
<td>30</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Calling-Station-ID</td>
<td>31</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>NAS-Identifier (if configured in BBSM)</td>
<td>32</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Acct-Status-Type</td>
<td>40</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Acct-Input-Octets</td>
<td>42</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acct-Output-Octets</td>
<td>43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acct-Session-ID</td>
<td>44</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Acct-Session-Time</td>
<td>46</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acct-Input-Packets</td>
<td>47</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acct-Output-Packets</td>
<td>48</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acct-Terminate-Cause</td>
<td>49</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAS-Port-Type</td>
<td>61</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Table 14-2  RADIUS Attribute Descriptions

<table>
<thead>
<tr>
<th>Attribute</th>
<th>No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-Name</td>
<td>1</td>
<td>The end user enters this name to authenticate against the RADIUS server and access the Internet through BBSM.</td>
</tr>
<tr>
<td>User-Password</td>
<td>2</td>
<td>The end user enters this password to authenticate against the RADIUS server and access the Internet through BBSM. The password is encrypted before being sent to the RADIUS server.</td>
</tr>
<tr>
<td>NAS-IP-Address</td>
<td>4</td>
<td>Either the IP address of the BBSM external NIC or the IP address entered as the NAS IP address on the WEBconfig RADIUS Server web page.</td>
</tr>
<tr>
<td>NAS-Port</td>
<td>5</td>
<td>The NAS-Port value is a numeric value (therefore the leading zeros of the site number are dropped). BBSM maps the NAS-Port attribute as the following: \textit{aaaabbcddd}, where \textit{aaa} = site number, \textit{bb} = cluster, \textit{cc} = switch, and \textit{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.</td>
</tr>
<tr>
<td>Service-Type</td>
<td>6</td>
<td>The number 2 in this field indicates \textit{Framed}.</td>
</tr>
<tr>
<td>Framed-Protocol</td>
<td>7</td>
<td>The number 1 in this field indicates \textit{PPP} (point-to-point protocol). For historical reasons, BBSM sends 1 in this attribute even though clients do not usually use PPP.</td>
</tr>
<tr>
<td>Framed-IP-Address</td>
<td>8</td>
<td>IP address of client connecting to the Internet through BBSM.</td>
</tr>
<tr>
<td>Reply-Message</td>
<td>18</td>
<td>If this attribute is included in the access-accept packet, BBSM forwards this string to the iPass client using the XML tag, \textit{&lt;AuthenticationReply&gt;}.</td>
</tr>
<tr>
<td>Class</td>
<td>25</td>
<td>Use this attribute to send optional information to the accounting server. If this attribute is included in the access-accept packet, BBSM sends this information unmodified to the accounting server.</td>
</tr>
<tr>
<td>Vendor-Specific</td>
<td>26</td>
<td>The end-user bandwidth (in kbps). You can use the bandwidth vendor-specific attribute (VSA) in two different scenarios:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- VSA sent from the RADIUS server to BBSM—In this scenario, BBSM is configured to use the RADIUS or RADIUSClear page set and the end user logs on. The RADIUS server sends the bandwidth VSA to BBSM in an access-accept packet. BBSM reads the VSA, and if the Bandwidth Throttle check box in WEBconfig is checked (bandwidth enabled), BBSM throttles the end user to that speed. The VSA is not sent back to the RADIUS server in the accounting packets. For setting the Bandwidth Throttle option, refer to Chapter 9, “Changing the Internal Network IP Address Ranges.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- VSA sent from BBSM to the RADIUS server—In this scenario, BBSM is configured to use the RADIUSUBand or RADIUSUBandClear page set. If the Bandwidth Throttle check box in WEBconfig is checked (bandwidth enabled), the bandwidth choice is displayed on the Start page and the end user selects a bandwidth and logs on. BBSM throttles the user to the chosen speed and sends the bandwidth VSA in all accounting packets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following is the format for the BBSM bandwidth VSA:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Type = 26</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Length (bytes) = 12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Vendor-ID = 5263</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Vendor-type = 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Vendor-length (bytes) = 6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vendor-string (kbps) = Specified bandwidth, such as 256</td>
</tr>
</tbody>
</table>
Configuring RADIUS Server Options

Follow this procedure to configure the RADIUS server billing options.

This procedure assumes that you have already run the Switch Discovery Wizard to configure the ports to use either the RADIUS page set or a custom page set. (Refer to the “Running the Switch Discovery Wizard” section on page 5-6.)

### Table 14-2 RADIUS Attribute Descriptions (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session-Timeout</td>
<td>27</td>
<td>If this attribute is included in the access-accept packet, BBSM terminates the session after the number of Session-Timeout seconds unless the session has terminated earlier for another reason.</td>
</tr>
<tr>
<td>Called-Station-Id</td>
<td>30</td>
<td>The MAC address of the BBSM internal NIC. The string is a sequence of 12 hexadecimal characters.</td>
</tr>
<tr>
<td>Calling-Station-Id</td>
<td>31</td>
<td>The MAC address of the client (end-user) NIC.</td>
</tr>
<tr>
<td>NAS-Identifier</td>
<td>32</td>
<td>The NAS Identifier value entered on the WEBconfig RADIUS Server web page. If no value is entered in this field, BBSM does not include this attribute in the RADIUS Access-Request packet.</td>
</tr>
</tbody>
</table>
| Acct-Status-Type | 40  | The number contained in this field indicates one of the following types of Accounting-Request packets:  
  1 = Start Accounting-Request  
  2 = Interim-Update Accounting-Request  
  3 = Stop Accounting-Request |
| Acct-Input-Octets | 42  | The number of octets (bytes) that BBSM received from the end user during the session. |
| Acct-Output-Octets | 43  | The number of octets (bytes) that BBSM transmitted to the end user during the session. |
| Acct-Session-Id | 44  | The unique Session ID assigned to each BBSM end-user session used to identify all authentication and accounting messages generated for one user session. |
| Acct-Session-Time | 46  | The number of seconds for which the end user received service. |
| Acct-Input-Packets | 47  | The number of packets that BBSM received from the end user during the session. |
| Acct-Output-Packets | 48  | The number of packets that BBSM transmitted to the end user during the session. |

### Configuring the RADIUS Server Options

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

**Step 2** In the NavBar, navigate to the RADIUS Server web page by choosing **Billing > RADIUS > Server**. The RADIUS Servers web page appears. (See Figure 14-1.)
Step 3 Configure the RADIUS server parameters, as described in Table 14-3 and click Save.

Note Install a server SSL certificate to enable secure connections between client sessions and the BBSM server. Refer to the “Installing an SSL Certificate” section on page 16-2.
### Table 14-3  RADIUS Server Web Page Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Enter the unique DNS name or IP address of the RADIUS server. The DNS name can contain a maximum of 64 characters.</td>
</tr>
<tr>
<td>Secret</td>
<td>Enter the RADIUS client password used to access the RADIUS server.</td>
</tr>
<tr>
<td>Timeout (in seconds)</td>
<td>Enter the number of seconds that the BBSM server waits before attempting to access the RADIUS server a second or third time or before going to the next RADIUS server. BBSM attempts to contact each RADIUS server three times before attempting to contact the next RADIUS server. The default for this setting is 5 seconds.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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 Server Timeout period and more than one RADIUS server is unavailable, the total time period during which BBSM attempts to contact the RADIUS servers may be greater than the timeout period for the browser itself. 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 attempts to contact the first RADIUS server three times within 60 seconds. If BBSM cannot contact the first RADIUS server, it tries to contact the second server three times, again within 60 seconds. However, because the timeout period for IIS is 90 seconds, the browser will time out before BBSM finishes searching for the second RADIUS server.</td>
</tr>
<tr>
<td>Rank</td>
<td>Enter the order in which the BBSM server attempts to contact the RADIUS servers. The first server to be contacted is the lowest ranked server, the second server to be contacted is the next ranked server; and so on. For example, if two RADIUS servers are configured with rank 30 and 31, server 30 will be contacted first, then 31 will be contacted. The default is 30.</td>
</tr>
<tr>
<td>NAS IP Address</td>
<td>If the BBSM server is behind a NAT router, enter the public IP address that the router assigned to the BBSM server. (Changing this IP address for one RADIUS server changes it for all previously configured RADIUS servers. If the field is left blank, the RADIUS access policy uses the IP address of the external NIC.)</td>
</tr>
<tr>
<td>NAS Identifier</td>
<td>Enter a unique server identifier, such as “BBSMServer1.” The RADIUS access policy uses this NAS identifier when sending authentication or accounting packets to the RADIUS server. If the field is left blank, the attribute is not sent.</td>
</tr>
<tr>
<td>RADIUS Accounting Interim Interval</td>
<td>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.</td>
</tr>
<tr>
<td>Enable Authentication</td>
<td>Check to enable BBSM to verify the username and password with a RADIUS Authentication server (Authentication Access-Request message).</td>
</tr>
<tr>
<td>Using Port</td>
<td>Enter the TCP port on the BBSM server that the RADIUS server uses to communicate with the RADIUS authentication server. The default is 1645.</td>
</tr>
<tr>
<td>Enable Accounting</td>
<td>Check to enable BBSM to contact the RADIUS Accounting server to log the Start, Interim-Update Accounting, and Stop accounting messages.</td>
</tr>
<tr>
<td>Using Port</td>
<td>Enter the TCP port on the BBSM server that the RADIUS server uses to communicate with the RADIUS accounting server. The default is 1646.</td>
</tr>
</tbody>
</table>
You can enable RADIUS to support multiple sessions on a single RADIUS account at one time. Follow this procedure to configure multiple concurrent RADIUS sessions.

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

**Step 2**
In the NavBar, navigate to the RADIUS Site web page by choosing Billing > RADIUS > Site x. The Site x web page appears. (See Figure 14-2.)

**Figure 14-2 RADIUS Site Web Page**

**Step 3**
To enable a RADIUS user to have a BBSM session active on more than one computer at the same time, check the **Allow multiple concurrent RADIUS sessions** check box. Leave it unchecked to prevent multiple computers from using the same RADIUS account at the same time. Click **Save**.
Configuring Credit Card Billing

If you are using credit card billing, you must configure a credit card authorization server by using the Credit Card Server web page on WEBconfig. This section also describes how to enter the merchant ID for each site and test the credit card interface.

As of BBSM 5.3, the credit card policy changes. Previously, the policy would terminate the user's session when he or she exceeded the authorization amount. (The authorization amount defaults to $10.00.) Now, the end user is never disconnected, even if he or she exceeds the authorization amount.

You must modify the approval amount to meet your needs. Most credit card companies, including the CyberSource billing server that is used on BBSM, do not allow charges to be posted in excess of the approval amount. If you are charging $0.50 per minute and your average user stays online for 30 minutes, you probably want to use about $30 to $50 for your approval amount so the charges will post even for above average users. The approval amount is the most you can charge one user for his or her Internet session.

The approval amount is set in the page. For instructions on modifying this value, refer to the Cisco BBSM 5.3 SDK Developer Guide.
Configuring the Credit Card Server Options

Follow this procedure to configure the credit card billing options.

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

**Step 2** In the NavBar, navigate to the Credit Card Servers web page by choosing **Billing > Credit Card > Server**. The Credit Card Servers web page appears. (See Figure 15-1.)

**Figure 15-1 Credit Card Servers Web Page**

![Credit Card Servers Web Page]

**Step 3** Configure the credit card options, as described in Table 15-1 and click **Save**.

**Table 15-1 Credit Card Server Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Billing Server</td>
<td>Enter the IP address or FQDN for the credit card server.</td>
</tr>
<tr>
<td>Connect Timeout</td>
<td>Enter the number of seconds during which BBSM attempts to connect to the credit card server. The default is 30 seconds.</td>
</tr>
</tbody>
</table>

**Buttons**

<table>
<thead>
<tr>
<th>Defaults</th>
<th>Displays the default parameter settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requery</td>
<td>Refreshes the web page (click before saving changes).</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the changes made to the web page.</td>
</tr>
</tbody>
</table>
Entering the Merchant ID

If you are using credit card billing, you must specify the merchant ID for the credit card server by using the Credit Card Site web page. Follow this procedure to enter this ID.

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

**Step 2**
In the NavBar, navigate to the Credit Card Server web page by choosing **Billing > Credit Card > Site x**. The Credit Card web page appears. (See Figure 15-2.)

**Figure 15-2 Credit Card Site Web Page**

**Step 3**
Enter the merchant ID and click **Save**. 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 and 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, the merchant ID has to match the name of the key files generated under `c:\opt\ics\keys` directory.
Testing the Credit Card Interface

Follow this procedure to test the credit card interface before deploying BBSM. (BBSM performs credit card authentication and billing through the CyberSource ICS billing server.)

**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 the `c:\opt\ics\keys` directory.
   b.  Enter this command: `Ecert <merchant ID>`.

See the following example:

```
C:\opt\ics\keys>ecert sclink1
The application will now send the newly created key pair and certificate request to the server.

Merchant id, sclink1
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\sclink1.pwd
Merchant certificate data written to, C:\opt\ics\keys\sclink1.crt
Merchant private key data written to, C:\opt\ics\keys\sclink1.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 **WEBconfig**. The BBSM 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 > Server**.
   b.  In the Billing Server Address field, enter the IP address of the signed credit card server; for example, `ic2test.ic3.com`.
   c.  In the Connect Timeout Seconds field, enter the number of seconds that the credit card attempts to validate a credit card before rejecting the end user’s input and click **Save**.

**Step 6**  Enter the currency type:
   a.  On WEBconfig, click **BBSM Server Settings**. The BBSM Server Settings web page appears.
b. From the drop-down menu, enter the local currency type that the credit card server uses. The default is USD and click **Save**.

**Step 7** Enter the merchant ID:

a. Navigate to the Credit Server web page by choosing **Billing > Credit Card > Site x**.

b. In the Merchant ID field, enter the merchant ID and click **Save**.

**Step 8** Choose the appropriate page set—Minute ICS or MinuteICSClear:

a. Navigate to the **Access Points** or **Switches** web page (depending on you usage) by choosing **Network Elements > Access Points (or Switches) > Site x**.

b. To access the Network Element Port Settings pop-up window, click Port Settings.

c. From the Page Set drop-down menu, choose **MinuteICS** or **MinuteICSClear**:
   - If you have SSL installed, choose **MinuteICS**.
   - If you do not have SSL installed, choose **MinuteICSClear**.

d. Click **Save**.

**Step 9** From a laptop, verify that you can access the Internet through the Credit Card page:

a. On a client connected to BBSM, open the browser. The Credit Card window appears.

b. Enter names and addresses. Each field on the form must be filled in, although the data does not have to be real.

c. For the Credit card number, enter **4111111111111111** (the number 4 followed by 15 ones)

d. For the expiration date, enter **2005**.

e. Click **Submit**. You will soon be connected to the Internet. When you have accessed the Internet, browse for 2 minutes and then disconnect.

**Step 10** Verify successful transactions on the CyberSource side:

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

a. Use your merchant ID and password to login.

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

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

This chapter provides an overview of BBSM security, the procedure to install an SSL certificate when it is required, and the procedure to configure secured sockets layer (SSL). It also provides the procedure for changing the MSDE username and password and creating or changing the BBSD and Web API account username and password.

Refer to these sections:
- Security Overview, page 16-1
- Installing an SSL Certificate, page 16-2
- Configuring Security, page 16-16

Security Overview

Although BBSM is not a security product, you can increase the security of your system by using the security components described in this section.

BBSM can be made secure in the following ways:

- Microsoft server security—BBSM operates on the Windows 2000 server operating system and includes the basic Microsoft server security. The default BBSM configuration ships with settings configured to enhance its security. Microsoft Networking (File and Print Sharing and Local NetBIOS) is disabled on both the internal and external interfaces of the BBSM server, which means that from the client to the server, only a few ports on BBSM are open to a client connection.

- Password protected with permission levels—The BBSM management interface is password protected with three different user privilege levels.

- For security reasons, the BBSM internal interface does TCP filtering by port. Only the following ports are open on the internal interface:
  - 23: Telnet
  - 80: HTTP
  - 443: HTTPS (SSL traffic)
  - 9488: Used internally by BBSM
  - 8000, 8080, 8888: Common ports for nonstandard proxy
• Anti-virus protection—BBSM can also be protected by installing McAfee NetShield anti-virus software. For information on installing and configuring McAfee NetShield on BBSM, refer to this website:
  

• Firewalls—Cisco recommends that you configure the firewall features available on the router by using access control lists. For added security, you can protect BBSM by using Cisco PIX firewalls.

• Additional security features—BBSM can also be configured with additional static routing filters to provide security for broadcasts, and you can implement a secure encrypted remote control application for remote management. The router that is installed on the property should also be configured with broadcast thresholds.

The security of the inside LAN must be provided by configuring the in-building LAN infrastructure. This configuration prevents one room from seeing another room’s packets, which eliminates attacks between clients and prevents malicious users from stealing authentication information when a session is being initiated. This configuration consists of horizontal protection that prevents clients from seeing other client traffic and vertical protection that prevents clients from seeing client traffic on another switch.

The configuration uses these features to provide protection:

• Port-to-port security (the protected port feature)— This feature prevents clients on two different ports from seeing each other without a Layer 3 device to intervene. It is supported on various Cisco Catalyst switches, such as the Catalyst 2900 XL, 2950, and 3550 switches. Because Cisco frequently adds new switches, this feature may also be supported on them.

• Private VLANs—On Cisco Catalyst 4000 and 6500 series switches, this feature provides Layer 2 isolation between ports within the same private VLAN.

• Publicly secure packet forwarding (PSPF)—On Cisco Aironet access points, this feature prevents client devices associated with the access point from communicating with other client devices on the wireless network and inadvertently sharing files. It provides Internet access to client devices without providing the other capabilities of a LAN.

The user’s session is also made secure by configuring the page set for SSL, which provides RADIUS or credit card security from the end user’s client to BBSM. When SSL is implemented, the end user’s authentication is secure from end to end. Refer to the following section on installing an SSL certificate.

Installing an SSL Certificate

This section describes how to install an SSL certificate on the BBSM server. The certificate is needed when end users will be entering sensitive data on the Connect page, such as credit card numbers or RADIUS account information. (When SSL encryption is used, the end user connects to the Internet using https instead of http.)

If you are using SSL encryption, you must use page sets that provide the SSL encryption protocol. The other default BBSM page sets transmit data in clear text.
Before You Start

Before you install the SSL certificate, read the following:

- You must purchase a fully qualified domain name (FQDN) for the BBSM server before you can purchase a Secure Server Digital ID (certificate). You cannot use a name purchased for another server. The name can be purchased from any domain name vendor; for example, you can purchase a name from VeriSign by going their website:
  
  http://www.verisign.com

  Go to the company’s website and follow its instructions for purchasing the name.

- 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.

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

- BBSM requires the use of 128-bit SSL encryption.

Caution

Because page sets whose names end in Clear do not use SSL security, Cisco does not recommend using them in production to transmit data to the BBSM server. (See Table 18-1.) The end user’s browser transmits RADIUS and credit card information to BBSM in clear text. BBSM provides them for demonstration and testing situations in which installing a server certificate is not feasible.

Generating a Certificate Signing Request

Follow this procedure to generate a Certificate Signing Request for your web server certificate. The BBSM administrator should perform this procedure. (BBSM servers use Microsoft IIS 5.0.)

Step 1  From the BBSM desktop, choose Start > Programs > Administrative Tools > Internet Services Manager. The Internet Information Services window appears.

Step 2  In the left pane, click the server name. The server folders appear in the right pane.

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.

Step 5  In the Secure communications section, click Server Certificate. The Welcome to the Web Server Certificate Wizard dialog box appears. (See Figure 16-1.)
Installing an SSL Certificate

Figure 16-1 Welcome to the Web Server Certificate Wizard Dialog Box

Welcome to the Web Server Certificate Wizard

This wizard helps you create and administer server certificates used in secure Web communications between your server and a client.

Status of your Web server:
Your Web Server doesn't have a certificate installed, and you don't have any pending requests.
Certificate Wizard will help you to create a new certificate for this Web Server or attach to an existing certificate.

To continue, click Next.

Step 6 Click Next. The Server Certificate dialog box appears. (See Figure 16-2.)

Figure 16-2 Server Certificate Dialog Box

Select the method you want to use for this web site:
- Create a new certificate.
- Assign an existing certificate
- Import a certificate from a Key Manager backup file.

Step 7 Verify that the Create a new certificate radio button is selected. If it is not, click it and then Next. The Delayed or Immediate Request dialog box appears. (See Figure 16-3.)
Figure 16-3  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, click it, and then click **Next**. The Name and Security Settings dialog box appears. (See Figure 16-4.)

Figure 16-4  Name and Security Settings Dialog Box

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

Step 10  In the Bit length drop-down menu, keep the default setting and click **Next**. The Organization Information dialog box appears. (See Figure 16-5.)
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 16-6.)
Step 13  In the Common name field, enter your website’s common name and click Next. The Geographical Information dialog box appears. (See Figure 16-7.) This is the name that is entered on the Security/SSL page in WEBconfig. Refer to Step 3 of the “Configuring Security” section on page 16-16.

Note  When you enter your website’s common name, 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 16-7  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 16-8.)

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.
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. Cisco recommends 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 16-9.)

Figure 16-8 Certificate Request File Name Dialog Box

![Certificate Request File Name Dialog Box](image1)

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. Cisco recommends 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 16-9.)

Figure 16-9 Request File Summary Dialog Box

![Request File Summary Dialog Box](image2)
Step 17 Verify that the information is correct and click **Next**. The Completing the Web Server Certificate Wizard dialog box appears. (See Figure 16-10.)

*Figure 16-10 Completing the Web Server Certificate Wizard Dialog Box*

![Completing the Web Server Certificate Wizard](image)

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 server.

---

**Purchasing a Secure Server ID from a Certificate Authority**

After generating the Certificate Signing Request on BBSM, you must purchase a Secure Server Digital ID (certificate) from a certificate authority (CA). This authenticates your website and enables the SSL encryption.

Step 1 Purchase a certificate from a CA; for example, you can purchase the certificate from VeriSign on their website:

http://www.verisign.com

Follow the company’s instructions for purchasing the certificate. (BBSM requires 128-bit encryption.)

Step 2 To verify that your organization’s legitimacy and registration with the proper government authorities, you must provide the CA with your company’s Dun & Bradstreet DUNS number. If you do not have a DUNS number, contact Dun & Bradstreet.

Step 3 At some point during enrollment, you will be asked to use a text editor, such as Windows Notepad, to open the CSR text file (c:\certreq.txt) that you created in the previous section.
Chapter 16  Configuring Security and SSL

Installing an SSL Certificate

Step 4  When prompted, 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-----
MIIBCTBtAIBABdBMQswCQYDVQQGEwJVUzEQQMA4GA1UECBMHcmxvcm1kYTEYMBYGY
A1UEChMPRkX1lcByBvbiBUaGU2MDQwEgYDVQQDDDA0MBsGAYGAIwDQYJKoZIhvcngC
v1FhZzYlLOQa090JtmnIWsQRHh0yDS+45oncjKm1zCG/I2AgMAAAGgADANBgkq
hkiG9w0BAQQFAANBAAAA9g+NiUh5YWrFQntG4iuDa/wqUshtpJy4PjdsD3ugy
5avuh3G/1PqGh2aXYIjHptJXfUBQzzSEINYtc=
-----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 you submit your completed application, your domain’s Technical and Organizational Contacts will receive an email 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 server.

Follow this procedure to install the granted certificate onto your BBSM server.

Step 1  Choose Start > Programs > Administrative Tools > Internet Services Manager. The Internet Information Services (IIS) window appears.

Step 2  In the tree in the left pane, click the server name.

Step 3  In the right pane, right-click Default Web Site, and select Properties. The Default Web Site Properties dialog box appears.


Step 5  In the Secure Communications pane, click Server Certificate. The Welcome to the Web Server Certificate Wizard window appears. (See Figure 16-1.)

Step 6  Click Next. The Pending Certificate Request dialog box appears. (See Figure 16-11.)
Step 7  Verify that the **Process the pending request and install the certificate** radio button is selected. If it is not, select it and click **Next**. The Process a Pending Request dialog box appears. (See Figure 16-12.)

**Figure 16-12 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 server at the beginning of this procedure, and then click **Next**. The Certificate Summary dialog box appears. (See Figure 16-13.)
Installing an SSL Certificate

Note
You cannot reinstall this certificate on a different machine.

Figure 16-13 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 16-14.)

Figure 16-14 Completing the Web Server Certificate Wizard Dialog Box
You now have a server certificate installed. You may want to test the website 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**

If your BBSM server becomes damaged or needs to be rebuilt, you will need to reinstall a backup of your server certificate onto your BBSM server. The following procedures explain how to manage certificates, export them (create backups), and import them (reinstall them) at a later date, if necessary, by using the Windows-based Microsoft Management Console (MMC) application snap-ins. (MMC is included in the Windows 2000 operating system and also runs in Windows 95, 98, and NT 4.0. It is part of the Microsoft Platform SDK and available for general use.)

MMC provides a GUI and programming framework in which consoles, which are collections of administrative tools, can be created, saved, and opened. It also provides an environment for running management applications and administrative tools (snap-ins). Their primary purpose is to perform management tasks and enable administrators and other users to create custom management tools 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. 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.

**Creating an MMC Snap-in for Managing Certificates**

To perform the backup, you must first create a new MMC and add the Certificates snap-in, as follows. Adding the snap-in enables you to work with any certificates in your computer’s certificate store. You can also add the snap-in to another MMC as long as MMC is opened in Author mode.

**Step 1**
From the BBSM 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**
Choose **Certificates** and click **Add**. The Certificates snap-in window appears.

**Step 7**
Click the **Computer account** radio button and then **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. Click **Close**.

**Step 9**
From the Add/Remove Snap-in window, click **OK**. The Console1 and Console Root windows appear.

**Step 10**
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 later on a damaged or rebuilt BBSM server. Now that you have added the Certificates snap-in, follow the procedure below to export the key pair that your web server is using.

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 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 choose 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 creates a PFX file.

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

Step 7
Choose a file name for saving the file. Do not include an extension in your file name. The wizard adds the suffix automatically. Click Next.

Step 8
Read the summary. Pay special attention to the location where the file is being saved. 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. Move this file to a floppy disk and store it in a secure location.

Importing a Server Certificate in IIS 5.0

This section describes how to reinstall a copy of the server certificate onto a BBSM server. To complete the process, 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 server at a later time.
To create an MMC snap-in to manage certificates, use the same procedure that is described in the “Creating an MMC Snap-in for Managing Certificates” section on page 16-13. After you create a new MMC and add the Certificates snap-in with this procedure, you can import the server certificate into your computer’s certificate store using the procedure below.

**Step 1**
From the Console Root window, open the Certificates (Local Computer) snap-in, navigate to **Personal**, and then to **Certificates**.

**Note**
No certificates are listed when no certificates 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 window showing what the wizard is about to do. If this information is correct, click **Finish**.

The server certificate for your web server is now located in the list of Personal Certificates. 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**
A screen showing the contents of your computer’s personal certificate store appears. Select your web server certificate and click **Next**.

**Step 8**
A summary window showing the certificate details appears. Verify that this information is correct, click **Next**, and then click **OK** to exit the wizard.

You now have an SSL-enabled web server. Be sure to protect your PFX files from any unauthorized personnel.
Configuring Security

You must enable the SSL security and specify the associated domain name by using the Security/SSL web page in WEBconfig. From this web page, you can also access these web pages:

- MSDE sa Account - Change Password Form
- BBSD Account - Change User Form
- Web API Account - Change User Form

Follow this procedure to configure SSL, change the MSDE password, and create (or later change) the BBSD and Web API usernames and passwords.

For additional information about passwords, refer to the “Entering Security Passwords” section on page 3-2.

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

**Step 2** In the NavBar, click **Security/SSL**. The Security/SSL web page appears. (See Figure 16-15.)

---

**Figure 16-15 Security/SSL Web Page**

![Security/SSL Web Page](image)
Step 3 Enter data based on the information shown in Table 16-1 and click Save.

**Table 16-1 Security/SSL Web Page Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Domain Name for SSL Page Sets</td>
<td>Check if you want to use SSL-enabled page sets. <strong>Note</strong> You must purchase a fully qualified domain name for the BBSM server to use SSL security. Refer to “Installing an SSL Certificate” section on page 16-2.</td>
</tr>
<tr>
<td>Full Domain Name</td>
<td>Enter the full domain name for the BBSM server that page sets will use to reach the BBSM server. This domain name must match the name on the SSL certificate that is installed on BBSM, such as cisco.com. This is the name entered in “Installing an SSL Certificate” section on page 16-2 (Step 13).</td>
</tr>
<tr>
<td>MSDE System Administrator (sa), Change</td>
<td>Click <strong>Change</strong> to access the MSDE ‘sa’ Password Form and change the password. (For additional information about BBSM passwords, refer to the “Entering Security Passwords” section on page 3-2.)</td>
</tr>
<tr>
<td>BBSD Account, Create (or Change)</td>
<td>Click <strong>Create</strong> to access the BBSD Account - Create User Form and create a BBSD username and password. Click <strong>Submit</strong> to enter the data. A confirmation dialog box appears. To ensure that only one BBSD account exists, the new account replaces the previous account so you are given the option to cancel. (These alerts appear only if the username is changed. If only the password is changed, the alert is not displayed.) The <strong>Create</strong> button on the Security/SSL web page now reads <strong>Change</strong>. When you click the Change button and the window pops up, the username is now filled in. (The username can be changed.) (For additional information about BBSM passwords, refer to the “Entering Security Passwords” section on page 3-2.)</td>
</tr>
<tr>
<td>Web API Account, Create (or Change)</td>
<td>Click <strong>Create</strong> to access the Web API Account - Create User Form and create a Web API username and password. Click <strong>Submit</strong> to enter the data. A confirmation dialog box appears. To ensure that only one Web API account exists, the new account replaces the previous account so you are given the option to cancel. (These alerts appear only if the username is changed. If only the password is changed, the alert is not displayed.) The <strong>Create</strong> button on the Security/SSL web page now reads <strong>Change</strong>. When you click the Change button and the window pops up, the username is now filled in. (The username can be changed.) (For additional information about BBSM passwords, refer to the “Entering Security Passwords” section on page 3-2.)</td>
</tr>
</tbody>
</table>

**Buttons**

<table>
<thead>
<tr>
<th>Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requery</td>
<td>Refreshes the web page (click before saving changes).</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the changes made to the web page.</td>
</tr>
</tbody>
</table>
Configuring Bandwidth Management

This chapter describes bandwidth management, including bandwidth throttling and bandwidth reservation. It provides the procedure for creating, configuring, and managing access codes, which are alphanumeric strings that BBSM generates for end users to access the Internet:

- Bandwidth Reservation Overview, page 17-1
- Configuring Bandwidth Throttling, page 17-3
- Configuring Bandwidth Reservation, page 17-3
- Creating and Configuring Access Codes, page 17-8

As of BBSM 5.2, BBSM supports the new bandwidth reservation feature, as well as the bandwidth throttling feature used in previous releases. These features are explained below:

- Bandwidth throttling—The specified bandwidth is a maximum bandwidth. Clients receive no more than the specified bandwidth.
- Bandwidth reservation—Clients in the reservation pool share the specified minimum bandwidth. Instead of using Quality of Service (QoS), bandwidth is reserved by using the Cisco IOS Class-Based Shaping feature. For additional information about Class-Based Shaping, go to the following website:
  
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/clsbsshp.htm

Bandwidth Reservation Overview

This section provides an overview of bandwidth reservation. Refer also to each section for detailed information about that configuration procedure.

With bandwidth reservation, hotel customers can reserve bandwidth for meetings that require broadband access. When hotel customers reserve meeting rooms, they can specify bandwidth for their meeting. During the meeting when guests are logged in, the reserved bandwidth is available only to meeting room guests.

Being able to reserve bandwidth provides several specific advantages to the hotel:

- An added source of revenue—Because the hotel can provide a range of bandwidths, it can offer a tiered pricing structure to meeting room customers.
- More efficient use of hotel Internet bandwidth—Guests use the Internet primarily in the evening. During the day, hotel bandwidth is usually underused and can generate additional meeting room revenue.
Hotels wanting to use the bandwidth reservation feature do not need to buy any additional bandwidth. Instead, they can re-allocate their existing bandwidth. For example, if a hotel has 1000 kbps allocated for guest use, a bandwidth reservation of 200 kbps would decrease the total amount of bandwidth available for general guest use to 800 kbps. However, reservations do not actually decrement the total hotel bandwidth unless someone is logged into the reservation. As soon as the last person using the reserved bandwidth logs out, the bandwidth is available again for guest use.

It is important not to oversubscribe the network. If the full amount of bandwidth were reserved, no bandwidth would be left for hotel guests. Each hotel must determine how much bandwidth it wants to provide for its guests and weigh that against the increased revenue potential of the bandwidth reservation system.

### What Bandwidth Reservation Adds to Your Router

In some cases, the external router is managed by a service provider who may be concerned about the configuration that BBSM adds to the router. If you are working with an ISP who needs more information about what the bandwidth reservation feature adds to the router, this section describes the router configuration in more detail. Note that no BBSM bandwidth reservation commands are ever entered manually on the router; BBSM adds them automatically when the bandwidth reservation feature is used.

Bandwidth reservation uses the IOS Class-Based Shaping feature to configure the router. Refer to the following website for documentation about Class-Based Shaping:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/clsbsshp.htm

The configuration added to the router consists of a policy map, several class maps (one for each class of service), and one extended access list for each class map. Some parts of the configuration are static, and some are dynamic, as follows:

- **Static**—The policy map is the static part of the configuration.
- **Dynamic**—Class maps and extended access lists are created dynamically as users log in to the reservations. When the last user logs out of a reservation, the class map and extended access list for that reservation are deleted from the running configuration.

None of the configuration is stored in permanent memory (NVRAM). It is only kept in the running configuration. If you reload the running configuration, you erase the bandwidth reservation configuration.

All of the configuration settings on the router contain the string *BBSM*. If you want to test the bandwidth reservation feature, first create a reservation. (Refer to the “Creating and Configuring Access Codes” section on page 17-8.) Then log into BBSM as an end user using an access code. Now Telnet to your external router and view the running configuration. Look for the BBSM string. The policy map, class maps, and extended access lists all have names that include this string. As mentioned earlier, when you deactivate the client session, the dynamic part of the configuration is removed. You can always reload the running configuration on the router to restore the previous configuration.
Configuring Bandwidth Throttling

The bandwidth throttling feature enables end users to choose a bandwidth when they connect. Bandwidth throttling enables you to control the maximum bandwidth that you allocate to end users on a per-port basis.

If you are using the AccessCode and MeetingRoom page sets, you can control bandwidth by choosing an Access Codes Bandwidth option—bandwidth disabled, throttling, or reservation—on the WEBconfig BBSM Server Settings web page. The options for this web page are described in Chapter 17, “Configuring Bandwidth Management.”

This section repeats the procedure to configure bandwidth throttling.

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

**Step 2** In the Bandwidth Management area, verify that you chose Throttling in the Access Codes Bandwidth field. This option enables bandwidth throttling. (If you choose None, bandwidth management is disabled.)

**Step 3** To reserve bandwidth, follow the procedure in the “Creating and Configuring Access Codes” section on page 17-8.

---

Configuring Bandwidth Reservation

The bandwidth reservation feature enables a property to set aside a specified bandwidth for a meeting room users. When a hotel customer reserves a meeting room, he or she has the option of specifying a bandwidth reservation for the meeting. At the time of the meeting, this bandwidth is available only to meeting room users, not for general usage. You must configure the bandwidth reservation option on the Bandwidth Reservation web pages in WEBconfig.

To configure bandwidth reservation, you must configure the following:

- The bandwidth management Reservation option on the BBSM Server Settings web page
- The external router
- The total property bandwidth
- The classes of service

The sections that follow describe how to configure these options.

---

Verifying the External Router

Follow this procedure to verify the external router for bandwidth reservation. Cisco recommends using a Cisco 2600 router. You must have Cisco IOS Release 12.1(2)T or later. Other routers may support this feature depending on the IOS version installed. Please consult the Cisco website for the full capabilities of your particular router and Cisco IOS software version.

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

**Step 2** In the Bandwidth Management area, verify that you chose Reservation in the Access Code Bandwidth field. This option enables bandwidth reservation for access codes.
Step 3  In the NavBar, navigate to the External Router web page by choosing Bandwidth Reservation > External Router. The External Router web page appears. (See Figure 17-1.)

**Figure 17-1  Bandwidth Reservation External Router Web Page**

![Bandwidth Reservation External Router Web Page](image)

**Step 4**  Enter the external router options based on the information shown in Table 17-1 and click Save.

### Table 17-1  External Router Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address for the external router.</td>
</tr>
<tr>
<td>Telnet ‘terminal’ Password</td>
<td>Enter the terminal password, as configured in IOS on the router (Telnet password).</td>
</tr>
<tr>
<td>IOS ‘enable’ Password</td>
<td>Enter the enable password, as configured in Cisco IOS on the router.</td>
</tr>
<tr>
<td>BBSM Router Interface</td>
<td>After you enter the correct passwords and click Save, the Router Interface field appears with the name of the BBSM router interface.</td>
</tr>
</tbody>
</table>

**Buttons**

- Restore Router Configuration: Restores the BBSM bandwidth reservation policy map to the router’s running configuration. Because BBSM does not write its configuration to the router’s memory, if the router is reset, the BBSM reservation settings are lost. To restore these settings, click this button. The static policy map is restored. The dynamic user information is not. Users need to reauthenticate to rejoin their reservation.

- Requery: Refreshes the web page (click before saving changes).

- Save: Saves the changes made to the web page.
Configuring the Total Bandwidth

Follow this procedure to configure the total bandwidth.

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

**Step 2**
In the NavBar, navigate to the Total Bandwidth web page by choosing **Bandwidth Reservation > Total Bandwidth**. The Total Bandwidth web page appears. (See **Figure 17-2**.)

**Figure 17-2  Bandwidth Reservation Total Bandwidth Web Page**

**Step 3**
Configure the bandwidth options based on the information shown in **Table 17-2** and click **Save**.
Configuring Bandwidth Reservation

Table 17-2 Total Bandwidth Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective Date</td>
<td>From the drop-down menus, choose the date that the total bandwidth setting takes effect at the property:</td>
</tr>
<tr>
<td></td>
<td>- The first date that you enter is always the date when you begin using bandwidth reservation.</td>
</tr>
<tr>
<td></td>
<td>- Subsequent dates are the scheduled dates when you will begin offering bandwidth changes.</td>
</tr>
<tr>
<td></td>
<td>The bandwidth setting remains in effect until another date begins.</td>
</tr>
<tr>
<td>Note</td>
<td>If you choose a date to decrease bandwidth, reservations already made for dates in this time period of decrease will be deleted.</td>
</tr>
<tr>
<td>Total Property Bandwidth</td>
<td>From the drop-down menu, choose the full bandwidth at the property, or choose Enter your bandwidth and enter a bandwidth.</td>
</tr>
<tr>
<td>Minimum Guest Bandwidth</td>
<td>Enter the minimum bandwidth for all users that are not in a reservation. This number will be subtracted from the Total Bandwidth to determine the bandwidth that is available for reservations. This must be a multiple of 8 kbps.</td>
</tr>
</tbody>
</table>

Buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Creates another entry when you are installing additional bandwidth or removing bandwidth. (You can have many bandwidth entries.) A blank web page appears so the new total bandwidth entry can be configured.</td>
</tr>
<tr>
<td>Requery</td>
<td>Refreshes the web page (click before saving changes).</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the changes made to the web page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the total bandwidth entry.</td>
</tr>
</tbody>
</table>

Configuring Classes of Service

Classes of service are configured using the Bandwidth Reservation Classes of Service web page. This page is optional because BBSM ships with several default classes of service. Use this page to add, modify, or delete classes of service.

BBSM creates bandwidth classes of service that correspond to levels of Internet service. In a particular day, several different bandwidth reservations can exist that are composed of different classes. For example, if a hotel set aside 500 kbps for meeting room bandwidth reservations, it could define three classes of service—300 kbps, 200 kbps, and 100 kbps. Notice that the total bandwidth exceeds the maximum of 500 kbps, so BBSM does not allow all three classes of service to be reserved for 1 day to prevent the hotel from reserving unavailable bandwidth. However, the hotel could reserve five reservations at the 100 kbps class on one day and three reservations with one at the 100 kbps class and two at the 200 kbps class the next day. Although the system ensures that no more than 500 kbps can be reserved in 1 day, the classes can be combined in any way to total 500 kbps. The BBSM server uses this method of managing classes rather than QoS because it provides greater flexibility.
After a class of service has been created, you can modify its properties or delete it using the Delete button until the class is used for a reservation. When past or future reservations exist at this class of service, it cannot be deleted. However, it can be disabled to prevent new reservations from being made.

Follow this procedure in this section to configure a class of service.

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

**Step 2** In the NavBar, navigate to the Classes of Service web page by choosing **Bandwidth Reservation > Classes of Service**. The Classes of Service web page appears. (See **Figure 17-3**.)

**Figure 17-3  Classes of Service Web Page**

![Figure 17-3 Classes of Service Web Page](image-url)
Step 3 Configure the bandwidth reservation class of service options based on the information shown in Table 17-3 and click Save.

Table 17-3 Classes of Service Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package name</td>
<td>Enter the name of the class of service. The BBSM operator will use this name when making bandwidth reservations, so descriptive names (such as Gold, Silver, and Bronze or First Class and Second Class) are recommended.</td>
</tr>
<tr>
<td>Bandwidth (in kbps)</td>
<td>For the specified service package (class of service), enter a bandwidth.</td>
</tr>
<tr>
<td>Price</td>
<td>Enter a price per access code. This is the suggested price, which can be changed at the time the reservation is made.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a package description. The description is displayed to the BBSM operator when making reservations, but the customer does not see the description. Use this field to write notes to those making reservations, such as Best service - for use by priority customers only.</td>
</tr>
<tr>
<td>Disable class of service</td>
<td>Check to keep the class of service, but disable it at this time. (If a class of service is disabled, no new reservations can be made with this class.)</td>
</tr>
</tbody>
</table>

Buttons

- **New** Enters a new class of service. A blank web page appears so the new class and options can be added.
- **Requery** Refreshes the web page (click before saving changes).
- **Save** Saves the changes made to the web page.
- **Delete** Deletes this class of service. Classes of service can be deleted only if they are not used for any bandwidth reservations (past or present). To phase out a class of service, disable it first. It can be deleted after 1 year, at which time the system automatically purges old reservations.

Creating and Configuring Access Codes

This section describes how to create access codes and configure them. Before creating and configuring them, you must choose a bandwidth management option on the BBSM Server Settings web page and, if you are using bandwidth reservation, configure reservation on the Bandwidth Reservation web pages. Refer to the “Configuring Bandwidth Reservation” section on page 17-3.

Internet access is purchased in these ways:

- **Specified date range (start and end date and time)**—This specified time period can be paid for when reserving the access code or at the time the access code is used. Only this option (with a specified start and end time) can be used to make reservations because the system could be oversubscribed by access codes specified by duration if too many users logged on at the same time.

- **Specified duration (in minutes, hours, days, or weeks)**—With this feature, access codes are based on duration of usage instead of a specific time period. The feature supports bandwidth throttling and not bandwidth reservation because BBSM would have no way of preventing oversubscribing.
an end user logs onto the Internet using access codes by duration, a disconnect window displays the
time remaining. The time is displayed in minutes only unless the time exceeds 1000 minutes, in
which case it is displayed in hours and minutes. The end user can log out and log in as many times
as he or she wishes. BBSM maintains the total internet usage time, and when the time lapses, the
end user is disconnected. If end users attempt to connect with an access code that has no time left
on it, they are given an error page similar to the page presented to a prepaid RADIUS user with no
time remaining.

This feature applies to exclusive access codes only. If an end user attempts to connect with an access
code tied to a duration and the Connect page specifies that the session should be non-exclusive
(set in the post page), BBSM automatically overrides this setting and forces the session to be
exclusive. If anyone else attempts to log in with that access code, he or she will receive an error page
stating that the access code is already in use.

When an end user finishes using all of their allocated time, BBSM disconnects them and purges the
access code from the system. This puts their access code back into the pool of available codes for
future use. The benefit of this is that it increases the number of codes for use in the future. The
drawback is that if the access code gets used right away, then the previous user might still remember
the code and could potentially steal some internet time from the new user.

These are some other BBSM access code features:

- For auditing purposes, the access code system enables you to view past and future reservations,
  which includes any reserved bandwidth.
- For those access codes that have a specified date range, BBSM stores access codes for 1 year for
  auditing purposes. After that, they are purged from the system so you do not need to delete access
codes.
- The BBSM server does not bill when users log in with access codes. In addition, access code charges
  cannot be sent to a PMS or local printer.

Follow this procedure to create and configure the access codes.

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

**Step 2**
In the Bandwidth Management area, verify that you chose **Throttling or Reservation** in the Access Code
Bandwidth field. This option enables bandwidth throttling or reservation for access codes.

**Step 3**
Click **Dashboard** in the upper right-hand corner and then click **Access Code Management**. The Codes
by Date web page appears. This web page is used to create access codes based on date range. The page
differs, depending on the access codes bandwidth options that you configured on BBSM Server Settings
web page in WEBconfig:

- **None**—If you chose *None* from the Access Codes Bandwidth drop-down menu, the bandwidth
defaults to Full Speed and that is shown in the Manage Codes web page.
- **Throttle**—If you chose *Throttle* from the Access Codes Bandwidth drop-down menu, the Manage
  Codes web page appears as shown in **Figure 17-4** without the Bandwidth Class of Service options.
- **Reservation**—If you chose *Reservation* from the Access Codes Bandwidth drop-down menu, the
  Manage Codes web page appears as shown in **Figure 17-5** with the Bandwidth Class of Service options.

Note the following features of bandwidth reservation:

- You can edit a bandwidth reservation at any time with the calendar user interface in WEBconfig. If
  you need to change the bandwidth for a reservation, you can choose a different class of service
  associated with the reservation before and during the event time.
If you modify the bandwidth during a meeting and users are logged into the reservation, the new bandwidth does not apply to the existing users, but to new end users logging in. This feature enables the hotel to change the bandwidth during a meeting if the system becomes too heavily subscribed.

To access the reserved bandwidth, end users connect to BBSM using an access code that is generated when the user reserves the bandwidth. When the end user makes the reservation, he or she specifies the number of needed access codes (the maximum number is 1000). Because all access codes for a group (reservation) share the reserved bandwidth, bandwidth is reserved per group, not per access code. Larger groups require more bandwidth.

The bandwidth reservation does not correspond to any particular port, so users are not limited to the meeting room. If meeting attendees are also hotel guests, they can use their access codes to log in from their rooms. (This functionality depends on the page set that is available from the guest rooms because not all page sets enable users to enter an access code.) Because access codes are confined to a site (not a port), users at one hotel site cannot travel to another site and connect with the same access code.

**Step 4** Create access codes by using the Codes by Date or Codes by Duration web page:

- If you want to create access codes by date, go to **Step 5**.
- If you want to create access codes by duration, go to **Step 6**.

**Step 5** Configure the options for creating access codes by date range, based on the information shown in Table 17-4 and click **Save**. You have completed the procedure to create access codes by date range.

---

**Note** If you try to modify a reservation while clients for that reservation are connected, bandwidth changes will not apply to these active clients.

**Figure 17-4 Codes by Date Web Page Using the Throttle Option**
Table 17-4 Options for Creating Access Codes by Date Range

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calendar</td>
<td>The calendar section shows you the following information:</td>
</tr>
<tr>
<td></td>
<td>• By scrolling, you can see previous and future months and make reservations by clicking the appropriate dates.</td>
</tr>
<tr>
<td></td>
<td>• From the drop-down menu on the right, you can see reservations for all customers, which is the default, or choose a specific customer’s reservations.</td>
</tr>
<tr>
<td></td>
<td>• As shown in the lower left-hand corner, the calendar is color coded to highlight dates for which reservations have been made.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Today</strong> to highlight the current day and see its reservations.</td>
</tr>
<tr>
<td>Customer</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Displays the chosen calendar and reservation date.</td>
</tr>
<tr>
<td>Site</td>
<td>Displays the site number for the applicable reservation.</td>
</tr>
<tr>
<td>Name</td>
<td>Shows the site name and the percentage of bandwidth used by that reservation. Click the name to recall the reservation details. (The fields at right are populated with the details.)</td>
</tr>
</tbody>
</table>
Chapter 17      Configuring Bandwidth Management

Creating and Configuring Access Codes

Access Codes
Customer Enter a customer name.
Set Start Date Time On the calendar at the left, click a starting date. Click Set Start Date and choose a starting time. The default is 12:00am (midnight).
Set End Date Time On the calendar at the left, click an ending date. Click Set End Date and choose an ending time. The default is 12:00am (midnight).
Code Prefix Enter an optional one- to three-letter customer code. After you save the changes, BBSM adds this prefix to the numeric portion of the access code when the access code is generated. The combination is the access code. For example, if you entered CIS and entered 5 for the length, the access codes would be in the form of CISxxxxx, where x is the numeric portion of the code. If no prefix is entered, the access code appears as xxxxx.
Quantity Enter the number of access codes that you need. The maximum number of access codes that can be saved is 1000. Because customer names do not have to unique for access codes, the same customer name can be used to create 1000 codes. Nevertheless, the maximum number allowed in the Quantity field is 1000.
Access Code Price Enter the price that you want to charge for each access code. Although the price is recorded for auditing purposes, BBSM does not perform any billing when users log in with access codes. (The currency type was chosen from the Currency Type drop-down menu on the BBSM Server Settings web page. The currency specified on that web page applies to all options.)
Length of Codes Enter the length of the numeric portion of the access code. The minimum length of the numeric portion of the access code is 4 numbers and the maximum length is 15 numbers. The default is 5 numbers.

Bandwidth Class of Service
(These fields apply only for bandwidth reservation.)
Package From the drop-down menu, choose a service package.
Bandwidth Displays the bandwidth in kbps for the entire group
Description Displays a description of the chosen bandwidth package.

Bandwidth Throttle
Bandwidth kbps Note This field only appears when bandwidth throttling is being used. From the drop-down menu, choose a maximum bandwidth that is applied to each user that logs in with one of the access codes.

Buttons
View Access Codes Shows the access codes that you configured.
New Adds a new reservation. A web page with blank fields appears so the access codes can be configured.
Requery Refreshes the web page (click before saving changes).
Save Saves the changes made to the web page.
Delete When you choose a reservation, deletes the reservation.
Step 6 Verify that you checked *Enable Bandwidth Throttle* or chose *Throttling* in the Access Code Bandwidth field on the BBSM Server Settings web page. Choosing one of these options allows the bandwidth to be specified on the Codes by Duration web page.

Step 7 Configure the options for creating access codes by duration and click **Save**. The View Access Codes button appears on the web page so you can view the access codes for this group. See Figure 17-6 and Table 17-5.

If you do not check this box, you can modify any other settings without altering the time remaining on the access codes (the Duration field is ignored).

**Note** The Reset Time Remaining check box appears on this page when you are editing access codes. This check box can be used to reset the time remaining on all access codes in the group. If this box is checked and you click Save, a confirmation dialog box appears, asking you to verify that you want to reset the time remaining. When you click OK, all codes in the group are updated so the time remaining is equal to the chosen duration.

Step 8 Click the **View Access Codes** button to verify your configuration. The values that you configured appear on the page.

*Figure 17-6 Codes by Duration Web Page*
## Creating and Configuring Access Codes

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer</td>
<td>Enter a customer name.</td>
</tr>
<tr>
<td>Duration of Each Code</td>
<td>Enter the numeric value for the duration that the access code can be used. From the drop-down menu on the right, choose minutes, hours, days, or weeks.</td>
</tr>
<tr>
<td>Price per Code</td>
<td>Enter the price that you want to charge for each access code. Although the price is recorded for auditing purposes, BBSM does not perform any billing when users log in with access codes. (The currency type was chosen from the Currency Type drop-down menu on the BBSM Server Settings web page. The currency specified on that web page applies to all options.)</td>
</tr>
<tr>
<td>Bandwidth (kbps per user)</td>
<td><strong>Note</strong> This option is only available when you check Enable Bandwidth Throttle or choose Throttling in the Access Code Bandwidth field on the BBSM Server Settings web page. Choosing one of these options allows the bandwidth to be specified on the Codes by Duration web page. From the drop-down menu, choose a maximum bandwidth that is applied to each user that logs in with one of the access codes.</td>
</tr>
<tr>
<td>Quantity</td>
<td>Enter the number of access codes that you need. The maximum number of access codes that can be saved is 1000. Because customer names do not have to be unique for access codes, the same customer name can be used to create 1000 codes. Nevertheless, the maximum number allowed in the Quantity field is 1000.</td>
</tr>
<tr>
<td>Code Prefix</td>
<td>Enter an optional one- to three-letter customer code. After you save the changes, BBSM adds this prefix to the numeric portion of the access code when the access code is generated. For example, if you entered CIS and entered 5 for the length, the access codes would be in the form of CISxxxx, where x is the numeric portion of the code. If no prefix is entered, the access code appears as xxxx. (The Code Prefix and Length of Each Code fields are disabled after the access code is created because they cannot be changed after the codes have been saved.)</td>
</tr>
<tr>
<td>Length of Each Code</td>
<td>From the drop-down menu, choose the number of digits for the numeric portion of the access code. The minimum length of the numeric portion of the access code is 4 numbers and the maximum length is 15 numbers. The default is 5 numbers. (This field is disabled after the access code is created because the prefix can no longer be changed.)</td>
</tr>
</tbody>
</table>
Finding Access Codes

Follow this procedure to find reservations and access codes by the customer name or code.

Step 1  From the Dashboard, click Access Code Management. The Codes by Date web page appears.
Step 2  From the menu bar, click Find Access Codes. The Find Access Codes web page appears. (See Figure 17-7.)

Figure 17-7 Find Access Codes Web Page

Step 3  Find access codes in one of the following ways:
   • In the Find by Customer area, choose a customer from the Customer drop-down menu.
   • In the Find by Access Code area, enter the access code in the Access Code field. (The access code entered does not have to be a complete access code. You can enter partial codes. The access code is not case sensitive—typing s123 in the Access Code field finds any codes that contain S123 or s123.

Note  If a customer is chosen and an access code is entered, BBSM will search only for the customer name and ignore the access code field.

Step 4  Click Find Codes. The View Access Codes web page appears. The access codes are displayed either by customer or access code order. The search string that was used is displayed at the top of the page. Also, the access codes that contained the search string are displayed in bold so they are easier to find on the page. (See Figure 17-8.)
To edit an existing group of access codes, click one of the **Edit** buttons on the page. When you click the Edit button for a group, you are taken to the View Access Codes web page that shows the access codes for one group. Access codes can only be edited on a group basis, rather than by individual access code. Editing by group means that more time cannot be added for only one access code. It can only be added to the entire group.

On the View Access Codes web page, click **Printable** to print the access codes in a larger format that can be given to guests. The Printer Format Access Codes web page appears.
## Finding Reservations by Date

Follow this procedure to find reservations by the date of the reservation.

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

**Step 2** From the menu bar, click **View by Year**. The Find Codes by Date web page appears, showing highlighted dates for the existing reservations. (See **Figure 17-9**.)

**Figure 17-9 Find Codes by Date Web Page**

![Find Codes by Date Web Page](image)

**Step 3** Click the date to view the details about the reservation. The Codes by Date web page appears, showing the existing reservations for the date.

## Access Codes for Meeting Rooms

The administrator or operator can configure access so that either multiple users or only one person at a time can use a particular access code. This is determined by the page set that you chose in the Network Element Port Settings pop-up window for the meeting room site or ports:

- **For access by only one person at a time per code**, choose the MeetingRoom page set.
- **For access by more than one person at a time per code**, choose the AccessCode page set.
(For additional information, refer to the “Page Set Overview” section on page 18-2 and Chapter 13, “Configuring PMS or Print Billing.”)

You can configure the site so it consists only of meeting rooms. In addition, you can manage your server to mix meeting rooms and guest rooms at the site. This configuration does not depend on the property’s physical layout.

**Note**

When using access codes, all of the BBSM sites are assumed to be located in the same time zone.

When you mapped your rooms, if you checked the “Check here if this is a meeting room” check box, the MeetingRoom page set was applied by default to these rooms. If you want to change the page set to the AccessCode page set, refer to the chapter on using the port control option in the *Cisco BBSM 5.3 Operations Guide*. 
Creating Custom Page Sets

This chapter provides an overview of BBSM page sets and the procedures to create custom page sets using either the Page Set Wizard to create a custom DailyHotel page set or the page set files to create a page set manually. The chapter also describes how to add these page sets to the list of available page sets in WEBconfig:

- **Page Set Overview, page 18-2**
- **Using the Page Set Wizard, page 18-5**—Use the wizard to create and name a custom page set based on the DailyHotel page set template. Refer to the section for the features that can be changed with the wizard.
- **Creating Custom Page Sets Manually, page 18-12**—If you are making more extensive changes to the GUI, are using a page set other than DailyHotel, or are changing the way your page set interacts with BBSM, use the procedure in this section to change the code. You do not need to install the SDK to make these changes. In addition to the changes you can make using the Page Set Wizard, you can make these changes by manually changing the code:
  - Use page set templates other than DailyHotel to create your custom page set
  - Replace the graphical presentation of the page set with more flexibility than with the wizard
  - Remove extraneous bandwidth options
- **Adding Custom Page Sets to BBSM, page 18-17**

Refer to this documentation for additional information about page sets:

- For an introduction to page sets and a description of the default BBSM page sets, refer to the “Page Set Overview” section on page 18-2. Cisco recommends that you read this section before creating your page set.
- If you are creating custom access, accounting, or PMS policy methods, you must install and use the SDK. Refer to the Cisco BBSM 5.3 SDK Developer Guide.
Page Set Overview

BBSM uses page sets made up of active server page (ASP) files, commonly called *pages*. When the end user starts a session, the page set ASP files execute on the BBSM server and on the end user’s browser.

Different page sets contain different types of ASP files. By choosing specific page sets, you are choosing ASP files that associate an access policy and, if applicable, an accounting policy with a specific port. (In general, page sets are named by combining the access and accounting policy names, such as DailyHotel and BlockICS.) These policies define the access and accounting methods for the end user’s session. They are described briefly below:

- **Access policies**—The access policy defines the end user’s process when connecting to the Internet. The default page sets enable you to choose these access policies: Access Code, Block, Daily, Minute, RADIUS, or Subscription.
- **Accounting policies**—The accounting policy determines how end users are billed for BBSM Internet services. BBSM provides these default accounting policies: ICS Credit Card, Cruise Line, Hotel, and RADIUS. If you do not want to bill the end user, you can use the Null accounting policy.

If the end user will be entering sensitive information, such as credit card information, then you should use page sets that provide the SSL encryption protocol. For these SSL page sets, you must buy and install an SSL certificate. For complete details on installing the certificate, refer to the “Installing an SSL Certificate” section on page 16-2. The other default BBSM page sets transmit data in clear text.

BBSM ships with default page sets. They are used in the following ways:

- The default page sets can be used without modification for demonstrations. They also enable you to configure a server and begin using it quickly for testing in the lab environment.
- They are used as templates from which you create custom page sets that are used in production:
  - You can use the page set template to create custom DailyHotel page sets using the Page Set Wizard if you are making simple changes such as adding a graphic and logo. For a description of the wizard and the step-by-step procedure for using it, refer to the “Using the Page Set Wizard” section on page 18-5.
  - You can create custom page sets manually by modifying the ASP files without using the SDK. Refer to the “Creating Custom Page Sets Manually” section on page 18-12.
  - Your developer can use the BBSM SDK to create new page sets if you are creating custom access, accounting, or PMS policies. Refer to the *Cisco BBSM 5.3 SDK Developer Guide* and the following software download URL:

    http://www.cisco.com/cgi-bin/tablebuild.pl/bbsm52

Table 18-1 describes these page sets and the access policy and accounting policy that page sets may use.

---

**Caution**

Because page sets whose names end in *Clear* do not use SSL security, Cisco does not recommend using them in production to transmit data to the BBSM server. (See Table 18-1.) The end user’s browser transmits RADIUS and credit card information to BBSM in clear text. BBSM provides them for demonstration and testing situations in which installing a server certificate is not feasible.

If you are using multinets, note that the page set assigned to the end user’s port determines whether an administrator or operator provisions the multinet or the end user provisions the multinet. Table 18-1 shows which page sets the end user can provision.
### Table 18-1  BBSM Default Page Set Descriptions

<table>
<thead>
<tr>
<th>Page Set</th>
<th>Uses SSL?</th>
<th>Who Selects Public/Private Multinet?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccessCode</td>
<td>No</td>
<td>Administrator or operator</td>
<td>Prompts the end user to enter an access code to access the Internet for an authorized period that the BBSM operator configures. Use this page set if you want multiple users to be able to access the Internet at the same time with one access code. (Refer also to the MeetingRoom page set.) By default, this page set uses the AccessCode access policy and no accounting policy.</td>
</tr>
</tbody>
</table>
| BiDirectional_DailyHotel | No        | End user                             | Demonstrates how to use the guest data that BBSM pulls from the PMS. Meant to be an example of how to take advantage of the bidirectional PMS interface, the page set provides the default DailyHotel page set functionality, plus functionality such as viewing guest folio and guest checkout. You must customize the BiDirectional ASP files to achieve the appropriate functionality. This page set uses the following default policies:  
  - Access policy—Daily  
  - Accounting policy—Hotel |
| BlockICS       | No        | End user                             | Prompts the end user to enter credit card information to access the Internet for a block of minutes.                                                                                                         |
| CruiseLine     | No        | End user                             | Prompts the end user to enter credit card information or access card information (access card information is not the same as an access code) to access the Internet per minute or for a block of minutes. This page set uses the following default policies:  
  - Access policy—Block  
  - Accounting policy—IscCreditCard |
| DailyHotel     | No        | End user                             | Provides the end user access for a 24-hour period and sends charges to the hotel’s PMS or local printer.                                                                                                        |
| DailyICS       | Yes       | End user                             | Prompts the end user to enter credit card information to access the Internet for a 24-hour period. These page sets use the following default policies:  
  - Access policy—Daily  
  - Accounting policy—IscCreditCard |
| DailyICSClear  | No        | End user                             |                                                                                                                                                                                                           |
### Table 18-1 BBSM Default Page Set Descriptions (continued)

<table>
<thead>
<tr>
<th>Page Set</th>
<th>Uses SSL?</th>
<th>Who Selects Public/Private Multinet?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MeetingRoom</td>
<td>No</td>
<td>Administrator or operator</td>
<td>Prompts the end user to enter an access code to access the Internet for an authorized period that the BBSM administrator or operator configures. Use this page if you want only one user to access the Internet at a time through the access code. By default, this page set uses the AccessCode access policy and no accounting policy.</td>
</tr>
<tr>
<td>MegaClear</td>
<td>Yes</td>
<td>No</td>
<td>Provides access flexibility to the end user and still controls access. Modify the page set to fit your needs.</td>
</tr>
<tr>
<td>MegaClear</td>
<td>Yes</td>
<td>No</td>
<td>Provides access flexibility to the end user and still controls access. Modify the page set to fit your needs.</td>
</tr>
<tr>
<td>MinuteICS</td>
<td>Yes</td>
<td>End user</td>
<td>Prompts the end user to enter credit card information to access the Internet per minute.</td>
</tr>
<tr>
<td>MinuteICSClear</td>
<td>Yes</td>
<td>No</td>
<td>Prompts the end user to enter credit card information to access the Internet per minute.</td>
</tr>
<tr>
<td>RADIUSUBand</td>
<td>Yes</td>
<td>End user</td>
<td>Prompts the end user to enter a RADIUS username and password to access the Internet. It also permits the end user to choose a bandwidth at a specified price. For this page set, the disconnect web page presents the end user with an estimated summary for the time of the active session and the charges accrued at the chosen bandwidth. By default, these page sets use the RADIUS access policy and RADIUS accounting if a RADIUS accounting server is configured.</td>
</tr>
<tr>
<td>Subscription</td>
<td>No</td>
<td>End user</td>
<td>Enables the end user to access the Internet for a specified date range. Use this page set to offer free Internet access on a port by specifying the date range in Port Control. By default, the page set uses the Subscription access policy and does not do billing (no accounting policy).</td>
</tr>
</tbody>
</table>
Using the Page Set Wizard

The Page Set Wizard option, located under Administration on the Dashboard, enables you to create a basic DailyHotel page set with a property photo and hotel logo. You can also modify or delete an existing DailyHotel page set that was created with the wizard.

These are the features that can be changed with the wizard:

- The template graphic and logo, which you can replace with a graphic that represents your organization. The image area for the graphic and the logo cannot be changed.

- The bandwidth options and prices.

- These defaults:
  - To post charges at the beginning of the session.
  - To deactivate the end user at the end of the session boundary, which means that the user would have to reauthenticate at the beginning of the next session.
  - To charge the end user by MAC address rather than by port. The feature enables the end user to reconnect anywhere on the property rather than being restricted to reconnecting in the room.

- The end time for the billing cycle.

- The portal URL.

Descriptive text can also be added to the Connect page.

Table 18-1  BBSM Default Page Set Descriptions (continued)

<table>
<thead>
<tr>
<th>Page Set</th>
<th>Uses SSL?</th>
<th>Who Selects Public/Private Multinet?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SubscriptionHome</td>
<td>No</td>
<td>Administrator or operator</td>
<td>Enables the end user to access the Internet for a per-port specified date range. When the user activates a session, BBSM redirects the user to the originally requested URL, which is usually the home page set in the browser. By default, the page set uses the Subscription access policy and does not do billing (no accounting policy).</td>
</tr>
</tbody>
</table>
| SubscriptionHotel     | No        | End user                             | Enables the end user to access the Internet for a specified (SubscriptionHotel) or varied (SubscriptionHotelMultipleDay) date range. If the user attempts Internet access outside the date range, these page sets enable the user to self-provision the subscription by billing it to the hotel’s PMS. These page sets use the following default policies:  
  - Access policy—Subscription
  - Accounting policy—Hotel |
| SubscriptionHotelMultipleDay | No        | End user                             | Enables the end user to access the Internet for a specified (SubscriptionHotel) or varied (SubscriptionHotelMultipleDay) date range. If the user attempts Internet access outside the date range, these page sets enable the user to self-provision the subscription by billing it to the hotel’s PMS. These page sets use the following default policies:  
  - Access policy—Subscription
  - Accounting policy—Hotel |
| SubscriptionICS       | No        | End user                             | Enables the end user to access the Internet for a per-port specified date range. If the end user attempts to access the Internet outside the date range, the page set enables the user to bill the subscription to a credit card. These page sets use the following default policies:  
  - Access policy—Subscription
  - Accounting policy—ICSCreditCard |

Using the Page Set Wizard

The Page Set Wizard option, located under Administration on the Dashboard, enables you to create a basic DailyHotel page set with a property photo and hotel logo. You can also modify or delete an existing DailyHotel page set that was created with the wizard.

These are the features that can be changed with the wizard:

- The template graphic and logo, which you can replace with a graphic that represents your organization. The image area for the graphic and the logo cannot be changed.

- The bandwidth options and prices.

- These defaults:
  - To post charges at the beginning of the session.
  - To deactivate the end user at the end of the session boundary, which means that the user would have to reauthenticate at the beginning of the next session.
  - To charge the end user by MAC address rather than by port. The feature enables the end user to reconnect anywhere on the property rather than being restricted to reconnecting in the room.

- The end time for the billing cycle.

- The portal URL.

Descriptive text can also be added to the Connect page.
The wizard automatically adds the new page set to the drop-down list of page sets in the WEBconfig Network Element Port Settings window.

For additional information about page sets, refer to the “Page Set Overview” section on page 18-2. Follow this procedure to create a new DailyHotel page set using the wizard.

**Step 1**

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

*Figure 18-1 Step 1 - Page Set Name*

Step 1 - Page Set Name

This wizard allows you to create or modify a Page Set. A Page Set is the set of web pages that the end user will see while they connect to the internet. For complete instructions on using this wizard, refer to the BBSM Documentation.

**Note**

Page Sets created by this wizard assume internet users are charged by the day (24 hour period) and that billing will be posted to a hotel Property Management System (PMS). For other connection schemes, please see the BBSM SDK Documentation.

Enter Name for New Page Set

OR

Select Existing Page Set

---

**Step 2**

Choose a name for your new page set, and enter it in the Enter Name for New Page Set field.

*Note*  
To modify an existing page set that was created earlier, click the drop-down arrow in the Select Existing Page Set field and choose the page set that you want to edit.

**Step 3**

Click **Next**. The Step 2 - Select a Layout web page appears. (See Figure 18-2.)
Step 4  Click the page set layout and then Next. The Step 3 - Import a Picture web page appears. (See Figure 18-3.)

Step 5  Click Browse to navigate to the file of the graphic that you want to appear on the Start page and click Next. (The graphic must be 175 by 225 pixels or smaller.) The Step 4 - Import a Logo web page appears. (See Figure 18-4.)

Note  To view the graphic that you chose to appear on the Start page, click Back.
Step 6  Click **Browse** to navigate to the file of the logo that you want to appear on the Start page and click **Next**. (The logo must be 175 by 70 pixels or smaller.) The Step 5 - Page Set Options web page appears. (See Figure 18-5.)

---

**Note**  To view the logo that you chose to display on the Start page, click **Back**.
Step 7 Check the Bandwidth Option check boxes for the rates you want to offer end users and enter a price for that rate. For example, if you want to offer a 512-kbps speed for $5.00 per day and a 256-kbps speed for $3.00 per day, just check the boxes next to 512 kbps and 256 kbps and enter the price for each.

Note If you checked the Bandwidth Throttle check box on the BBSM Server Settings web page, all bandwidth options are available. Otherwise, only the Full-Speed bandwidth option is available.

Step 8 Choose the other page set options. (If you choose Specific Time, you can choose a specific time for the user session to end from the User Session Ends drop-down menu. (See Figure 18-6.) Remember that page sets created with the Page Set Wizard assume that Internet users are charged by the day (24-hour period) and that billing will be posted to a PMS or printer.
Chapter 18      Creating Custom Page Sets

Using the Page Set Wizard

Figure 18-6  Step 5 - Page Set Options with “Specific Time” Selected

---

Step 9  Click Next. The Step 6 - Preview web page appears with the name of your new page set. In this example, the page set is named Delta. (See Figure 18-7.)

Figure 18-7  Step 6 - Preview

---

Step 10  To view your new page set, click Preview Page Set. (See Figure 18-8.), and then close the page set preview.
Figure 18-8 Preview of Custom Page Set

**Step 11** To save your new page set, click Finish. The Step 7 - Finish web page appears. (See Figure 18-9.)

**Note** If you want to edit your page set, click the appropriate link in the NavBar on the left, make your changes, and click Finish.

Figure 18-9 Step 7 - Finish

---

To save your new page set, click **Finish**. The Step 7 - Finish web page appears. (See Figure 18-9.)

**Note** If you want to edit your page set, click the appropriate link in the NavBar on the left, make your changes, and click **Finish**.
Creating Custom Page Sets Manually

This section describes how to create custom page sets manually without using the Page Set Wizard. To make the basic changes in this section, you do not need to use the SDK. However, if you decide to change the access, accounting, or PMS policies that BBSM uses, you must use the SDK.

If you create your page set manually, you must also add it to the list of available BBSM page sets. For this procedure, refer to the “Adding Custom Page Sets to BBSM” section on page 18-17. If the page set is created using the Page Set Wizard, you do not need to add the page set to the list because the wizard automatically adds the new page set to the drop-down list of page sets in the WEBconfig Network Element Port Settings window.

(You must have administrator privileges to use WEBconfig to add your page set to the registry.)

Before You Start

Please read the following information before beginning to create your page set:

- You must have a BBSM server to perform this procedure.
- Use Windows Notepad or another text editor to edit the ASP files that control the page set parameters.
- Give your customized page set a new name. The BBSM default page sets are provided only as templates. If you do not rename your customized page sets, they can be removed or replaced when a BBSM patch or service pack is installed.
- Page sets include the following ASP files (pages):
  - Start pages—Defines the first page that the end user sees
  - Post pages—Displays the Connecting... message. It calls the functions needed to connect the end user.
  - Package pages—Stores the settings for the page set.
  - GIF files—Define the graphical representation of the page set.

- If you want to debug ActiveX server components in page sets, you can develop your page set on a server that has the development environment installed and use Microsoft Visual Studio as an editor.
Page Set Creation Procedure

Follow this procedure to create your custom page set. In the procedure, we create a custom page set using the DailyHotel page set template for an example. You can create custom page sets from other page set templates similarly, although page set parameters differ with each page set.

In the example, we are changing the following DailyHotel page set parameters:

- The page set name so end user can view only the pages he or she is supposed to view.
- The end time for the billing cycle from 12:00 to 4:30 p.m.
- The default to begin posting charges at the beginning of the session.
- The default to deactivate the end user at the end of the session boundary.
- The default to not charge a MAC address for re-use within the 24-hour period, regardless of which port is used.
- The pricing for package 1 from 9.95 to 10.95.

We are also removing several bandwidth options.

Step 1 Determine the page set that meets your needs by reviewing the “Page Set Overview” section on page 18-2.

Step 2 Within the c:\atcom\ekgnkm folder (where the BBSM page set files are located), create a subdirectory, such as c:\atcom\ekgnkm\YourNewDirectory, for your new page set files. (Although new files can be created in c:\atcom\ekgnkm, Cisco recommends saving them in a separate folder.)

Note If you have installed a BBSM service pack and inadvertently overwritten a custom page set, the previous page set can be retrieved. A backup of all previous page sets is located in the c:\atcom\patch directory. Look for the folder named Backup####, where #### is the patch number that corresponds to your patch or service pack (found on WEBpatch).

When you find your original page set, do not copy it directly back to the ekgnkm directory. Instead, you must integrate your custom page set with the new page set that was installed with the service pack. Cisco recommends that you cut and paste changes that you made to the custom page set into the new page set so you are using the most up-to-date page set with your new service pack.

Step 3 Change the write permissions of the ASP files that can be edited, the NewNamePackage.asp and NewNamePost.asp files, as shown below:

Step 4 Copy all of the page set template’s ASP and GIF files into the new subdirectory. Rename the ASP files with the name of your new page set, such as NewNameStart.asp.

a. Right-click the NewNamePackage.asp file and select Properties.

b. Uncheck the Read-only check box and click OK.

Step 5 If you want to change the default portal (the end user is directed to this home page when he or she gains Internet access) in the NewNamePost ASP file, follow these steps:

a. Using Microsoft Notepad, open the NewNamePost.asp file.

b. Change the default home page, www.cisco.com, to a new default URL.

c. Save the file and close Notepad.
Step 6  
If you want to change the page set parameters in the NewNamePackage ASP file, follow these steps:


b. Note the following default code that will be changed in this example:

```html
<%
  var strPageToCheck = "DailyHotel";
  (strSessionBoundary = "12:00";
  bPostAtStart = false;
  bRenewSession = true;
  bWelcomeBackMAC = false;

  var PackagePriceArray = new Array
  (9.95, //package 1, $9.95
   7.95, //package 2, $7.95
   5.95, //package 3, $5.95
   3.95, //package 4, $3.95
   1.95 //package 5, $1.95
  );
  var PackageKbpsArray = new Array
  (0, //package 1, full speed
   512, //package 2, 512 Kbits/sec
   256, //package 3, 256 Kbits/sec
   128, //package 4, 128 Kbits/sec
   64 //package 5, 64 Kbits/sec
  );
  var PackagePublicPrivateIPArray = new Array
  (1, //package 1, multinet 1
   1, //package 2, multinet 1
   1, //package 3, multinet 1
   2, //package 4, multinet 2
   2, //package 5, multinet 2
   2, //package 6, multinet 2
  );
%
```

c. Use the following guidelines to change the code:

To change the strPageToCheck parameter to ensure that the end user can view only the pages he or she is supposed to view, replace the default page set name of DailyHotel with the name of your new page set.

---

Note  
Later in the procedure you will also change the name of the page set in the Windows registry. The strPageToCheck name in the package file and the name in the registry must be the same. The name is not case sensitive, so DailyHotel is the same as dailyhotel.
To change the `strSessionBoundary` parameter so that the end time for your billing cycle changes from 12:00 to 4:30 p.m., enter **16:30** between the quotes. Cisco recommends that you read the following specifications for this parameter:

- Use a string of the form HH:MM, where HH = the hours in the range 0 through 23 (0 means midnight, 12 means noon, and 23 means 11 p.m.) and MM = the minute in the range 00 through 59.

- The following example shows the system default session boundary of noon. As shown, placing a space between the quotation marks also sets the system default to noon:

  ```javascript
  var strSessionBoundary = "12:00"
  var strSessionBoundary = " "
  ```

- This example shows an example session boundary of 2:30 p.m.:

  ```javascript
  var strSessionBoundary = "14:30"
  ```

**Note** If a customer activates shortly before the time set for the session boundary, the session could end very soon after it starts. For example, if the session boundary is set for 12 a.m. (midnight) and a customer activates a session at 11:30 p.m., the session terminates at 12 a.m. (1/2 hour later). However, if another customer activates a session at 12:30 a.m., the session terminates at 12 a.m. the next day.

To set the time so that the session ends 24 hours after activation, modify the line to specify an empty string for the session boundary (with no space between the quotation marks); for example, as follows:

```javascript
var strSessionBoundary = ""
```

To change the `bPostAtStart` parameter to begin posting charges at the beginning of the session, change it to **true**.

To change the `bRenewSession` parameter to deactivate an end user at the end of a session so that he or she must reauthenticate at the beginning of the next session, change it to **false**.

To change the `bWelcomeBackMAC` parameter, refer to the following information about how the parameter works:

- Setting the parameter to **true**—After the end user authenticates, he or she can reconnect until the session boundary without being charged. The user can log in from anywhere on the property (any port).

- Setting the parameter to **false**—After the end user authenticates, that room (port) will now allow anyone to reconnect until the session boundary. This includes the original user that authenticated as well as anyone else that enters the room. No other ports on the property will allow the original user to reconnect, only that one port.

To change the `PackagePriceArray` pricing of package 1 from 9.95 to 10.95, change **9.95** to **10.95** at the beginning of the line. Cisco recommends that you change the corresponding dollar amount following the // comment mark to the same figure. You can add or remove pricing packages as you want. You must also remove the corresponding `PackageKbpsArray` lines.

To remove 64 kbps and 128 kbps `PackageKbpsArray` pricing packages, remove the appropriate lines in the code. Then you need to remove the corresponding `PackagePriceArray` lines. Be sure to remove the trailing comma from the last entry in each array.
Creating Custom Page Sets Manually

Chapter 18      Creating Custom Page Sets

Creating Custom Page Sets Manually

**Note**  
If items are removed from the price and kbps arrays, you also need to change the PackagePublicPrivateIPArray (multinet) array. All arrays should have the same number of elements.

**Step 7**  
Note that your parameters have changed to the following:

```html
<%  
  var strPageToCheck = "NewName";
  (  
    strSessionBoundary = "16:30";
    bPostAtStart = true;
    bRenewSession = false;
    bWelcomeBackMAC = true;

    var PackagePriceArray = new Array
    (  
      10.95, //package 1, $10.95
      7.95, //package 2, $7.95
      5.95 //package 3, $5.95
    );
    var PackageKbpsArray = new Array
    (  
      0, //package 1, full speed
      512, //package 2, 512 Kbits/sec
      256 //package 3, 256 Kbits/sec
    );
    var PackagePublicPrivateIPArray = new Array
    (  
      1, //package 1, multinet 1
      1, //package 2, multinet 1
      2, //package 3, multinet 2
    );
  %>
```

**Step 8**  
Save your changes and exit Notepad.

**Step 9**  
Change all references to the name of your new page set in all ASP files, such as NewNamePost.asp.

**Step 10**  
In your new subdirectory, replace the default GIF files with any new graphics:

a. Replace background colors with your customized colors.

b. Replace the text and font displayed to the end user with your customized text.

c. Replace graphical references in the ASP files to the names of your new GIF files.

**Step 11**  
Register your page set and add it to the list of BBSM available page sets. For instructions, refer to the “Adding Custom Page Sets to BBSM” section on page 18-17 for instructions.

**Step 12**  
Test your new page set:

a. Physically connect a client to a port.

b. From the BBSM Dashboard, click Port Control. The Port List web page appears.

c. In the left-hand column, check the port that the client is connected to and then click Port Settings. The Port Settings window pops up.
d. From the Page Set drop-down menu, choose your page set. The Start Page text box automatically populates with the URL of your Start page. Click Save.

e. Open the browser on the client. Your Start page should be displayed.

\[\text{Note}\] If your page set uses SSL, you must have a valid certificate installed on your server to test your pages. If you do not have a certificate installed, you will be unable to view the secure pages when you connect a client. For testing purposes, you can make your BBSM a certificate authority and then sign your own certificate. This procedure should only be used on a development server and never on a release server. This method is only used for testing secure page sets and is not an acceptable solution for installing a valid certificate on your server. For detailed instructions, refer to the “Installing an SSL Certificate” section on page 16-2.

f. Verify that your changes were made.

Adding Custom Page Sets to BBSM

If you created a custom page set manually without using the Page Set Wizard, follow this procedure to add the new page set to the list of available BBSM page sets. You do not need to perform this procedure if you used the Page Set Wizard because the DailyHotel page sets created using the Page Set Wizard are added to the BBSM page sets automatically.

If needed, contact the Cisco TAC to be sure that your web page can be supported. Refer to the “Obtaining Technical Assistance” section in the preface to this user guide.

For additional information about page sets, refer to the following:

- Page Set Overview, page 18-2
- Using the Page Set Wizard, page 18-5
- Creating Custom Page Sets Manually, page 18-12

Step 1  From the Dashboard, click WEBconfig. The BBSM Server Settings web page appears.

Step 2  In the NavBar, select the Custom Page Sets web page. The Custom Page Sets web page appears. (See Figure 18-10.)
Step 3  Add the custom page set to BBSM based on the information shown in Table 18-2 and click **Save**.

**Table 18-2  Custom Page Sets Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page Set</td>
<td>Enter the name of the page set.</td>
</tr>
</tbody>
</table>
| Start Page| Enter the complete URL of the Start page for your page set. The URL must be in the form `http://%iport%...` because BBSM translates `%iport%` to be either the BBSM internal IP address or the BBSM domain name, if applicable. For example, if you saved your page set in a new directory within the `c:\atcom\ekgnkm` directory, type the following:

```
http://%iport%/ekgnkm/YourNewDirectory/NewNameStart.asp3
```

The `%iport%` is automatically expanded to the IP address or domain name of the BBSM server.

**Caution**  If your Start page requests sensitive information from the end user, you should use SSL, and the protocol part of the URL will be `https`, instead of `http`.

<table>
<thead>
<tr>
<th>Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Adds a new page set. A new blank web page appears so the page set and Start page can be added.</td>
</tr>
<tr>
<td>Requery</td>
<td>Refreshes the web page (before saving the changes).</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the changes made to the web page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes this page set.</td>
</tr>
</tbody>
</table>
Configuring Walled Gardens

BBSM enables you to define free access to specific websites. This subset of the Internet that unauthenticated BBSM end users can access is called a walled garden. These walled gardens enable you to increase revenue by marketing various services to your guests.

The following are typical walled garden links:

- Local weather and attractions
- Online concierge and room services
- Hotel chain corporate or loyalty program portals
- Vendor services, such as car rental agencies

In BBSM, a URL, a network IP address, and subnet mask define each free-access site.

Walled gardens are configured per server so all sites share the same walled gardens. However, end users normally access walled garden sites through links on the Connect page. If you want some ports to have access to walled garden sites while other ports do not, then create different Connect pages for the applicable ports.

From the BBSM perspective, walled gardens open up filters from the internal network (client network) to the external network (Internet) so a user on the internal network can access services on the external network without authenticating to BBSM, hence providing free access to specific sites on the external network that are set up on the walled garden web page.

Setting up walled gardens is a two-step process.

- The first step is to set up the filter entry, which is entered on the Walled Garden web page in WEBconfig. Three pieces of information are needed:
  - Full domain name—You enter the domain name of the walled garden website, such as www.cisco.com, in this field.

    **Note** This domain name is used when a client’s browser is configured to use a web proxy. In this case, the packets that BBSM sees have an unresolved destination address (the proxy server does the resolution). For this reason, BBSM compares the destination host name in the packet to the destination host name configured in the walled garden.

  - IP address—You enter the IP address (or addresses) of the site (or sites) to be accessed for free.

  - Subnet mask—You enter the subnet mask. In most cases, this IP address should be quadruple 255s (255.255.255.255), which limits access only to the IP address specified above. Any attempts by the client to redirect to another IP address forces BBSM to display the appropriate access page.
Note: You can enter a less restrictive mask for an entire subnet block.

- Typically, the second step is to place links on the Connect page that refer to the sites entered on the Walled Garden web page. Your web developer can add these links for you.

  Sometimes the IP address assigned to a domain changes. In this case, you will need to modify your walled garden settings:
  - Update the walled garden page in WEBconfig with the new IP address.
  - In your Connect page, replace any references to the old IP address with the new IP address. (Normally, you would use domain names in the HTML code in your web page so this may not apply.)

Follow this procedure to establish the path for each walled garden site by using the Walled Garden web page in WEBconfig and to refer to these sites from the Connect page, which is the typical step after configuring your web pages.

Step 1 From the Dashboard, click WEBconfig. The BBSM Server Settings web page appears.

Step 2 In the NavBar, click the Walled Garden link. The Walled Garden web page appears. (See Figure 19-1.)

**Figure 19-1 Walled Garden Web Page**

Step 3 Configure the Walled Garden options based on the information shown in Table 19-1 and click Save.

Step 4 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 these servers.
Step 5  Add the links to the walled garden pages to the Connect page. This is the typical next step after configuring your walled gardens. Your web developer can add these links for you. Cisco recommends using domain name URLs instead of IP addresses in the HTML code, as this is standard practice for web development.

Note  If the IP address of your walled garden changes, you must re-enter the walled garden IP address in WEBconfig. You must do this even if the domain name has not changed.

Table 19-1  Walled Garden Web Page Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Domain Name</td>
<td>Enter the domain name of the walled garden website; for example, <a href="http://www.cisco.com">www.cisco.com</a>.</td>
</tr>
<tr>
<td>IP Address</td>
<td><strong>Defining a Walled Garden on a Server</strong></td>
</tr>
</tbody>
</table>
| Subnet Mask    | To define a walled garden on a server, enter the domain name’s IP address and a subnet mask of 255.255.255.255. For example, for www.cisco.com, enter the following:  
  - IP address = 198.133.219.25  
  - Subnet mask = 255.255.255.255  
  **Defining a Walled Garden on a Subnet**  
  To define a walled garden on a subnet, you can enter the IP address for each site in the walled garden individually as above or you can enter the subnet’s IP address and its subnet mask. For example, all of the following IP addresses are part of the 198.133.219.x subnet:  
  - www.cisco.com = 198.133.219.25:  
  - business.cisco.com = 198.133.219.124  
  - newsroom.cisco.com = 198.133.219.119  
  You can incorporate these sites into a walled garden with just one subnet IP address and its subnet mask:  
  - IP address = 192.133.219.0  
  - Subnet mask = 255.255.255.0  
  The x.x.x.0 address defines the walled garden as a subnet, not just an individual IP address. This subnet includes the range of IP addresses from 198.133.219.1 to 198.133.219.255. (Different subnet masks include different address ranges.) |

<table>
<thead>
<tr>
<th>Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Adds a new walled garden site. Text fields on the page are cleared so that new data can be entered.</td>
</tr>
<tr>
<td>Requery</td>
<td>Refreshes the web page (click before saving changes).</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the changes made to the web page.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes this website from BBSM.</td>
</tr>
</tbody>
</table>
Chapter 20

Configuring the Port Hop Delay

This chapter describes the port hopping feature and provides the procedure for configuring it in WEBconfig.

Port Hopping Overview

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

Port hopping is disabled by default, and only the administrator can enable it. For the procedures to configure port hopping, refer to the following sections:

- To configure port hopping for the entire BBSM server during the initial configuration, run the Switch Discovery Wizard. Refer to the “Running the Switch Discovery Wizard” section on page 5-6.
- To configure ports for port hopping when entering a new network device in WEBconfig, use the Network Element Port Settings pop-up window. Refer to Chapter 13, “Configuring PMS or Print Billing.”
- To configure ports after network devices have been configured, use the Port Control feature. Refer to the chapter on using port control in the Cisco BBSM 5.3 Operations Guide.

When port hopping is enabled, BBSM keeps the session active when the user moves to another port or dissociates temporarily. 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 network, BBSM 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 then deactivates the session, and the user must reauthenticate to regain Internet access.

Port hopping events are logged to the Transaction History report. You can view these transactions through the Reporting Pages link on the Dashboard.
Port Hopping Overview

Note the following operational parameters for port hopping:

- **Searching for end user**—When port hopping is enabled and an end user disappears from the network, BBSM begins searching configured network devices for the end user. BBSM first searches the last known network device that the end user was associated with. If the user is not found, BBSM then searches the other network devices 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 includes the search time in the session duration.
  - If the search fails to find the user before the port hop delay time period expires, BBSM does not include the search time in the session duration. As a result, users who turn off their computers to terminate sessions are not charged BBSM’s search time after they have disconnected.

- **Port hopping between sites**—Port hopping is not allowed across BBSM sites. If a user disappears from the network for less time than the port hop delay time period, the session remains active until BBSM finds the user again on a port at the same BBSM site. However, if BBSM finds the user on a port at a different BBSM site from where the active session originated, the session is deactivated.

  **Note**

  A user could move from the original site, authenticate to another site, and then move back to the original site within the port hop delay time period. BBSM then deactivates the original active session even though the user moved back to the original site. You should deploy your network to prevent overlap between cells on different sites.

- **Port hopping from a port hop disabled port**—Port hopping is enabled on a per-port basis. The end user can 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 cannot hop from a port hop disabled port at all. If this is attempted, BBSM deactivates the session.

- **Port policy**—As the user hops from port to port, the port policy that BBSM associates with the user session follows the user to each new port. BBSM applies the bandwidth limit (in kbps) specified at session activation to the session as the user moves from port to 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.

Port hopping works with any BBSM page set to varying degrees:

- **Wireless network**—Page sets such as DailyHotel that use the BBSM port and room numbers for billing are not useful because rooms are not recognized in wireless networks. The signal from an access point extends beyond walls. Because most access points, such as Cisco Aironet access points, configure all users to the same port number, using the Hotel accounting policy would not provide useful billing information.

- **Wired network**—The BBSM port ID and room numbers are more meaningful when using PMS billing. When using port hopping, BBSM keeps track of the original port and room number to make sure that charges incurred during the session are billed correctly to the user. As a user moves from port to port, although the system reports each new port and location, BBSM bills only the original port and room.
Configuration Procedure

The port hop delay time period sets the number of minutes that BBSM searches for the end user after disassociating from the original port. If the end user is not found within this time frame, the BBSM session is terminated. Port hopping must be configured for each port.

Follow this procedure to set the number of minutes for the port hop delay.

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

**Step 2** In the NavBar, navigate to Port Hopping site x web page by choosing Port Hopping > Site x. The Site x web page appears. (See Figure 20-1.)

**Figure 20-1 Port Hopping Site Web Page**

![Port Hopping Site Web Page](image)

**Step 3** In the Port Hop Delay field, enter the number of desired minutes between 1 and 60. The default number of minutes is 20.

**Step 4** If desired, click Requery to repopulate the web page with the stored data and click Save.
CHAPTER 21
Cisco BBSM 5.3 Configuration Guide
78-15807-01

Configuring Alerts

As of BBSM 5.3, BBSM provides enhanced error reporting. BBSM now creates events in the Windows Application Log for many errors that were previously unreported. Error-notification SNMP traps, called alerts, can be generated by enabling the Alerts option. When this option is enabled, BBSM not only creates Windows events but also generates alerts for them. These alerts can be displayed by using third-party tools.

These are the different options for viewing BBSM events and errors:

- Use the System Summary web page. Refer to the chapter on monitoring performance with the System Summary web page in the Cisco BBSM 5.3 Operations Guide.
- View the application events for BBSM in the Windows Event Log Viewer.
- Enable the Alerts options and use third-party tools to view the SNMP trap alerts.

This section describes how to configure BBSM to generate alerts for system errors.

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

**Step 2** In the NavBar, navigate to the Alerts web page. The Alerts web page appears. (See Figure 21-1.)
Step 3  Configure the Alerts options based on the information shown in Table 21-1 and click Save.

**Table 21-1  Alerts Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Alert</td>
<td>Check this box to generate SNMP trap alerts.</td>
</tr>
</tbody>
</table>
| Alert Level        | Click the lowest level of alert that you want to receive: *Error*, *Warning*, or *Information*. Note the following about the events that will be sent based on the alert levels:  
  - If *Information* is checked, all alerts will be sent.  
  - If *Warning* is checked, only Warning and Error events will be sent.  
  - If *Error* is checked, only Error events will be sent. |
| Trap Destination   | Enter the IP address or FQDN of the SNMP manager that BBSM should send events to. |
| SNMP Community String | Enter the SNMP read-write community string (password) of the SNMP Manager that BBSM should send events to. |
Configuring Port Test Parameters

A port test is an optional test that can be run on client ports to ensure that they have a good connection to the network. Running a port test requires a client to be connected to the port that is being tested. For this reason, port testing is normally done during room mapping after the port is assigned a room number (before disconnecting). Refer to the “Mapping Rooms” section on page 13-9.

If you want to change the default port test parameters, follow this procedure.

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

**Step 2** In the NavBar, navigate to the Port Test Settings web page by choosing **Port Test Settings > Site x > Port Test Settings**. The Port Test web page appears. (See Figure A-1.)

**Figure A-1 Port Test Web Page**

![Port Test Web Page](image)

**Step 3** Configure the port test parameters based on the information shown in Tables A-1 and A-2 and click **Save**.
### Table A-1 Port Test Web Page Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Switch Information</strong></td>
<td></td>
</tr>
<tr>
<td>Site Number</td>
<td>Displays the identifying information for the network element that will use the entered test settings.</td>
</tr>
<tr>
<td>Cluster Number</td>
<td></td>
</tr>
<tr>
<td>Switch Number</td>
<td></td>
</tr>
<tr>
<td>Stack IP Address</td>
<td></td>
</tr>
<tr>
<td>Switch Type</td>
<td></td>
</tr>
<tr>
<td><strong>Test Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Switch Mode</td>
<td>Choose a rate within the ranges that the switch can support. The default is (10\text{Mbps}).</td>
</tr>
<tr>
<td>(in Mbps)</td>
<td></td>
</tr>
<tr>
<td>Pings to Send</td>
<td>Enter the number of pings to send. The range is 300 to 700, and the default is 500.</td>
</tr>
<tr>
<td>Inter Packet Delay</td>
<td>Enter an interpacket delay in milliseconds (msec). (See Table A-2.)</td>
</tr>
<tr>
<td>(in msec)</td>
<td></td>
</tr>
<tr>
<td>Echo Data Size</td>
<td>Enter a size in bytes for the echo data. The range is 768 to 1280, and the default is 1024.</td>
</tr>
<tr>
<td>(in bytes)</td>
<td></td>
</tr>
<tr>
<td><strong>Buttons</strong></td>
<td></td>
</tr>
<tr>
<td>Defaults</td>
<td>Displays the default parameter settings.</td>
</tr>
<tr>
<td>Requery</td>
<td>Refreshes the web page (click before saving changes).</td>
</tr>
<tr>
<td>Save</td>
<td>Saves the changes made to the web page.</td>
</tr>
</tbody>
</table>

### Table A-2 Inter Packet Delay Switch Mode Options

<table>
<thead>
<tr>
<th>Switch Mode (Mbps)</th>
<th>Inter Packet Delay</th>
<th>Default</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>85</td>
<td>85–90</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>45</td>
<td>45–50</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>10–15</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>7</td>
<td>6–9</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>3</td>
<td>1–5</td>
<td></td>
</tr>
</tbody>
</table>
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 B-1, you do not need to make any changes. However, you can change these settings by editing the Windows 2000 registry.

Base your decision of whether or not to change the default bandwidth parameters on the peak number of users that you expect to be using the BBSM server at the same time. However, keep in mind that BBSM continues to operate correctly even if the maximum number of users is exceeded occasionally and performance is degraded.

**Note**
You can only make these changes locally and not from a remote server.

**Caution**
Incorrect registry settings can render your BBSM server unusable. Alter only the parameters listed in Table B-1. Always backup the registry before making any changes.
Follow this procedure to change the registry settings.

Step 1  Choose Start > Run. The Run window appears.
Step 2  Enter regedit and click OK. The Registry Editor window appears.
Step 3  Double-click HKEY_LOCAL_MACHINE.
Step 4  Navigate to System > CurrentControlSet > Services > ATNAT > Parameters.
Step 5  Right-click anywhere in the right pane of the Registry Editor window.
Step 6  To back up the file before making any changes, choose Registry > Export Registry File and follow the instructions.
Step 7  From the New drop-down menu, select DWORD Value.
Step 8  Rename the entry to the parameter name you want to change. For applicable parameter names, see Table B-1 on page B-2.
Step 9  Double-click the new parameter name. (See Figure B-1. Note that BTWQueueSize is shown here only as an example.)

### Table B-1  BBSM Bandwidth Management Configurable Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BWTQueueSize</td>
<td>Amount of data per link to queue before discarding. The default should be adequate for TCP clients. For UDP clients (streaming audio or video), you must select a transmission rate below the bandwidth limit to avoid losing packets because of queue overflow. The default number of bytes is 151,400.</td>
</tr>
<tr>
<td>PacketPoolSize</td>
<td>The number of packet descriptors. The default is 50.</td>
</tr>
<tr>
<td>LookaheadPoolSize</td>
<td>The number of look-ahead buffer descriptors, which the packet descriptor indicates. Set the PacketPoolSize and LookaheadPoolSize parameters to a higher number than the anticipated maximum number of packets queued for bandwidth management. The default is 50.</td>
</tr>
</tbody>
</table>

- 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 6 packets per TCP client.

- For UDP clients, this number is the BTWQueueSize parameter value divided by the packet size. Calculate both and select the larger of the two values. For example, assume that the BWTQueueSize value is 15140 KB. Because the Ethernet packet size is 1514 bytes, divide 15140 by 1514 bytes to establish 10 packets per client. Because 10 is greater than 6, 10 packets per client would be used.
Changing Server Bandwidth Parameter Settings

**Figure B-1  New Parameter Name**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Default)</td>
<td>REG_SZ</td>
<td>(value not set)</td>
</tr>
<tr>
<td>ClientPage</td>
<td>REG_SZ</td>
<td>/algihm/algihm.exe</td>
</tr>
<tr>
<td>ComputerName</td>
<td>REG_SZ</td>
<td>10.10.2.1</td>
</tr>
<tr>
<td>ConnectPage</td>
<td>REG_SZ</td>
<td>/algihm/prepareconnect.asp</td>
</tr>
<tr>
<td>DebugLevel</td>
<td>REG_DWORD</td>
<td>0x00000000 (0)</td>
</tr>
<tr>
<td>DebugMask</td>
<td>REG_DWORD</td>
<td>0x00000000 (0)</td>
</tr>
<tr>
<td>DNSProxy</td>
<td>REG_DWORD</td>
<td>0x00000000 (0)</td>
</tr>
<tr>
<td>EnableTransparentProxy</td>
<td>REG_DWORD</td>
<td>0x00000000 (0)</td>
</tr>
<tr>
<td>LocalMappedAddressEnd</td>
<td>REG_DWORD</td>
<td>0x000002fe (169422836)</td>
</tr>
<tr>
<td>LocalMappedAddressStart</td>
<td>REG_DWORD</td>
<td>0x000002eb (169422803)</td>
</tr>
<tr>
<td>NtpServer</td>
<td>REG_DWORD</td>
<td>0x00000102 (169427778)</td>
</tr>
<tr>
<td>OmitServer</td>
<td>REG_DWORD</td>
<td>0x00000000 (0)</td>
</tr>
<tr>
<td>WebServer</td>
<td>REG_DWORD</td>
<td>0x00000201 (169428035)</td>
</tr>
<tr>
<td>WebServerPort</td>
<td>REG_DWORD</td>
<td>0x00000000 (0)</td>
</tr>
<tr>
<td>BTWQueueSize</td>
<td>REG_DWORD</td>
<td>0x00000000 (0)</td>
</tr>
</tbody>
</table>

The **Edit DWORD Value** dialog box appears. (See Figure B-2.)

**Figure B-2  Edit DWORD Value Dialog Box**

- **Step 10** Click **Decimal**.
- **Step 11** In the Value data field, enter the new value in the appropriate units for that parameter name and then click **OK**. See Table B-1 on page B-2 for a list of parameters.
- **Step 12** To add another parameter, repeat Steps 5 through 11 for each new parameter.
- **Step 13** To change other parameters, repeat Steps 9 through 11 for each parameter.
- **Step 14** Close the Registry Editor window.
- **Step 15** Reboot the server for the new changes to take effect.
GLOSSARY

A

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

access point  A wireless network device that provides physical access to a mobile node.

access policy  An access policy defines how an end user gains access to the Internet through BBSM. The access policy is the BBSM logic that controls the duration of the Internet access for the end user.

access policy module  BBSM ships with several access policy modules. An access policy controls the web user interface that an end user experiences before the session is active, and it also monitors the end user’s session while it is active. An integrator can create a new access policy module by writing a DLL in C++.

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

accounting policy module  BBSM ships with several accounting policy modules. An accounting policy module charges for various services that the access policy module provides. An access policy determines when or if it should invoke an accounting policy module. An integrator can create a new accounting policy module by writing a DLL in C++.

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

Active Server Page  See ASP.

administrator  A user who has authentication rights on the BBSM server. The administrator has full access to control and configure the system; that is, to add and edit sites and PMS systems and gain access to all other resources available on the BBSM system. Administrator access is on a global, not per-site, basis. See also Operator and Reports user.

API  application program interface. An API is the language and message format by which an application program communicates with communications software. Standardized APIs allow application programs to be developed independently of the underlying method of communication. Typically, APIs make it easier for software developers to create the links that an application needs to communicate with the operating system or with the network.

ARP  Address Resolution Protocol. ARP is a protocol for mapping IP addresses to physical addresses in the local network.

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 that information.
AtDial
1. Running as a Windows 2000 service, the component of BBSM configuration and logging data.
2. The BBSM SQL server database that contains BBSM configuration and logging data.

Athdmn
A BBSM service that provides the interface between BBSM and a PMS system. Required to support PMS billing.

authentication
The process by which BBSM identifies users by verifying their credentials, using an external system such as a RADIUS or credit card server.

authorization
The process by which BBSM allows the client access to the Internet by obtaining user credentials for authentication (such as username, password, and credit card number) and other policy preferences, such as bandwidth selection.

B

barred
In the hospitality industry, the term barred is used to describe a guest room that is cash only and not allowed to make charges.

BBSD
(Cisco) Building Broadband Service Director. BBSD is a feature of BBSM that provides centralized usage reporting for a group of BBSM servers.

BBSM
(Cisco) Building Broadband Service Manager. BBSM is an authentication, authorization, and accounting router, built on Windows 2000 technology, that controls access to and charging for Internet access in building-centric applications, such as hotels, apartments, and multi-tenant offices.

bridged network
A bridged network is a network in which all devices are in the same broadcast domain.

byte order
The order of bytes in a binary representation of a number. When transmitted on the Internet, the most significant byte is first; for example, a 16-bit word representation of 256 would be 0x0100. On a host computer, such as an Intel computer, the least significant byte is first; for example, a 16-bit word representation of 256 would be 0x0010.

C

certificate authority
A CA is a company that issues and manages security credentials (certificates). The CA verifies the information that the certificate requestor provides. If the CA successfully verifies the requestor’s information, the CA then issues a certificate to the requestor.

cable modem
A device that enables you to hook up your PC to a local cable TV line and receive high-speed data.

CAS
call accounting system.

certificate
An electronic credential that is used to establish identity during web transactions to secure the communication between the web server and the web browser. The certificate contains sufficient information for the recipient to verify that the certificate is real. See also CA.

certificate authority
See CA.
**certificate request**
A file generated by following the certificate request generation procedure. An administrator generates a certificate request, sends the request to a certificate authority, and receives from the certificate authority a signed certificate for installation on the Microsoft Internet Information Server (IIS).

**client**
The hardware device, such as a laptop or PC, that the end user uses to access the Internet through BBSM. See also end user.

**client search**
The process used to search network devices in a BBSM network to locate the stack, 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 enables a user or developer to launch an application from a terminal and work with it interactively.

**CMTS**
Cable modem termination system. A CMTS is a component that exchanges digital signals with cable modems on a cable network. When a CMTS sends signals to a cable modem, it converts them into IP and sends the signal to a router for transmission over the Internet.

**CNR**
Cisco Network Registrar. CNR is a Cisco DHCP server that runs on Windows or Solaris and can be extended with C++ DLLs.

**COM**
common object model. COM is a platform-independent, distributed, object-oriented system for creating binary software components that can interact. It requires a formal separation of interface and implementation; that is, it requires that clients communicate with objects exclusively through interface references.

**COS**
class of service.

**CPE**
customer premises equipment.

**CSR**
certificate signing request.

**customer**
An individual or organization who purchased BBSM.

**D**

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

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

**default gateway**
The IP address configured on the router that is used as the interface between the BBSM network and the Internet. This IP address is routable.

**deprecated parameter**
An API feature that is still supported but not recommended for use because it may be removed in the future. Usually a newer feature has superseded a deprecated parameter.
DHCP
Dynamic Host Configuration Protocol. DHCP is a protocol that allows TCP/IP settings of a networked computer, called a DHCP client, to be configured automatically from a central DHCP server. In the BBSM network, the BBSM server is a DHCP server, and a guest computer may be a DHCP client.

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

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

external network
BBSM connects the external network to the internal network. BBSM does not enable an end user to transmit packets to the external network until the end user has an active session. See internal network.

F
folio
An itemized list of hotel charges that the end user accrues.

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

FQDN
fully qualified domain name. An FQDN is the part of a URL that defines the server addressed by the URL. For example, the FQDN of http://www.microsoft.com/default.asp is www.microsoft.com.

G
gateway address
The address of the gateway used to reach a specified destination such as a destination on a network or the Internet. Gateways are devices that route packets between different physical networks.

GUI
graphical user interface.
Handheld PC  The Handheld PC is a Microsoft class of PC devices that has a half-sized VGA screen (640 by 240 pixels) or a full-sized screen with or without an integrated keyboard.

HTTP  Hyper-Text Transmission Protocol. HTTP is a TCP protocol used to request and deliver web pages.

ICMP  Internet Control Message Protocol. ICMP is a TCP/IP protocol used to send error and control messages. For example, a router uses ICMP to notify the sender that its destination mode is not available. A ping utility sends ICMP echo requests to verify the existence of an IP address.

IETF  Internet Engineering Task Force. The IETF is the main standards organization for the Internet. It is a large, open, international community of network designers, operators, vendors, and researchers concerned with identifying problems and opportunities in IP data networks and proposing technical solutions to the Internet community.

IIS  (Microsoft) Internet Information Server. IIS is Microsoft’s web server that runs under Windows NT. You can install a certificate on the server to enable it to serve pages using Netscape’s SSL security protocol.

Inetinfo  Inetinfo is the process in the Microsoft IIS in which the BBSM Access Policy ActiveX server components run.

integrator  A software developer that uses the BBSM SDK to extend the functionality of the BBSM.

internal adapter  The internal adapter communicates with the local area network (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 computers, and the BBSM internal interface. See also external network.

IP address  Internet Protocol address. The 32-bit (IPv4) address of a network interface on a computer. A computer with multiple network interfaces typically has a different address for each interface.

iPass Smart Client  The iPass Smart Client is a piece of software on an end-user PC that controls the user experience for gaining access to the Internet in a visitor-based network.

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 enables the BBSM administrator to generate a certificate request and install a signed certificate.

**KeyView Pro**
A desktop utility that provides instant access to virtually all the popular file formats for viewing, printing, or converting files to Rich Text Format (RTF).

### L

**LAN**
local area network.

**LRE**
long-reach Ethernet.

### M

**MAC address**
Media Access Control address. The MAC address is the client’s unique hardware number. BBSM uses the MAC address to identify the location (or port) of a client. After BBSM identifies the port that a client is using, BBSM applies the per-port policy to the client session.

**mapped port**
The port has an entry in the port_map table. The values in the Room_number and Time_of_last_configure fields may be either default values or updated values.

**mapped room**
Because enterroom.asp has been run successfully from the port, the port’s port_map table entry has a correct room number value in the Room_number field and a time and date value in the Time_of_last_configure field.

**Mbps**
megabits per second (millions of bits per second). Mbps is a measure of bandwidth on a data transmission medium.

**MDU**
multiple dwelling unit.

**META tag**
A special HTML tag that provides information about a web page. Unlike normal HTML tags, meta tags do not affect how the page is displayed. Instead, they provide information such as who created the page, how often it is updated, what the page is about, and which keywords represent the page’s content. Many search engines use this information when building their indices.

**MFC**
Microsoft Foundation Classes. MFC is a library of C++ classes that Microsoft developed.

**MHU**
multiple hospitality unit.
MIB  management information base.
mixed network  BBSM supports networks that contain a mixture of bridged and routed networks by combining bridged and fully routed network associations. Some switches reside on the BBSM server’s internal network, and others are accessible through routers on the internal network.
MMC  Microsoft Management Console. The MMC is a Windows-based application that provides a GUI and a programming framework in which consoles (collections of administrative tools) can be created, saved, and opened.
module  A software component that implements the functionality of the BBSM system. BBSM supports access policy modules, accounting policy modules, property management system (PMS) modules, and network device 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 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. This allows a company to shield internal addresses from the Internet.
NE  network element. An NE is a device connected to the internal network. An end user connects his or her computer to an NE, and then BBSM queries the NE to determine the end user’s location.
network  A network connects all buildings, sites, and ports together with the BBSM server. The network is configured with routers, switches, and other network hardware. BBSM supports bridged networks, fully routed networks, and mixed networks that are a combination of bridged and fully routed networks. See also bridged networks, fully routed networks, and mixed networks.
network byte order  The order of bytes in a binary representation of a number as transmitted on the Internet. The most significant byte is first; for example, a 16-bit word representation of 256 would be 0x0100.
network element  See NE.
network device module  BBSM ships with support for several types of network equipment, such as a variety of Ethernet switches, DSL access multiplexers, and cable modem head ends. A developer can add support for new equipment by writing a network device DLL in C++.

NIC  network interface card. The NIC is an adapter card inserted into a computer to provide network communication capabilities. It connects the server to the network. It is also referred to as an Ethernet adapter.

operator  A BBSM user who can perform some administrative functions on the BBSM server but does not have access to the full administrative interface. An operator is allowed to change entries in the port map and access code tables. Operator access is on a per-site basis. See also Administrator and Reports user.

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

package file  An ASP file (page) included in some page sets that defines configuration information for the page set. 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.

page set  A set of active server page (ASP) files that the end user can view and that the administrator specifies for each port. BBSM restricts the end user from viewing pages that are part of any page set other than the port’s allowed page set. BBSM ships with several template page sets that implement various end-user interfaces. You can use these page sets to create custom page sets that reflect your own business.

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 handheld computer that enables you to store, access, and organize information. Most PDAs work on either a Windows-based or a Palm operating system. PDAs can be screen based or keyboard based, or both.

plug and play  A set of features that allows a client to access the Internet without reconfiguring network and browser settings.

PMS  property management system. A PMS is a software system used in the hospitality industry to manage customer accounting and billing.

PNF  patch information file. A PNF is a text file that contains sections and keys that include all the information that WEBpatch needs to install a patch.

Pocket PC  A Pocket PC is a Microsoft class of PC devices that has a quarter-sized VGA screen (320 by 240 pixels).

policy  Any rule that determines the use of resources within the network. A policy can be based on the user, the port, the device, the subnetwork, the network, or the application.
port

The jack into which an end user connects a PC to access the Internet. In the case of a wireless network device, such as an access point, the port is a virtual jack. BBSM enables the administrator to configure the page set and start page on a per-port basis.

port hopping

A feature that enables 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.

post page

An ASP file (page) included in page sets that displays the Connecting... message. The post page calls the functions needed to connect the end user.

Property Management System

See PMS.

pre-connect page

A web page that implements logic to determine the physical location of the client requesting the page. Used by the policy server to determine the access and accounting policies that apply to a client session.

pseudo-debug

A Microsoft Visual C++ project build configuration that generates executables and DLLs that contain symbolic debug information but invoke the release version of the Microsoft memory management library. Release executables and DLLs can invoke pseudo-debug DLLs so developers of pseudo-debug DLLs can debug their DLLs in a release environment.

Q

QoS

quality of service. QoS usually refers to the prioritization of packets over a network.

R

RADIUS

Remote Authentication Dial-In User Service. RADIUS is a client/server protocol and software that enables network access servers to communicate with a central server to authenticate dial-in users, authorize their access to the requested system or service, and send accounting information about their use of the requested system or service.

redirect

The procedure by which a web server tells a web browser to obtain a certain requested page from a different location.

remote client

A hardware device, such as a laptop or PC, through which an end user accesses a BBSM server from the external network.

Reports

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

Reports user

A BBSM user who has read-only access to the Reports web applications. This user has more access permissions than an end user but fewer access permissions than an Operator. A Reports user has access to the information for only one site. See also Operator and Administrator.

RFC

Request for Comments. An RFC is a series of notes on topics concerning the Internet. RFCs can be purely informational, or they can specify a proposed, draft, or approved Internet standard. Online versions of RFCs are available at the following URL: http://www.ietf.org/rfc.html
rogue user  
An end user who attempts to access the BBSM server fraudulently or maliciously.

rout ed network  
In routed networks, some computers cannot communicate with each other directly. Instead, they must send packets through one or more relays (routers). In a routed network, the only plug-and-play feature that works is redirection of the initial web page request.

RX  
A communications abbreviation for receive, as contrasted with transmit.

S

SDK  
software developer’s kit. An SDK is a set of routines and utilities that developers use to write an application. The BBSM SDK is used to customize and extend the functionality of the BBSM server.

server reboot  
In the BBSM system, the situation in which the server is powered off or shut down for any reason (such as a power outage or patch installation) and the server restarts. When the BBSM server is shut down, clients lose access to the Internet and BBSM services, and active sessions are disrupted. End users cannot connect to the BBSM server or terminate active sessions. After the server restarts, clients still may not be able to resume active sessions because session states are not preserved across server reboots.

server-side script  
A series of statements that a web server executes when a client’s browser requests a page.

service restart  
The situation in which BBSM service has stopped for any reason (such as being stopped through WEBconfig) and BBSM 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 BBSM 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 or unplugging the Ethernet connection, or the client’s moving out of range).

session  
A set of interactions between an end user and BBSM. The session starts when BBSM serves the page set’s start page. At this point, the session is inactive, which means that the user does not have access to the Internet. The session becomes active when BBSM authorizes the user to access the Internet according to the access policy and accounting policy that are specified by the page set. The session ends when AtDial deactivates service for the end user. Note that transactions pertaining to the session can still exist after the session deactivates. These transactions are still associated with that session.

site  
In BBSM documentation, a site is a collection of clients behind network devices connected to the Internet through a single network device. It is a subset of the BBSM internal network. Each network device and all of its ports are associated with exactly one site. One or more mutually exclusive sites always exist in the BBSM internal network. A site is often a single geographic location, such as a single hotel or large building.

SMTP  
Simple Mail Transfer Protocol. SMTP is a TCP/IP protocol used for sending email 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 enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

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 | An ASP file (page) included in page sets that defines the first page displayed to the end user sees when he or she attempts to connect to the Internet. The start page prompts the user to authenticate for authorization to access the Internet. |
| subscription | A subscription is a period during which BBSM enables the end users to create sessions. If a user attempts to create a session outside any subscription period, BBSM denies the session. |
| switch | 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 device. |
| **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. A TCP port is a port (on an Internet host) that is supporting a particular networking application that needs a unique identity. |
| **Terminal Services** | A Microsoft remote management tool that comes enabled on the BBSM 5.3 appliance. It can be used to access and manage the server remotely. |
| **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. |
| **ToD** | An abbreviation for time of day when used in the term ToD server. |
| **TX** | A communications abbreviation for transmit, as contrasted with receive. |

| 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 Internet web sites that unauthenticated BBSM end users can access.

**WEBpatch**  The web-based utility included with BBSM that allows remote updates to the BBSM server.

**web service**  A programmable entity that provides a particular device 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 a PDA (Microsoft Handheld PC).

**WISPr**  Wi-Fi service provider roaming.

---

**X**

**XML**  extensible markup language. XML is a standard format for data on the web. It enables developers to describe and deliver structured data to and from any application.

**XML document**  An XML device that can include nested XML devices. *See also XML device.*

**XML device**  An XML device is made up of a start tag, an end tag, and data in between the tags. The starting and ending tags describe the data within the tags, which is the value of the device. For example, `<IP>192.168.10.1<IP>` is an XML device. *See also XML.*
A

Access Code Management option 17-8
access codes
and meeting rooms 17-17
and time zones 17-18
bandwidth options 8-3
cannot be used with PMS billing 17-9
managing 17-8
accessing the BBSM Dashboard
locally 1-7
remotely 1-7
access points
configuring 12-2
deleting 12-5
security 8-2, 16-2
Access Points web page 12-2
access policies 18-2
accounting policies 18-2
adding
BBSM sites 10-1
cable modems 13-13
custom page sets to BBSM 18-17
new Operators 1-11
new Reports users 1-11
PMS call types 13-6
VLANs, reconfiguring the access point 12-4
Address Change Wizard
deleting multinet 2 3-4
running 5-1
Administrator, entering password 3-2
Administrators user group 1-8
aging period
for CMTSs 12-11
for switchetime
aging period for automatic disconnection, switches 12-14

B

bandwidth
configuring management options 8-1
configuring reservation options 17-3
managing and reserving 17-8
reservation
configuring classes of service 17-6
configuring total bandwidth 17-5
overview 17-1
reservations
verifying the external router 17-3
specifying 14-5
throttling
configuring 8-3
definition 17-1
overview and configuration procedure 17-3
bandwidth, changing default server parameter settings 8-1
Bandwidth Reservation
web pages
Classes of Service 17-6
Bandwith Reservation
web pages
External Router 17-3
Total Bandwidth 17-5
BBSM server
documentation ix
router 0 1-3
BBSM Server Settings web page 8-1
billing
credit card 15-1
PMS 13-1
print 13-1
RADIUS 14-3
boundary, session 18-15
Bridged-Configuration CMTS configuration web page 12-11
bridged networks 1-4
C

cable modems
  configuring CMTSs for 12-7
  replacing or adding 13-13

Call Types web page 13-6
certificate, installing 16-2
  changing
    default server bandwidth parameter settings 8-1
    internal network IP addresses 9-1
    port settings 13-13

classes of service
  overview 17-6

Client for Microsoft Networks check box, unchecking 13-8

clients
  connecting to BBSM 1-12

  clock, changing while clients connected 3-2

clustering
  overview 12-2
  Switches web page 12-12

CMTSs
  configuring 12-7
  dynamic port-room configuration procedure 13-13

CMTS web page 12-7

configuring
  access codes 17-8
  access points 12-2
  bandwidth management options 8-1
  bandwidth reservation
    classes of service 17-6
    options 17-3
    total bandwidth 17-5
    verifying the external router 17-3

BBSM sites 10-1

credit card billing
  configuring 15-1
  merchant ID 15-3
  testing the credit card interface 15-4
  credit card interface, testing 15-4

currency type 8-2

custom page sets 18-13

Custom Page Sets web page 18-17

CyberSource credit card interface 15-4

D

Dashboard options 1-7

Administration
  Page Set Wizard 1-8
WEBconfig 1-8
WEBpatch 1-8
WEB PMS Test 1-8

Operations
  Access Code Management 1-11
  Client Deactivation 1-11
  Map Rooms 1-11
<table>
<thead>
<tr>
<th>Port Control</th>
<th>1-11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports</td>
<td>1-11</td>
</tr>
<tr>
<td>Deleting</td>
<td></td>
</tr>
<tr>
<td>Access points</td>
<td>12-5</td>
</tr>
<tr>
<td>dual-VLAN config</td>
<td>5-3</td>
</tr>
<tr>
<td>multinet 2</td>
<td>5-5</td>
</tr>
<tr>
<td>PMS call types</td>
<td>13-7</td>
</tr>
<tr>
<td>Routers</td>
<td>11-3</td>
</tr>
<tr>
<td>Sites</td>
<td>10-3</td>
</tr>
<tr>
<td>Switches</td>
<td>12-15</td>
</tr>
<tr>
<td>DHCP IP addresses</td>
<td></td>
</tr>
<tr>
<td>Changing in WEBconfig</td>
<td>9-1</td>
</tr>
<tr>
<td>Entering ranges in the Address Change Wizard</td>
<td>5-1</td>
</tr>
<tr>
<td>DHCP IP address ranges</td>
<td></td>
</tr>
<tr>
<td>Temporary</td>
<td>9-6</td>
</tr>
<tr>
<td>DNS</td>
<td></td>
</tr>
<tr>
<td>Forwarding, configuring</td>
<td>6-1</td>
</tr>
<tr>
<td>Resolving requests</td>
<td>6-1</td>
</tr>
<tr>
<td>Documentation, related</td>
<td>ix</td>
</tr>
<tr>
<td>Duplicate IP address feature, configuring</td>
<td>8-2</td>
</tr>
<tr>
<td>Installing service packs and patches before BBSM configuration</td>
<td>3-4</td>
</tr>
<tr>
<td>SSL certificate</td>
<td>16-2</td>
</tr>
<tr>
<td>Internet browser</td>
<td></td>
</tr>
<tr>
<td>Accessing the Dashboard</td>
<td>1-7</td>
</tr>
<tr>
<td>Browsers</td>
<td></td>
</tr>
<tr>
<td>Configuring for room mapping</td>
<td>13-9</td>
</tr>
<tr>
<td>Inter packet delay, Port Test Settings option</td>
<td>A-2</td>
</tr>
<tr>
<td>IP addresses</td>
<td></td>
</tr>
<tr>
<td>Changing in WEBconfig</td>
<td>9-1</td>
</tr>
<tr>
<td>Duplicate</td>
<td>8-2</td>
</tr>
<tr>
<td>Entering in the Address Change Wizard</td>
<td>5-1</td>
</tr>
<tr>
<td>Public-private overview</td>
<td>9-2</td>
</tr>
<tr>
<td>IP Addresses web page</td>
<td>9-1</td>
</tr>
<tr>
<td>IPSec</td>
<td>2-5</td>
</tr>
<tr>
<td>IRB-Configuration CMTS configuration web page</td>
<td>12-9</td>
</tr>
<tr>
<td>E</td>
<td>16-3, 18-2</td>
</tr>
<tr>
<td>EAP support with wireless LANs</td>
<td>12-2</td>
</tr>
<tr>
<td>Echo data size, Port Test Settings option</td>
<td>A-2</td>
</tr>
<tr>
<td>Enabling</td>
<td></td>
</tr>
<tr>
<td>Bandwidth management</td>
<td>8-3</td>
</tr>
<tr>
<td>End user connection sequence</td>
<td>1-12</td>
</tr>
<tr>
<td>Example, changing page set parameters</td>
<td>18-13</td>
</tr>
<tr>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Features, advanced</td>
<td>2-1</td>
</tr>
<tr>
<td>Find Access Codes web page</td>
<td>17-15</td>
</tr>
<tr>
<td>Foreign (Static) IP address ranges</td>
<td></td>
</tr>
<tr>
<td>Changing in WEBconfig</td>
<td>9-1</td>
</tr>
<tr>
<td>Entering in the Address Change Wizard</td>
<td>5-1</td>
</tr>
<tr>
<td>H</td>
<td></td>
</tr>
<tr>
<td>HTTPS, with SSL</td>
<td>16-2</td>
</tr>
<tr>
<td>M</td>
<td></td>
</tr>
<tr>
<td>Management IP address ranges</td>
<td></td>
</tr>
<tr>
<td>Changing in WEBconfig</td>
<td>9-1</td>
</tr>
<tr>
<td>Entering in the Address Change Wizard</td>
<td>5-1</td>
</tr>
<tr>
<td>Managing</td>
<td></td>
</tr>
</tbody>
</table>
access codes 17-8
bandwidth 8-3
mapping
  access points 12-2
  CMTS ports 12-7
  locations 13-9
  rooms for cable modems 13-13
  rooms for switches and access points 13-10
  switches 12-12
Map Rooms option 13-9
meeting rooms
  and access codes for 17-17
  and time zones 17-18
Microsoft
  Microsoft ISA used by BBSM for proxy server 2-7
  Microsoft Management Console (MMC) 16-13
  server security 16-1
modifying
  DailyHotel page sets using the Page Set Wizard 18-5
MSDE
  functionality breaks if BBSM appliance renamed 3-1
multinets
  and subnets 9-2
  assigning in Management range 9-6
  configuring
    IP addresses 9-5
    Windows for 3-4
deleting multinet 2 5-5
page sets and provisioning by administrator or end user 18-2
private-public IP address overview 9-2
running
  Address Change Wizard 5-1
  Switch Discovery Wizard 5-6

N

NAS identifier 14-6, 14-8
NAT
  IP address 14-5, 14-8
  with VPN clients 2-5
navigational buttons 1-12
networks
  bridged 1-4
  routed 1-4

O

Operators user group 1-11

P

page sets
  custom
    adding to BBSM 18-17
    using the Page Set Wizard 18-5
  multinet provisioning by administrator or end user 18-2
  registering 18-16
  renaming 18-13
  using
    with BBSM, overview 18-2
    with SSL 16-3, 18-2
Page Set Wizard 18-5
passwords 3-2
  RADIUS 14-3
  setting for new sites 10-4
  SNMP 11-3, 12-5, 12-11, 12-14
patches
  installing
    before BBSM configuration 3-4
permissions 1-6
pings to send, Port Test Settings option  A-2
PMS
  billing not supported by access code page sets 17-9
  configuring billing options 13-1
  connecting 7-1
  supported protocols 13-2
  testing the interface (WEB PMS Test) 7-3
  two-way interface 13-2
  verifying that charges are posting 7-4
PMS/Printer Settings web page 13-4
port 9488 1-7
port hop delay, configuring 20-3
port hopping
  configuring port hop delay 20-3
  description 20-1
Port Hopping Site x web page 20-3
port test parameters, configuring  A-1
Port Test Settings web page  A-1
prepaid RADIUS 14-2
index

print billing 13-1
printing
 connecting a local printer 7-1
private and public IP addresses
 configuring 9-5
 overview 9-2
procedures
 creating custom page sets 18-13
protected port feature, configuring 8-2
protected port feature, security 16-2
proxy server 2-7
PSPF feature, configuring 8-2
publications, related ix
publicly secure packet forwarding (PSPF) 16-2
public secure packet forwarding (PSPF), configuring 8-2
\q
QoS, Class-Based Shaping used instead by BBSM 17-1
\r
RADIUS
 configuring 14-3
 prepaid 14-2
 Server web page 14-3
 Site x web page 14-9
 using with BBSM 14-1
 with user-provisioned bandwidth (UBand page sets) 14-2
registering
 page sets 18-16
remote access
 to Dashboard 1-7
 unchecking Client for Microsoft Networks 13-8
removing VLANs, reconfiguring the access point 12-4
renaming page sets 18-13
replacing, cable modems 13-13
Reports user group 1-11
requirements, connecting an end-user client to BBSM 1-12
reserving bandwidth 17-8
Reset Time Remaining, with Codes by Duration web page 17-13
resolving DNS requests 6-1
retrieving overwritten page sets 18-13
roaming, using access points 12-2
room mapping
 basic procedure 13-10
 configuring laptops 13-7
dynamic port-room CMTS procedure 13-13
Routed CMTS configuration web page
 multinet 12-10
routed networks 1-4
router 0 1-3
routers
deleting 11-3
external
 configuration added by bandwidth reservation feature 17-2
 restoring router configuration 17-4
 verifying for bandwidth reservation 17-3
internal
 configuring 11-1
 restrictions when using "Router Supports SNMP" 11-3
Routers web page 11-1
 supporting SNMP 11-3
\s
sample, changing page set parameters 18-13
security
 accounting policies 18-2
 configuring 16-16
 configuring PSPF (port-to-port security) 8-2, 12-2, 16-2
 entering SQL 'sa' and Windows Administrator passwords 3-2
Security/SSL web page 16-16
service packs
 installing
 before BBSM configuration 3-4
session boundary 18-15
single nets
 and subnets 9-2
 configuring IP addresses 9-5
private-public IP address overview 9-2
sites
 configuring 10-1
deleting 10-3
setting passwords for 10-4
Sites web page 10-1
SMTP forwarding 8-2
SSL
configuring 16-16
installing certificate 16-2
logging into BBSM remotely 1-7
Security/SSL web page 1-10
SSL page sets disabled when SSL not installed on BBSM server 1-2, 5-14
using with page sets 16-3, 18-2
subnets, with singlenets and multinet 9-2
supported PMS protocols 13-2
Switch Discovery Wizard
enabling clustering 12-2
running 5-6
switches
clustering overview 12-2
deleting 12-15
switch mode, Port Test Settings option A-2
system clock, changing while clients connected 3-2
system requirements 1-2

T
TCP/IP properties 9-7
Temp DHCP address ranges
changing in WEBconfig 9-1
entering in the Address Change Wizard 5-1
testing
credit card interface 15-4
PMS interface 7-3
time
aging period for automatic disconnection, CMTSs 12-11
changing system clock 3-2
initialization and number of IP addresses 9-7
lease with DHCP 9-7
preconfigured period of inactivity with disconnection 12-3
Reset Time Remaining with Codes by Duration web page 17-13
zones and access codes 17-18
timeout period, IIS 14-8
topics, advanced 2-1
transparent proxy
enabling 8-2
logging proxy entries 8-3
remote proxy servers 2-8
web proxy overview 2-7
troubleshooting
IP addresses 9-5
TCP/IP properties 9-5
two-way PMS interface 13-2

U
UBand page sets, using with RADIUS servers 14-2
uplink ports
defined 12-13
user groups 1-6
Administrators 1-8
Operators 1-11
Reports 1-11
users
adding
Operators 1-11
Reports users 1-11

V
VLANs
adding or removing a VLAN and reconfiguring the access point 12-4
configuring Windows for dual VLANs 4-1
overview 2-4
VPN clients
using with BBSM 2-5
with public-private IP addressing 9-2

W
walled gardens
creating and configuring 19-1
Walled Garden web page 19-1
web proxy
overview 2-7
used with walled gardens 19-1
WEBconfig
   Access Points web page 12-2
   Bandwidth Reservation
      Classes of Service web page 17-6
      External Router web page 17-3
      Total Bandwidth web page 17-5
   BBSM Server Settings web page 8-1
   Bridged-Configuration CMTS configuration web page 12-11
   Call Types web page 13-6
   CMXS web page 12-7
   Credit Card
      Server web page 15-1
      Site x web page 15-3
   Custom Page Sets web page 18-17
   IP Addresses web page 9-1
   IRB-Configuration CMTS configuration web page 12-9
   PMS/Printer Settings web page 13-4
   Port Hopping Site x web page 20-3
   Port Test Settings web page A-1
   RADIUS
      Server web page 14-3
      Site x web page 14-9
   Routed CMTS configuration web page
      multinet 12-10
   Routers web page 11-1
   Security/SSL web page 16-16
   Sites web page 10-1
   Switches web page 12-12
   Walled Garden web page 19-1
WEB PMS Test option 7-3
Windows
   adding
      Operators 1-11
      Reports users 1-11
   adding Reports users 1-11
   changing
      the name of BBSM appliance breaks MSDE functionality 3-1
   configuring
      dual VLANs 4-1
      laptops and browsers for room mapping 13-7
      multinets 3-4
   entering
      Administrator password 3-2
   using Network and Dial-up Connections only to set up multinets, not to set IP addresses 5-3
   wizards
      Address Change 5-1
      Page Set 18-5
      Switch Discovery 5-6