



Cisco BBSM 5.3 Operations Guide

Software Release 5.3
November 2003

Corporate Headquarters

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

Customer Order Number: DOC-7816161=
Text Part Number: 78-16161-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)



Preface v

Conventions	v
Related Publications	vi
Obtaining Documentation	vi
Cisco.com	vi
Documentation CD-ROM	vi
Ordering Documentation	vii
Documentation Feedback	vii
Obtaining Technical Assistance	vii
Cisco TAC Website	vii
Opening a TAC Case	viii
TAC Case Priority Definitions	viii
Obtaining Additional Publications and Information	viii

CHAPTER 1

Deactivating and Reactivating Client Sessions 1-1

Deactivating Client Sessions	1-2
Reactivating Client Sessions	1-4

CHAPTER 2

Viewing and Printing Reports 2-1

Accessing Reports	2-1
Usage Reports	2-2
Transaction History Reports	2-4
Active Ports Report	2-7
Access Code Reports	2-8
Access Code Report	2-9
Unused Code Report	2-10
Access Code History Report	2-13
Mapping Report	2-15
Viewing the Mapping Report	2-16
Editing Mapping Report Entries	2-17
RADIUS Session History Report	2-19
Walled Garden Report	2-21

CHAPTER 3

Monitoring Performance (System Summary) 3-1

CHAPTER 4

Using Port Control 4-1

Changing the Port Settings for a Single Port 4-2

Changing the Port Settings for a Multiple Ports 4-6

Replacing, Adding, or Removing a Cable Modem 4-7

CHAPTER 5

Installing Service Packs or Patches (WEBpatch) 5-1

Before You Start 5-1

Patch Installation Procedure 5-2

CHAPTER 6

Troubleshooting 6-1

Clearing Pending Hotel Charges 6-1

Troubleshooting Tips 6-3

No BBSM Start Page 6-3

No Internet Access 6-4

Email Not Working 6-4

PMS Charges Not Posting 6-5

RADIUS Problems 6-6

Software Download Failures 6-6

BBSM Not Functioning 6-8

Using the Trace Debugging Utility 6-9

GLOSSARY

INDEX



Preface

This guide is written for the personnel responsible for operating the Building Broadband Service Manager (BBSM) after it has been configured. 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 result enables service providers to offer Internet services on a port-by-port basis.



Note

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 accesses the Internet through the BBSM system.

This guide is organized into the following chapters:

- [Chapter 1, “Deactivating and Reactivating Client Sessions,”](#) describes how to deactivate one or more active sessions, temporarily or permanently, and reactivate a permanently deactivated client.
- [Chapter 2, “Viewing and Printing Reports,”](#) describes how to view and print reports of BBSM activities and functions for each site.
- [Chapter 3, “Monitoring Performance \(System Summary\),”](#) explains the System Summary, which is a single web page that enables you to monitor the BBSM system status and all BBSM services.
- [Chapter 4, “Using Port Control,”](#) describes how to update network device port data and test the ports.
- [Chapter 5, “Installing Service Packs or Patches \(WEBpatch\),”](#) describes how to view, transfer, and install service packs or patches and view the patch log.
- [Chapter 6, “Troubleshooting,”](#) provides troubleshooting tips.

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 Configuration Guide* (order number DOC-7814689=)
- *Cisco BBSM 5.3 SDK Developer Guide* (available on Cisco.com)
- *Cisco BBSM 5.3 Software Installation Guide* (order number DOC-7815714=)

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:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpc/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- 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:

<http://tools.cisco.com/RPF/register/register.do>

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:

<http://www.cisco.com/en/US/learning/index.html>



Deactivating and Reactivating Client Sessions

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

Cisco strongly recommends deactivating all client sessions when installing service packs, patches, and upgrades.

You may also want to deactivate a client for security reasons or problems related to one client. If you discover that one client is causing problems such as using too much bandwidth, downloading illegal content, or spreading viruses, you can deactivate it on the Deactivate Clients web page by using the client IP address or location.

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

- A temporary deactivation allows clients access to the Connect page so they can reconnect immediately after they are disconnected.
- A permanent deactivation prevents the client from reconnecting unless an administrator or operator reactivates the client. The client's MAC address is disallowed from the network, but the IP address is not.

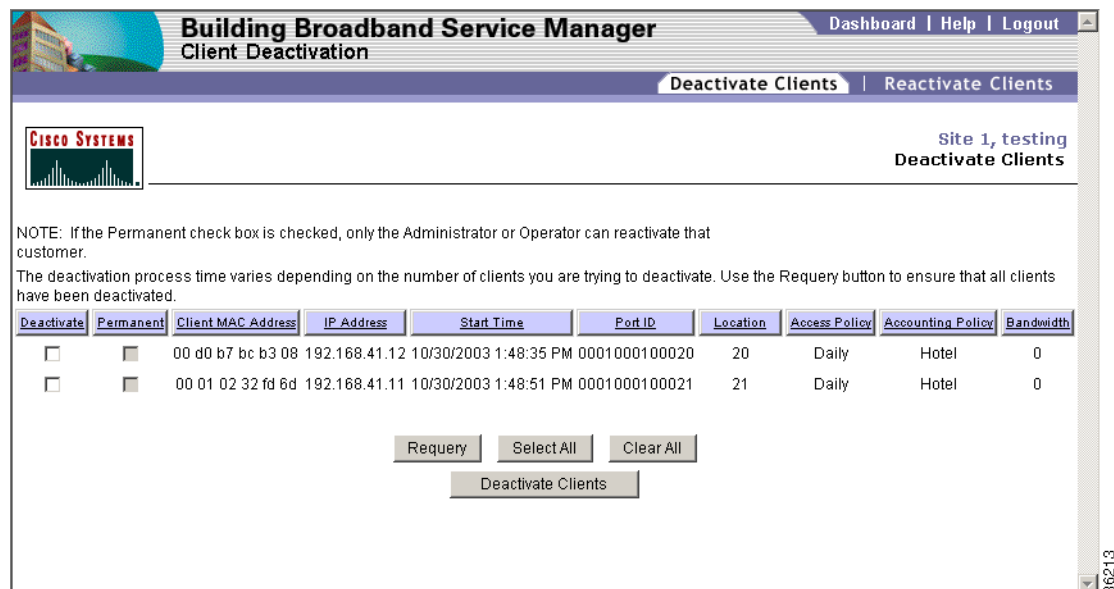
When navigating through the sessions, note that you can sort each column in ascending or descending order by clicking the column heading.

Deactivating Client Sessions

Follow this procedure to temporarily or permanently deactivate client sessions.

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

Figure 1-1 Deactivate Clients



- Step 2** Select the client sessions you want to temporarily or permanently deactivate based on the information shown in [Table 1-1](#).
- Step 3** Click **Deactivate Clients**. When a permanently deactivated client tries to access the Internet, the client is redirected to the Deactivated Session web page.

Table 1-1 Deactivate Clients Options

Option	Description
Deactivate	Check the box to select the session for deactivation.
Permanent	After you have checked Deactivate, check this box to select the session for permanent deactivation.
Client MAC Address	Displays the client's MAC address.
IP Address	Displays the client's IP address.
Start Time	Displays the date and time that the client's session began.
Port ID	Displays the port ID number that the client is connected to. For an explanation of the Port ID, refer to Chapter 4, "Using Port Control."
Location	Displays the end user's location number.
Access Policy	Displays the access policy that is applied to this user.
Accounting Policy	Displays the accounting policy that is applied to this user.
Bandwidth	Displays the end user's bandwidth rate.
Buttons	
Requery	Refreshes the web page (before clicking Deactivate Clients).
Select All	Selects all client sessions at once.
Clear All	Deselects all client sessions.
Deactivate Clients	Deactivates the client sessions that you checked.

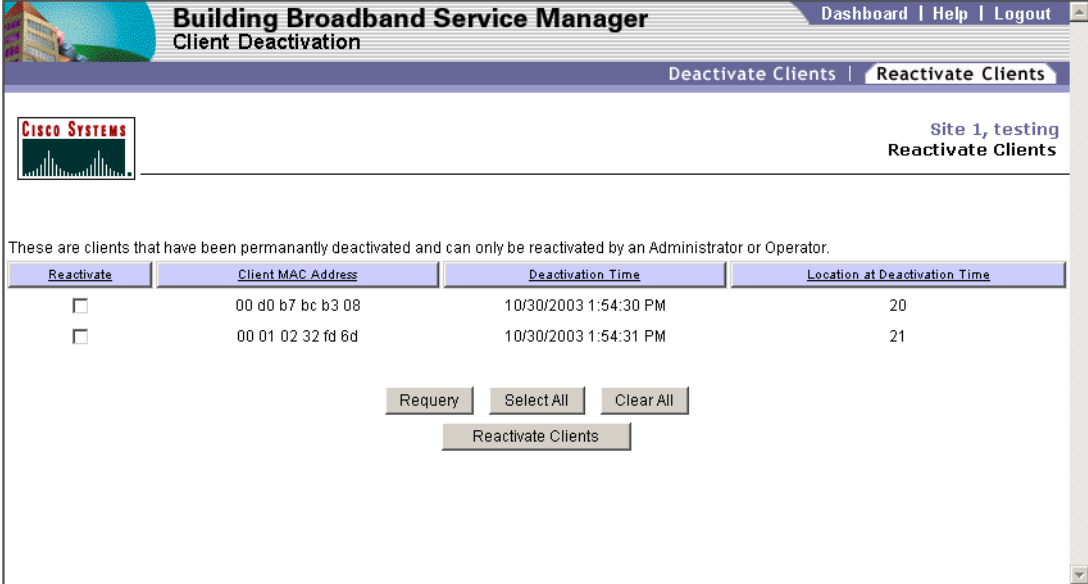
Reactivating Client Sessions

When clients are permanently deactivated, the deactivation is absolutely permanent unless an administrator or operator reactivates them.

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

- Step 1** From the Dashboard, click **Client Deactivation**. The Deactivate Clients web page appears. (See [Figure 1-1](#).)
- Step 2** Click **Reactivate Clients**. The Reactivate Clients web page appears. (See [Figure 1-2](#).)

Figure 1-2 Reactivate Clients



Building Broadband Service Manager
Client Deactivation

Dashboard | Help | Logout

Deactivate Clients | **Reactivate Clients**

CISCO SYSTEMS Site 1, testing
Reactivate Clients

These are clients that have been permanently deactivated and can only be reactivated by an Administrator or Operator.

Reactivate	Client MAC Address	Deactivation Time	Location at Deactivation Time
<input type="checkbox"/>	00 d0 b7 bc b3 08	10/30/2003 1:54:30 PM	20
<input type="checkbox"/>	00 01 02 32 fd 6d	10/30/2003 1:54:31 PM	21

Requery Select All Clear All

Reactivate Clients

86247

- Step 3** Reactivate the appropriate clients based on the information shown in [Table 1-2](#).
- Step 4** Click **Reactivate Clients**.

Table 1-2 *Reactivate Client Options*

Option	Description
Reactivate	Check this check box to reactivate a client that was permanently deactivated.
Client MAC Address	Displays the client's MAC address.
Deactivation Time	Displays the date and time that the client was permanently deactivated.
Location at Deactivation Time	Displays the physical location of the client that was permanently deactivated.
Buttons	
Requery	Refreshes the web page (before clicking Reactivate Clients).
Select All	Selects all of the clients.
Clear All	Deselects all of the clients.
Reactivate Clients	Reactivates the permanently deactivated clients.



Viewing and Printing Reports

You can view and print reports of BBSM activities and functions for each site by clicking the **Reporting Pages** option on the Dashboard. Use Internet Explorer to view any of the following reports:

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

Accessing Reports

Follow this procedure to access BBSM reports.

-
- | | |
|---------------|---|
| Step 1 | From the Dashboard, click Reporting Pages . The Usage Report Options web page appears. |
| Step 2 | To request a report, click a report on the menu bar at the top of the web page. (See Figure 2-1 .) |
| Step 3 | For all report web pages, select a sorting method by clicking a column heading. Clicking the heading a second time switches the order of rank between ascending and descending. |
-

Usage Reports

Usage reports enable you to obtain site Internet-use data for a day, month, or year. By default, the time ranges are based on the time that the charge is posted to the PMS. The posted charges span the 24 hours leading up to the posting time. For example, if a hotel sends its PMS data to its data-processing center at 4 a.m. each day, the posted charges include data from 4 a.m. the previous day to the 4 a.m. the current day.

The Calendar Day Offset feature enables you to realign the time boundaries with another time such as guest check-out. The feature normally indicates the date change at midnight. When the clock reaches midnight, the date is advanced; for example, *11:59pm Oct 27* advances to *12:00am Oct 28*. If you change the time at which the date is advanced to 4 a.m., then *3:59am Oct 27* advances to *4:00am Oct 28*. This change applies only to the report; it does not affect the data.

Refer to the following example of how the Calendar Day Offset feature affects the dates displayed on reports:

- A charge is posted at 6 p.m. on January 3, 2002.
- If the Calendar Day Offset is set to *12:00am* (midnight), the 6 p.m. charge would be displayed on the Usage By Day report as being posted on January 3.
- If the Calendar Day Offset is set to *4:00pm*, charges posted after 4 p.m. are considered to be posted on the next day, so the 6 p.m. charge would be displayed on the report as being posted on January 4.

Follow this procedure to generate and view usage reports.

- Step 1** From the Dashboard, click **Reporting Pages**. The Usage Report Options web page appears. (See [Figure 2-1](#).)

Figure 2-1 Usage Report Options

The screenshot shows the 'Building Broadband Service Manager' interface. At the top, there's a navigation bar with 'Dashboard | Help | Logout'. Below it, a secondary navigation bar includes 'Usage | Transaction History | Active Ports | Access Codes | Mapping | RADIUS | Walled Garden'. Under 'Usage', there are links for 'Usage By Year | Usage By Month | Usage By Day'. The main content area is titled 'Usage Report Options' and includes a Cisco Systems logo. It instructs the user to 'Use the form below to choose a usage report based on time parameters.' The form contains a 'Report Type' dropdown menu set to 'Usage By Day', a 'Calendar Day Offset' section with input fields for '3', '00', and a time dropdown set to 'PM', and a 'Get Usage Report' button. The page is for 'Site 1, Pacific Plaza'.

- Step 2** From the Report Type drop-down menu, choose a type of report:
- Usage By Year
 - Usage By Month
 - Usage By Day
- (You can also select the report type on the secondary navigation bar.)

**Note**

If you choose the Usage By Year report, you can still see the Usage By Month report for any year in the report by clicking that year. You can also click the Usage By Month and Usage By Day reports to view additional detail.

- Step 3** To change the default time of the date boundary, choose a time from the Calendar Day Offset drop-down menus.
- Step 4** To generate and view the report, click **Get Usage Report**. The report appears. (Figure 2-2 shows a Usage By Day report. Table 2-1 describes the report columns.)

Figure 2-2 Usage By Day Report

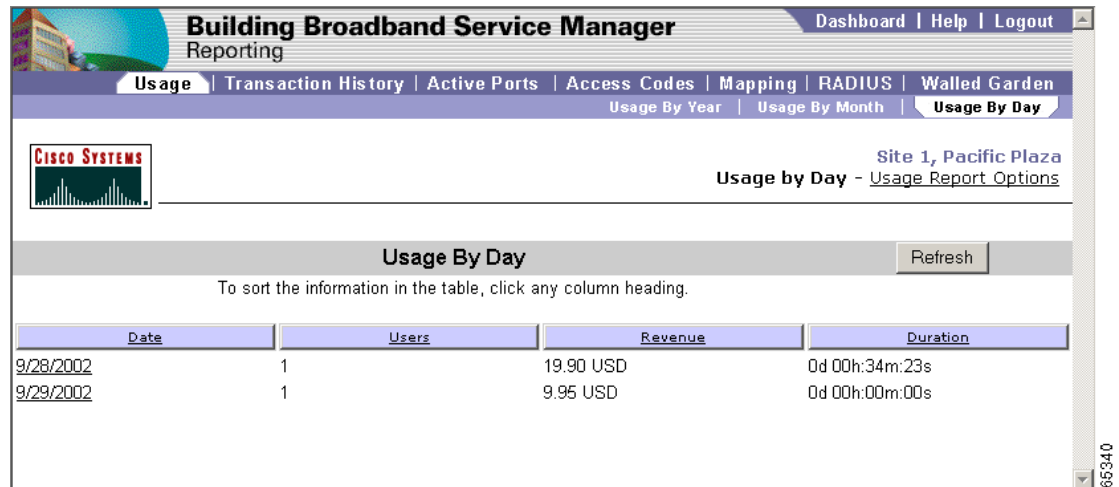


Table 2-1 Usage Report Column Descriptions

Column	Description
Year Month Date	Depending on the type of report that you request, the field displays data for the year, month, or day. Click a report entry to see a more detailed report. For example, if you click year 2002, the Usage By Month report appears, showing the monthly usage for 2002. When you click the date in a Usage by Day report, the Users field changes to Room Number and shows you usage by room number.
Users/ Room Number	For the specified time period, this field shows the number of Internet users. When you click the left-hand Date column in the Usage by Day report, the Users column changes to Room Number.
Revenue	Displays the revenue that was generated for that time period.
Duration	Displays the length of time that the Internet was used for the year, month, or day.

Transaction History Reports

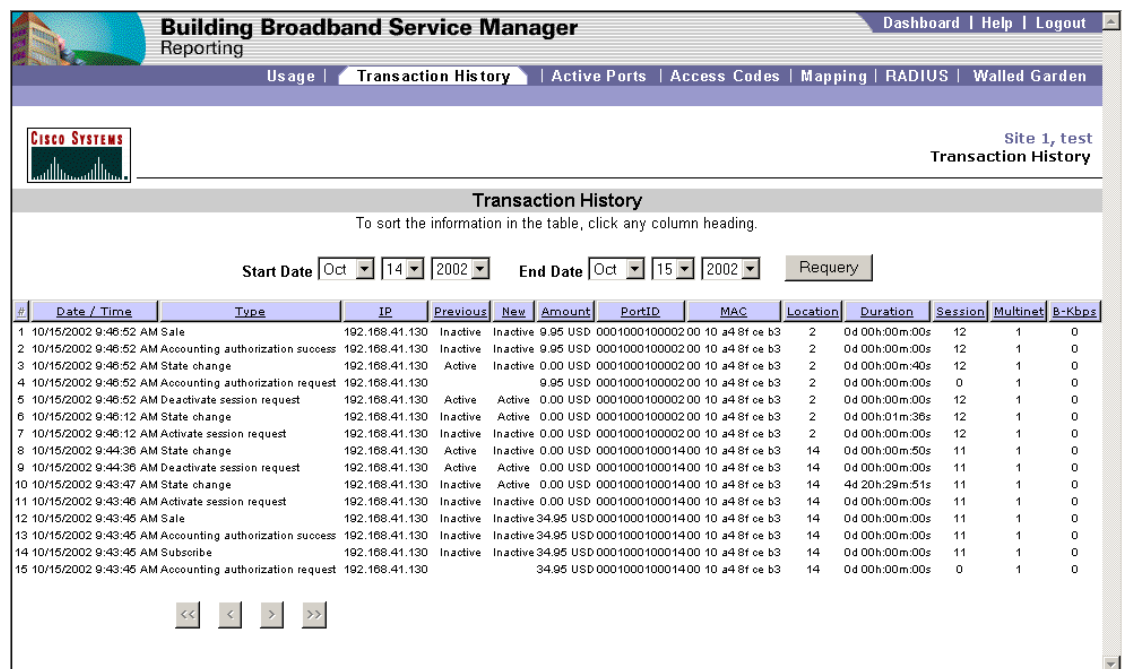
The Transaction History report shows the details of BBSM transactions. If you want to export this data or truncate part of it, use standard SQL commands. For the database schema, refer to the *Cisco BBSM 5.3 SDK Developer Guide*.

For auditing purposes, these transactions are never deleted from the BBSM database.

Follow this procedure to generate and view reports.

- Step 1** From the Dashboard, click **Reporting Pages**. The Usage Report Options web page appears.
- Step 2** Click **Transaction History**. The Transaction History web page appears. (See [Figure 2-3](#).)

Figure 2-3 Transaction History Report



- Step 3** Choose the starting and ending dates for the report.
- Step 4** To generate a new report, click **Requery**. [Table 2-2](#) describes the Transaction History report columns.

Table 2-2 BBSM Transaction History Report Columns

Column	Description
#	Displays the transaction number.
Date / Time	The date and time of the transaction.
Type	The type of transaction that occurred. (For descriptions of the transaction types, see Table 2-3 .)
IP	The IP address of the applicable client.
Previous	Designates the state of the port (Active or Inactive) before the transaction.
New	Designates the state of the port (Active or Inactive) after the transaction.
Amount	The cost of the transaction, if any.
PortID	The Port ID of the applicable client.
MAC	The MAC address of the applicable client.
Room	The guest room or location number of the client.
Duration	The session duration.
Session	For each IP address, the unique number that identifies the session.
Multinet	The multinet (1 or 2) that was used for the client IP address range for this transaction.
B-kbps	Displays the bandwidth limit in kbps that applied to the session. If the bandwidth is displayed with an <i>sh</i> following it, the client was part of a bandwidth reservation; that is, the bandwidth was shared.

[Table 2-3](#) describes all of the possible BBSM transaction types. The transaction is shown in the Type column of the Transaction History report.

Table 2-3 BBSM Transaction Types

Type	Description
Access policy deactivated session	The BBSM access policy has forced the session to be deactivated. This could happen if the user's time expired, if the credit card was denied, or if the access code became invalid.
Accounting authorization request	One of the ICS or PMS page sets is being used, and BBSM has requested authentication from the credit card server or the PMS.
Accounting request failed	An error occurred in posting the charge or in processing the response from the credit card server or the PMS.
Accounting authorization success	In response to a BBSM request for authorization from the PMS or credit card server, BBSM has received approval that allows the session to continue.
Accounting authorization failure	In response to a BBSM request for authorization from the credit card server or the PMS, BBSM has received a denial that prohibits the session from continuing. A possible reason is an invalid credit card number.
Administrative deactivate session request	The administrator deactivated the client from BBSM.
Activate session request	The user has received the Connect page and clicked Connect, and BBSM is waiting for authentication. (The user may be using the Internet at this time.) If an ICS page set is being used, BBSM is preparing to send the request to the credit card server.
Atdial Initialization Error	An error occurred during BBSM initialization.

Table 2-3 BBSM Transaction Types (continued)

Type	Description
Athdmn PMS Up	BBSM has established a connection to the PMS.
Athdmn PMS Down	Although PMS billing is configured on BBSM, the system has lost its connection to the PMS.
Athdmn print Up	BBSM has established a connection to the local printer.
Athdmn print Down	Although print billing is configured on BBSM, the system has lost its connection to the local printer.
Begin Bandwidth Boost	The user has chosen to pay extra to increase their bandwidth for a specific duration.
Deactivate session request	BBSM has received a request for disconnection. The end user has manually disconnected from BBSM by clicking Disconnect.
End Bandwidth Boost	The user's increased bandwidth time has expired.
Error reading MSMQ	The BBSM message queue cannot be read. When this error is reported, BBSM is no longer operational.
Failed to open MSMQ	The BBSM message queue could not be opened. When this error is reported, BBSM is no longer operational.
ICSCreditCard Server Up	BBSM has established a connection to the credit card server.
ICSCreditCard Server Down	Although credit card billing is configured on BBSM, the system has lost its connection to the credit card server.
Invalid Site	BBSM could not post a charge because the user's site number has not been defined in BBSM.
Launch Thread Failed	BBSM failed to initialize the thread used to search for clients on the internal network.
Port Hop Started	The user started a port hop by leaving the access point perimeter.
Port Hop Completed	The user has successfully moved from one port to another.
Port Hop Failed, attempt to hop to another site	The user moved to hop, and the session was unexpectedly terminated.
Port Hop Time Expired, deactivating session	The user's port hop was not completed within the port hop delay time period.
Registry Error	BBSM data cannot be read from the Windows registry. When this error is reported, BBSM is no longer operational.
Sale	BBSM has just charged the end user.
Sale Enqueued	A credit card sale has been put into the BBSM queue for processing. Charges are stored on the server hard drive before being sent to the credit card billing.
State change	BBSM has changed the state of the end user's port from Active to Inactive or from Inactive to Active.
Subscribe	One of the Subscription page sets is being used, and BBSM has requested authentication.
Switch port no longer active, disconnected	BBSM has detected that the user is no longer connected to the port and has deactivated the session.
Temporary DHCP deactivate session request	In a multinet configuration, BBSM sends the end user a temporary DHCP IP address. When this temporary lease expires, BBSM deactivates the session for the temporary IP address, and this transaction is reported. This deactivation process is transparent to the end user. The end user's session continues uninterrupted with the new, permanent IP address.

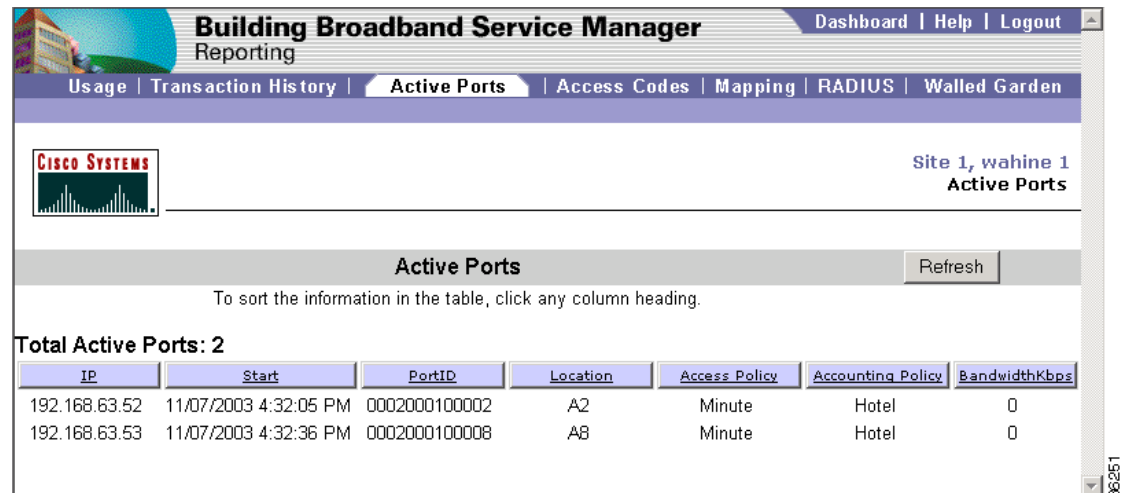
Table 2-3 BBSM Transaction Types (continued)

Type	Description
Unrecognized IP address for client	The client's IP address cannot be found in the BBSM internal network.
Unrecognized message in MSMQ	The BBSM message queue contains an unrecognized message.

Active Ports Report

The Active Ports report shows end users that are connected to the internet at the time the report is produced. Follow this procedure to view the Active Ports report.

- Step 1** From the Dashboard, click **Reporting Pages**. The Usage Report Options web page appears.
- Step 2** Click **Active Ports**. The Active Ports report appears. (See [Figure 2-4](#).)

Figure 2-4 Active Ports Report

- Step 3** Sort data in ascending or descending order by clicking a column heading. [Table 2-4](#) describes the report columns.

Table 2-4 Active Ports Report Column Descriptions

Column	Description
IP	The IP address of the connected client.
Start	The time that the connection started.
PortID	The client port. The number includes the switch, cluster, and port identifiers.
Room	<p>The room or location number:</p> <ul style="list-style-type: none"> If you used the Switch Discovery Wizard to configure the ports, the default room or location designation is <i>unmapped</i>, which means that the room has not been mapped to the port yet. If you configured the ports using the WEBconfig Network Element Port Settings pop-up window, the room number shows the location prefix you chose in the Port Settings window with the port number after it, such as <i>SW1-128</i>. If the port was configured using the Map Rooms feature, the room number is the actual number you gave it.
Access Policy	The access policy used for the client.
Accounting Policy	The accounting policy used for the client.
BandwidthKbps	The bandwidth rate, with 0 indicating full speed. If you reserved the bandwidth, the bandwidth rate indicates the reservation and (<i>shared</i>) after the number, such as <i>256 (shared)</i> .

Access Code Reports

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

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

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

Access Code Report

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

- Step 1** From the Dashboard, click **Reporting Pages**. The Usage Report Options web page appears.
- Step 2** Click **Access Codes**. The Access Code Report options web page appears. (See [Figure 2-5](#).)

Figure 2-5 Access Code Report Options

- Step 3** From the Customer Name drop-down menu, choose the customer for whom you want to view the access codes.
- Step 4** To generate and view the report, click **Find Codes**. The Access Code Report appears. (See [Figure 2-6](#). [Table 2-1](#) describes the report columns.)

Figure 2-6 Access Code Report

Start Valid	End Valid	Price	Class of Service	Bandwidth	Access Codes
Aug 5 2002 8:00AM	Aug 8 2002 12:00PM	10.00 USD	Silver	128	PAC5640 PAC6983 PAC1047 PAC9661 PAC377 PAC9710 PAC1266 PAC4013

Table 2-5 Access Report Column Descriptions

Column	Description
Start Valid	The start date for the reservation.
End Valid	The end date for the reservation.
Price	The price for the access code.
Class of Service	The class of service that the access code is providing
Bandwidth	The minimum bandwidth (in kbps) of the reservation.
Access Codes	The access codes for the reservation.

Unused Code Report

The Unused Code Report shows the access codes assigned to a customer that clients have not used to access the Internet. Follow this procedure to view the Unused Code report.

- Step 1** From the Dashboard, click **Reporting Pages**. The Usage Report Options web page appears.
- Step 2** Click **Access Codes**. The Access Code Report web page appears. (See [Figure 2-5](#).)
- Step 3** Click **Unused Code Report**. The Unused Code Report options web page appears. (See [Figure 2-7](#).)

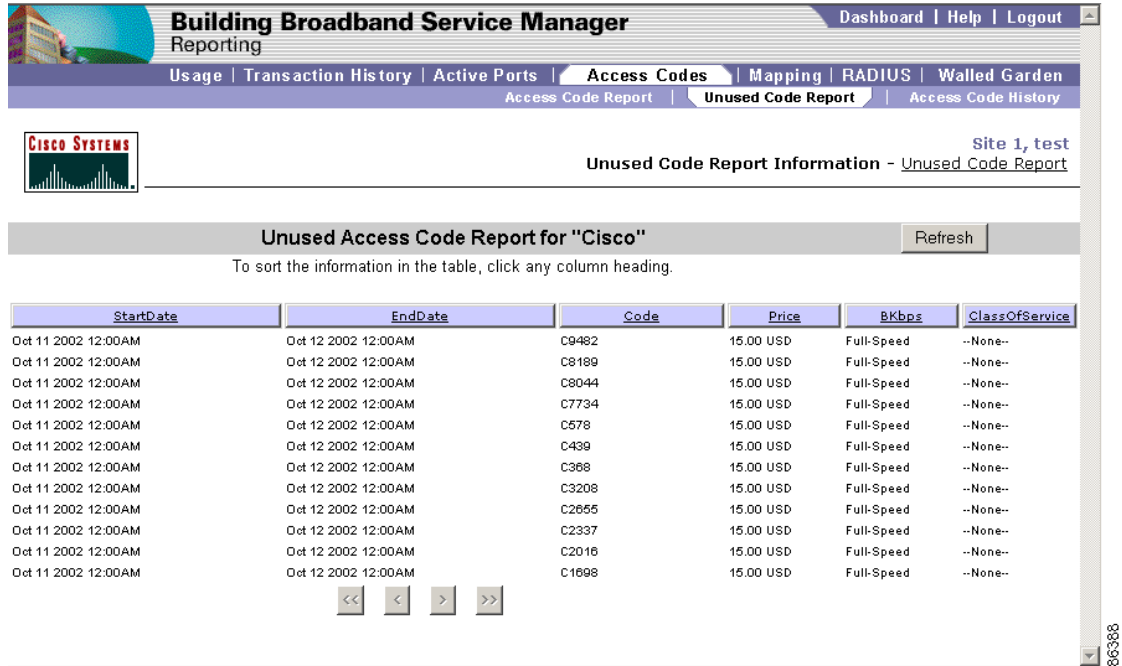
Figure 2-7 Unused Code Report Options

The screenshot shows the 'Building Broadband Service Manager' web interface. The top navigation bar includes 'Dashboard | Help | Logout'. Below this is a 'Reporting' section with tabs for 'Usage', 'Transaction History', 'Active Ports', 'Access Codes', 'Mapping', 'RADIUS', and 'Walled Garden'. The 'Access Codes' tab is selected, and within it, the 'Unused Code Report' sub-tab is active. The main content area features the Cisco Systems logo on the left and 'Site 1, test Unused Code Report' on the right. A heading 'Unused Access Code Report' is centered. Below the heading, a text prompt says 'Choose the customer from the drop-down list to view their unused access codes.' There is a 'Customer Name' label next to a drop-down menu currently showing 'Please Select Customer'. Below the menu is a 'Find Codes' button. A vertical sidebar on the right contains the number '74782'.

- Step 4** From the Customer Name drop-down menu, choose the customer for which you want to view the access codes.
- Step 5** To generate and view the report, click **Find Codes**. The Unused Code Report appears. ([Figure 2-8](#) shows a report for access codes using bandwidth reservation, and [Figure 2-9](#) shows a report for bandwidth rates without bandwidth reservations. [Table 2-6](#) describes the report columns.)

Figure 2-8 Unused Code Report Showing Bandwidth Reservation Access Codes



Figure 2-9 Unused Code Report Showing Non-Bandwidth Reservation Access Codes**Table 2-6 Unused Code Report Column Descriptions**

Column	Description
StartDate	The start date of the reservation.
EndDate	The end date of the reservation.
Code	The access code used for the reservation.
Price	The price for the access code.
Bkbps	The minimum bandwidth (in kbps) of the reservation. If no reservation was made, the rate is <i>None</i> .
ClassOfService	The class of service that the access code is providing. If no reservation was made, the class of service is <i>None</i> .

Access Code History Report

The Access Code History report shows end-user activity for access codes that clients have used to access the Internet. Follow this procedure to generate and view a summary or detailed report.

- Step 1** From the Dashboard, click **Reporting Pages**. The Usage Report Options web page appears.
- Step 2** Click **Access Codes**. The Access Code Report web page appears. (See [Figure 2-5](#).)
- Step 3** Click **Access Code History**. The Access Code History options web page appears. (See [Figure 2-10](#).)

Figure 2-10 Access Code History Report Options

The screenshot shows the 'Building Broadband Service Manager' Reporting interface. The top navigation bar includes 'Usage', 'Transaction History', 'Active Ports', 'Access Codes' (selected), 'Mapping', 'RADIUS', and 'Walled Garden'. Below this, there are sub-tabs: 'Access Code Report', 'Unused Code Report', and 'Access Code History' (selected). The page title is 'Site 1, Pacific Plaza Access Code History'. The main heading is 'Access Code History Report'. Below the heading, a message states: 'Use the form below to choose the access code history report you want to view.' The form contains four fields: 'Report Type' (set to 'Detailed'), 'Customer Name' (set to 'All'), 'Codes Used On or After' (set to 'Sep 28 2002'), and 'Codes Used Before' (set to 'Sep 29 2002'). A 'Generate Report' button is at the bottom of the form. The Cisco Systems logo is visible on the left side of the page.

- Step 4** From the Report Type drop-down menu, choose **Detailed** or **Summary**.
- Step 5** Choose a customer name. To see data for all customers, keep the default selection of *All*.
- Step 6** From the **Codes Used On or After** drop-down menus, choose the start date.
- Step 7** From the **Codes Used Before** drop-down menus, choose the end date.
- Step 8** To view the report, click **Generate Report**. The Access Code History report appears. ([Figure 2-11](#) shows a summary report, and [Figure 2-12](#) shows a detailed report. [Table 2-7](#) describes the Access Code History report columns.)

Figure 2-11 Summary Access Code History Report

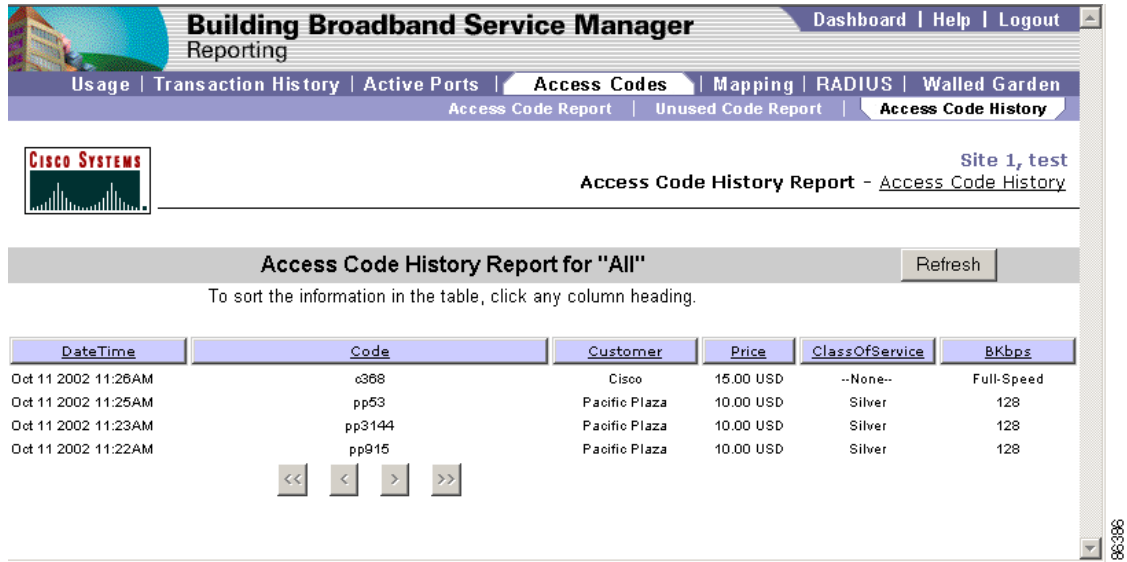


Figure 2-12 Detailed Access Code History Report

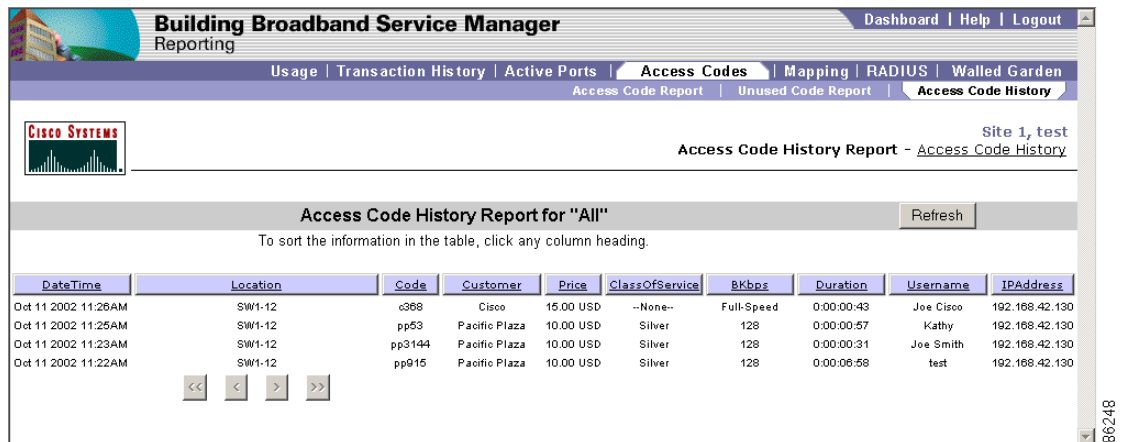


Table 2-7 Access Code History Report Column Descriptions

Column	Description
DateTime	The date and time that the end user logged off.
Location	The room or location number: <ul style="list-style-type: none"> If you used the Switch Discovery Wizard to configure the ports, the default room or location number is <i>unmapped</i>, which means that the room has not been mapped to the port yet. If you configured the ports using the WEBconfig Network Element Port Settings pop-up window, the room number shows the location prefix you chose in the Port Settings window with the port number after it, such as <i>SW1-128</i>. If the port was configured using the Map Rooms feature in WEBconfig, the room number is the actual number you gave it.
Code	The access code used to log in.
Customer	The customer name used when the reservation was made.
Price	The price and currency type for the access code or bandwidth rate.
ClassofService	The class of service used for the reservation, or if no reservation was made, an entry of <i>--None--</i> is displayed.
BKbps	The bandwidth used for the reservation, or if no reservation was made, the actual bandwidth rate, such as <i>Full-Speed</i> .
Duration	The length of time that the end user was logged on.
Username	The name that the end user entered when he or she logged in with the access code.
IPAddress	The end user's IP address.

Mapping Report

The Mapping report lists room or location numbers with their corresponding port numbers and port configuration information. There are two web page options available from the secondary navigation bar:

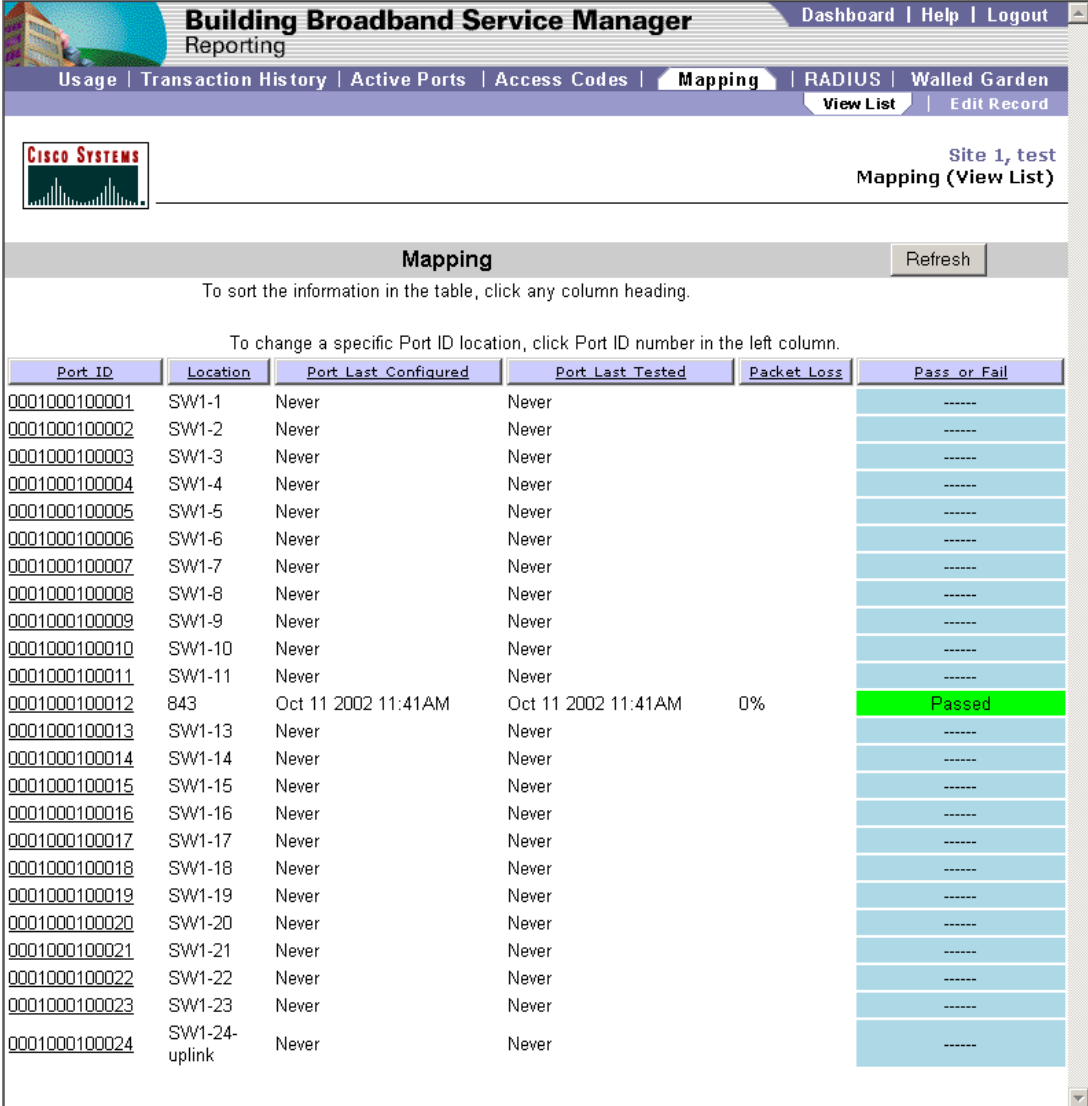
- View List—Shows a complete list of mappings
- Edit Record—Enables you to change a selected record

Viewing the Mapping Report

The View List web page lists the room or location numbers and their associated port IDs. Follow this procedure to view the Mapping report.

- Step 1** From the Dashboard, click **Reporting Pages**. The Usage Report Options web page appears.
- Step 2** Click **Mapping**. The Mapping View List web page appears. (Figure 2-13 shows a Mapping report. Table 2-8 describes the report columns.)

Figure 2-13 Mapping Report



Port ID	Location	Port Last Configured	Port Last Tested	Packet Loss	Pass or Fail
0001000100001	SW1-1	Never	Never		-----
0001000100002	SW1-2	Never	Never		-----
0001000100003	SW1-3	Never	Never		-----
0001000100004	SW1-4	Never	Never		-----
0001000100005	SW1-5	Never	Never		-----
0001000100006	SW1-6	Never	Never		-----
0001000100007	SW1-7	Never	Never		-----
0001000100008	SW1-8	Never	Never		-----
0001000100009	SW1-9	Never	Never		-----
0001000100010	SW1-10	Never	Never		-----
0001000100011	SW1-11	Never	Never		-----
0001000100012	843	Oct 11 2002 11:41AM	Oct 11 2002 11:41AM	0%	Passed
0001000100013	SW1-13	Never	Never		-----
0001000100014	SW1-14	Never	Never		-----
0001000100015	SW1-15	Never	Never		-----
0001000100016	SW1-16	Never	Never		-----
0001000100017	SW1-17	Never	Never		-----
0001000100018	SW1-18	Never	Never		-----
0001000100019	SW1-19	Never	Never		-----
0001000100020	SW1-20	Never	Never		-----
0001000100021	SW1-21	Never	Never		-----
0001000100022	SW1-22	Never	Never		-----
0001000100023	SW1-23	Never	Never		-----
0001000100024	SW1-24-uplink	Never	Never		-----

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

Table 2-8 Mapping Report Column Descriptions

Column	Description
Port ID	The port of the client. The number indicates the switch, cluster, and port.
Location	<p>The room or location number:</p> <ul style="list-style-type: none"> If you used the Switch Discovery Wizard to configure the ports, the default room or location number is <i>unmapped</i>, which means that the room has not been mapped to the port yet. If you configured the ports using the WEBconfig Network Element Port Settings pop-up window, the room number shows the location prefix you chose in the Port Settings window with the port number after it, such as <i>SW1-128</i>. If the port was configured using the Map Rooms feature in WEBconfig, the room number is the actual number you gave it.
Port Last Configured	The time that the room was mapped. If the room is not mapped, enter <i>Never</i> .
Port Last Tested	The time that the port was last tested. If the port is not tested, enter <i>Never</i> .
Packet Loss	The results of the port test showing the percentage of packets lost. If the room is not mapped, leave the field blank.
Pass or Fail	The entry is either <i>Passed</i> or <i>Failed</i> . If the room is not mapped, leave the field blank.

Editing Mapping Report Entries

Follow this procedure to edit entries in the Mapping report by using the Mapping (Edit Record) web page. You must have administrator or operator privileges to view and use this page.

This enables you to enter a new room number or location for a specific port without physically going to the port and connecting a client. You can also perform this procedure from the Port Control web page.



Note

Use caution when entering new room numbers from this page because entering an incorrect room number causes charges to be posted to the wrong room. The best way to ensure that a port is mapped to the correct room number is to go to the room, connect a client, and use the Map Rooms web page that is accessed from the BBSM Dashboard.

- Step 1** From the Dashboard, click **Reporting Pages**. The Usage Report Options web page appears.
- Step 2** Click **Mapping**. The Mapping (View List) web page appears. (See [Figure 2-13](#).)
- Step 3** From the Port ID column, click a port entry. (You can also click **Edit Record**.) The Mapping (Edit Record) web page appears, showing the Mapping Input Form. (See [Figure 2-14](#).)

Figure 2-14 Mapping Input Form

Building Broadband Service Manager
Reporting

Usage | Transaction History | Active Ports | Access Codes | **Mapping** | RADIUS | Walled Garden

View List | Edit Record

CISCO SYSTEMS

Site 1, Pacific Plaza
Mapping (Edit Record)

Mapping Input Form

Enter the revised location for the Port ID number shown below, then click the Update button.
Once you have completed making your changes, click the Return button.

Port ID 0001000100001

Location

- Step 4** Enter your changes on the Mapping Input Form and click **Update**.
- Step 5** To return to the Mapping (View List) web page, click **Return** or **View List**.

RADIUS Session History Report

The RADIUS Session History report provides a history of all RADIUS sessions based on either a particular RADIUS server or user. Follow this procedure to view the report.

- Step 1** From the Dashboard, click **Reporting Pages**. The Usage Report Options web page appears.
- Step 2** Click **RADIUS**. The RADIUS Session History web page appears. (See [Figure 2-15](#).)

Figure 2-15 RADIUS Session History Options

The screenshot shows the 'Building Broadband Service Manager' interface. The top navigation bar includes 'Dashboard | Help | Logout'. Below it, a sub-navigation bar has 'Usage | Transaction History | Active Ports | Access Codes | Mapping | **RADIUS** | Walled Garden'. The main content area is titled 'RADIUS Session History' and includes a Cisco Systems logo. It prompts the user to 'Search for RADIUS session information based on the date range and one of the identification options below.' The search options are: 'RADIUS Server' (with a dropdown menu showing '-- RADIUS Server --') or 'Customer Name' (with a dropdown menu showing '-- Customer Name --'). Below these, it asks for 'the following dates:' with 'Start Date' (Sep 27 2002) and 'End Date' (Sep 28 2002). A 'View RADIUS Report' button is at the bottom. The page number '65330' is visible in the bottom right corner.

- Step 3** From the RADIUS Server or Customer Name drop-down menus, choose a RADIUS server or customer.
- Step 4** Choose the starting and ending dates for the report.
- Step 5** To generate and view the report, click **View RADIUS Report**. The RADIUS Session History report appears. (See [Figure 2-16](#).)

Figure 2-16 RADIUS Session History Report

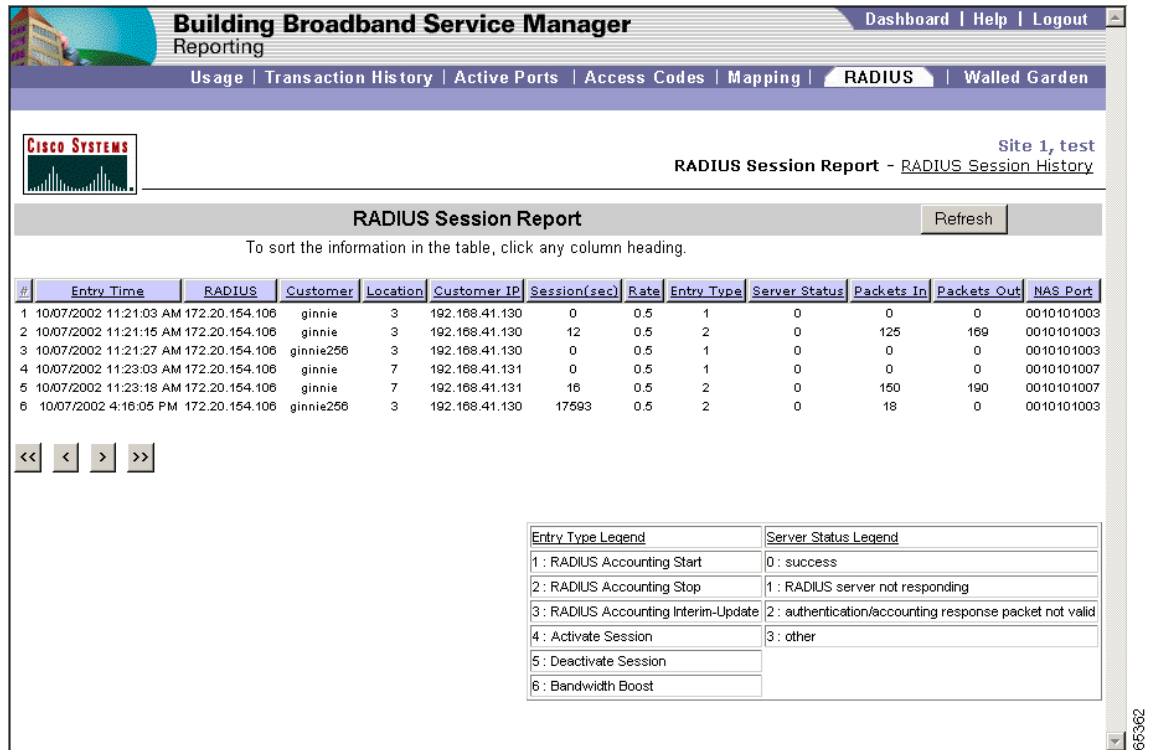


Table 2-9 describes the RADIUS Session History report data.

Table 2-9 RADIUS Session History Report Columns

Column	Description
#	The session number.
Entry Time	The time that the end user logged in.
RADIUS	The IP address or fully qualified domain name (FQDN) of the RADIUS server that the end user connected to.
Customer	The end user's login name.
Room	The end user's location.
Customer IP	The end user's IP address.
Session (sec)	The session duration in seconds.
Rate	The cost of the session.
Entry Type	Indicates the type of entry: <ul style="list-style-type: none"> 1 = RADIUS Accounting Start 2 = RADIUS Accounting Stop 3 = RADIUS Accounting Interim-Update 4 = Activate Session 5 = Deactivate Session 6 = Bandwidth Boost

Table 2-9 RADIUS Session History Report Columns (continued)

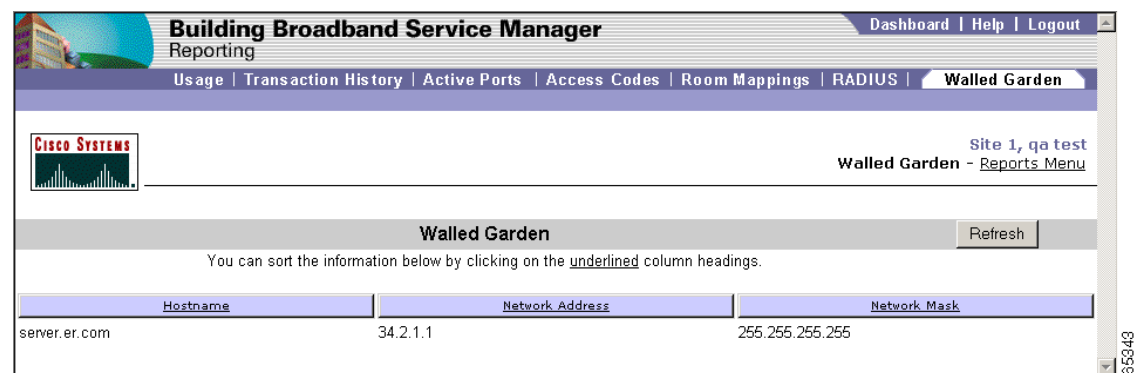
Column	Description
Server Status	Indicates whether or not the login was successful: <ul style="list-style-type: none"> 0 = Successful 1 = RADIUS server not responding 2 = Authentication/accounting response packet not valid 3 = Other
Packets In	The number of packets that BBSM received from the end user during the user's session.
Packets Out	The number of packets that BBSM transmitted to the end user during the user's session.
NAS Port	The location of the NAS port.

Walled Garden Report

The Walled Garden report displays all of the current walled garden configurations that you created using the Walled Garden web page of WEBconfig. [Figure 2-17](#) shows an example of the report.

Follow this procedure to view the Walled Garden report.

- Step 1** From the Dashboard, click **Reporting Pages**. The Usage Report Options web page appears.
- Step 2** Click **Walled Garden**. The Walled Garden report web page appears. (See [Figure 2-17](#).)

Figure 2-17 Walled Garden Report

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



Monitoring Performance (System Summary)

The System Summary is a single web page that enables you to monitor the BBSM system status and all BBSM services. Because it enables you to access the BBSM database, you must use a valid MSDE username and password.

The data that is displayed varies depending the system configuration. In a hotspot configuration, the System Summary functions in a similar, but not identical, way. For example, in the heading data on the first page, which shows the report date and time stamp, the hotspot summary displays a single *Location Name and Location Description* instead of *BBSM Hotspot System Information*.



Note

Refer to the *Cisco BBSM 5.3 Configuration Guide* for the procedure to enter or change the MSDE username and password.

Follow this procedure to use the System Summary.

- Step 1** From the Dashboard, click **System Summary**. The System Summary web page appears. (See [Figure 3-1](#).)

Figure 3-1 System Summary

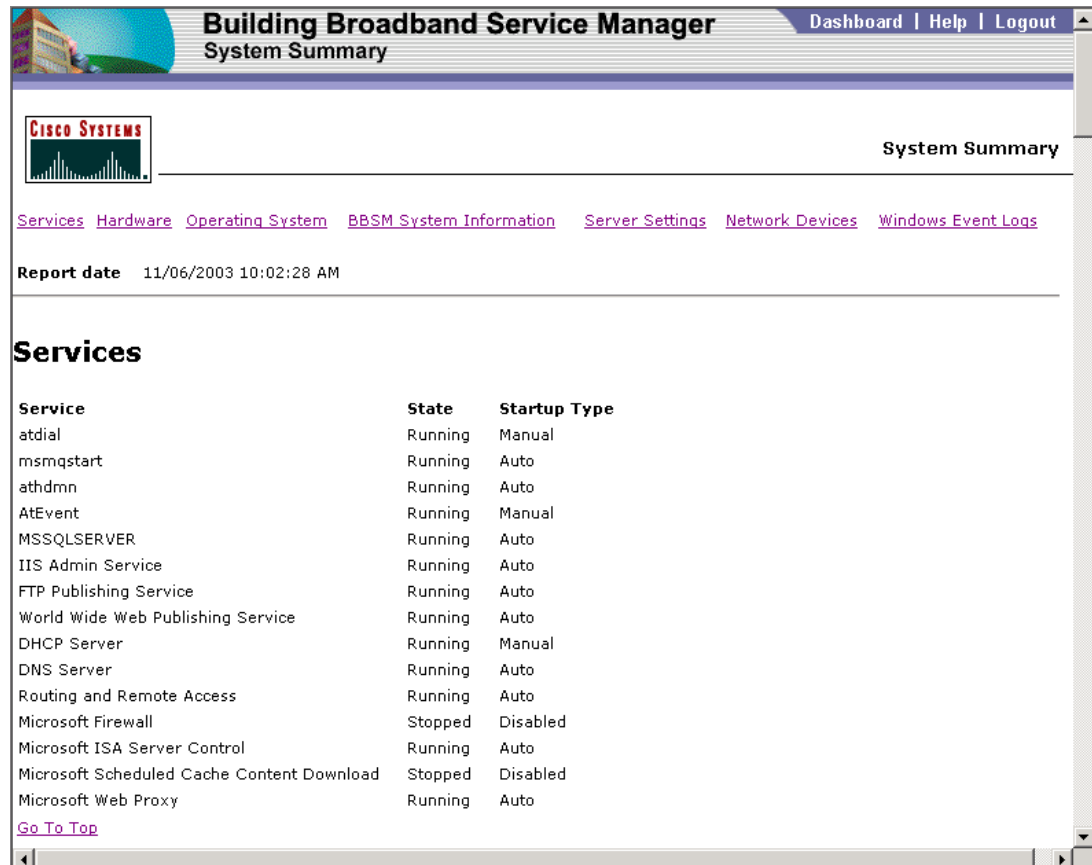
- Step 2** Enter an MSDE username and password and then click **Submit**. To use the MSDE *sa* account, enter *sa* for the username and then enter the *sa* password for your server. This password was entered either from the Set Passwords application if you bought a BBSM appliance or during the BBSM software installation if you bought the software CD. Refer to the section on entering passwords in the *Cisco BBSM 5.3 Configuration Guide*.

If your username and password are correct, the System Summary web page shows the system data. (Figure 3-2 shows the beginning of the web page.) If your information is incorrect, the log-in page shown in Figure 3-1 appears again with an error message.



Note If you click Reset, the values are reset to the original values.

Figure 3-2 System Summary Showing Section Headings and Services Data



Step 3 View the system data by clicking the section headings or scrolling down the page:

- **Services**—Lists the service names with current status and startup type. Each BBSM system service displays a status of *Running* or *Stopped* and a startup type of *Auto*, *Manual*, or *Disabled*. All of the services in the table should display a status of *Running*. (See [Table 3-1](#) for the BBSM service and its display name.)

Table 3-1 System Summary Displayed Services

BBSM Service	Display Name
atdial	atdial
msmqstart	msmqstart
athdmn	athdmn (not shown in a hotspot configuration)
atevent	Atevent
mssqlserver	MSSQLSERVER
iisadmin	IIS Admin Service
msftpsvc	FTP Publishing Service
w3svc	World Wide Web Publishing Service
DHCP	DHCP Server
DNS	DNS Server
RemoteAccess	Routing and Remote Access
fwsrv	Microsoft Firewall
isactrl	Microsoft ISA Server Control
w3schdwn	Microsoft Scheduled Cache Content Download
w3proxy	Microsoft Web Proxy

- **Hardware**—Displays the system processors and Ethernet adapters
- **Operating System**—Displays operating system data in the following sections:
 - Windows OS
 - Installed Windows Hotfixes
 - DNS Forwarding
- **BBSM System Information**—Provides the system and site data in these sections:
 - Release
 - Patch History
 - IP Address Ranges
 - Sites
- **Server Settings**—Displays the configuration data that BBSM stores
- **Network Devices**—Displays network device data in these sections (a non-hotspot BBSM configuration also displays the site number):
 - External Gateway Router
 - Configured Routers

- Configured Network Devices
 - Port Configuration
- Windows Event Logs—Displays the system logs in the following sections:
 - System Event Log
 - Application Event Log
 - DNS Server Event Log
- Helpful Sites—Provides links that may be useful to the user



Using Port Control

The Port Control web pages enable you to update network device port data and test the ports. (You must have administrator or operator privileges to use these web pages.)

This section is divided into the following three subsections:

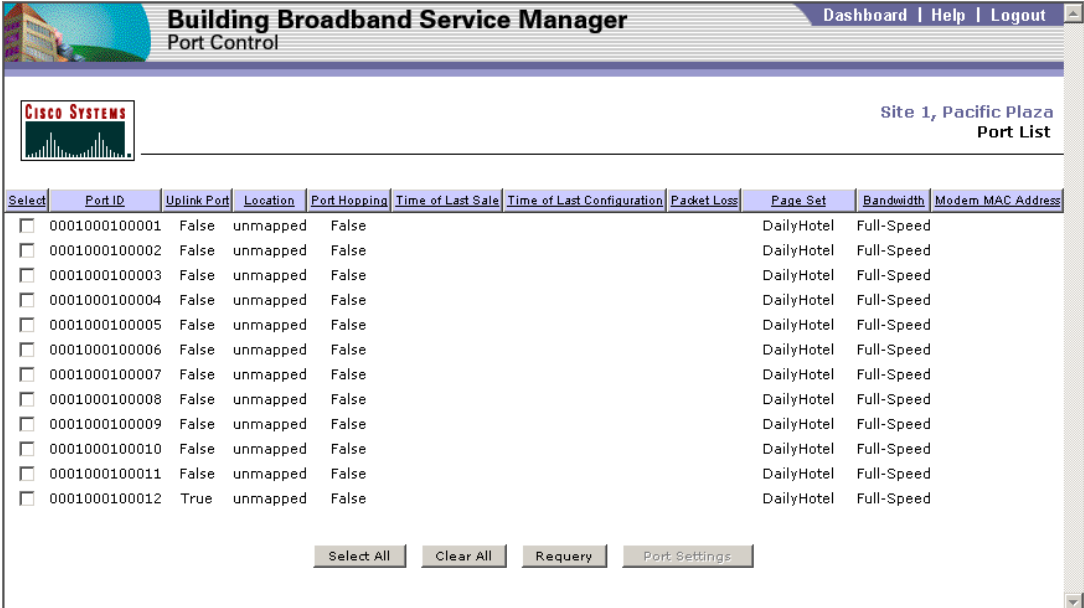
- [Changing the Port Settings for a Single Port, page 4-2](#)—How to change the port data for a single switch, access point, or CMTS port.
- [Changing the Port Settings for a Multiple Ports, page 4-6](#)—How to change the port data for multiple switch or access point ports.
- [Replacing, Adding, or Removing a Cable Modem, page 4-7](#)—How to perform these procedures for a cable modem (CMTS port).

Changing the Port Settings for a Single Port

Follow this procedure to change the port data for a single port and test the port. To replace, add, or remove a cable modem, refer to the [“Replacing, Adding, or Removing a Cable Modem”](#) section on page 4-7.

- Step 1** From the Dashboard, click **Port Control**. The Port List web page appears. [Figure 4-1](#) shows the type of port control data that appears if you are using a switch or access point. [Figure 4-2](#) shows the type of data that appears if you are using a CMTS.

Figure 4-1 Port List Showing Switch or Access Point Data



The screenshot shows the 'Building Broadband Service Manager' interface with the 'Port Control' section active. The page title is 'Site 1, Pacific Plaza Port List'. Below the title is a table with 11 columns: Select, Port ID, Uplink Port, Location, Port Hopping, Time of Last Sale, Time of Last Configuration, Packet Loss, Page Set, Bandwidth, and Modem MAC Address. The table contains 12 rows of data. The first 11 rows have 'False' for Uplink Port, Location, Port Hopping, and Packet Loss, and 'DailyHotel' for Page Set and 'Full-Speed' for Bandwidth. The 12th row has 'True' for Uplink Port, 'False' for Location, Port Hopping, and Packet Loss, and 'DailyHotel' for Page Set and 'Full-Speed' for Bandwidth. Below the table are four buttons: 'Select All', 'Clear All', 'Requery', and 'Port Settings'.

Select	Port ID	Uplink Port	Location	Port Hopping	Time of Last Sale	Time of Last Configuration	Packet Loss	Page Set	Bandwidth	Modem MAC Address
<input type="checkbox"/>	0001000100001	False	unmapped	False				DailyHotel	Full-Speed	
<input type="checkbox"/>	0001000100002	False	unmapped	False				DailyHotel	Full-Speed	
<input type="checkbox"/>	0001000100003	False	unmapped	False				DailyHotel	Full-Speed	
<input type="checkbox"/>	0001000100004	False	unmapped	False				DailyHotel	Full-Speed	
<input type="checkbox"/>	0001000100005	False	unmapped	False				DailyHotel	Full-Speed	
<input type="checkbox"/>	0001000100006	False	unmapped	False				DailyHotel	Full-Speed	
<input type="checkbox"/>	0001000100007	False	unmapped	False				DailyHotel	Full-Speed	
<input type="checkbox"/>	0001000100008	False	unmapped	False				DailyHotel	Full-Speed	
<input type="checkbox"/>	0001000100009	False	unmapped	False				DailyHotel	Full-Speed	
<input type="checkbox"/>	0001000100010	False	unmapped	False				DailyHotel	Full-Speed	
<input type="checkbox"/>	0001000100011	False	unmapped	False				DailyHotel	Full-Speed	
<input type="checkbox"/>	0001000100012	True	unmapped	False				DailyHotel	Full-Speed	

Select All Clear All Requery Port Settings

Figure 4-2 Port List Showing CMTS Data

Port Control - Microsoft Internet Explorer

Address: http://localhost:9488/ports1/portList.asp

Building Broadband Service Manager
Port Control

Dashboard | Help | Logout

Site 1, 1
Port List

Select	Port ID	Uplink Port	Location	Port Hopping	Time of Last Sale	Time of Last Configuration	Packet Loss	Page Set	Multinet	Bandwidth	Modem MAC Address
<input type="checkbox"/>	0001000100001	False	unmapped	True				AccessCode	2	Full-Speed	Modem Removed
<input type="checkbox"/>	0001000100002	False	test-2022	True				AccessCode	2	Full-Speed	00 06 53 14 7c e9
<input type="checkbox"/>	0001000100003	False	test-3033	True				DailyHotel	2	Full-Speed	00 a0 73 2c 7d 1f
<input type="checkbox"/>	0001000100004	False	1022	True		10/07/2002 4:38:26 PM		DailyHotel	2	Full-Speed	00 07 0e 01 b1 25

Select All Clear All Requery Port Settings

Done Local intranet

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

Step 3 Click **Port Settings**. The Port Settings window for a single-port change pops up. Figure 4-3 shows the type of data that appears in the window if you are using a switch or access point. Figure 4-4 shows the type of data that appears in the window if you are using a CMTS.



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

Figure 4-3 Port Control Port Settings Window Showing Switch or Access Point Data

Port Control - Port Settings

Port Settings

Port ID: 0001000100017

Port Location: unmapped

Start Authorized Period: Jan 1 2002 Time 07:59 AM

End Authorized Period: Dec 31 2002 Time 07:59 PM

Bandwidth Per User: Full-Speed

Page Set: DailyHotel

Start Page: http://%iport%/ekgnkm/DailyHotelStart.asp

Uplink Port: ☐

Enable Port Hopping: ☐

Client IP Address Range (DHCP): ☒ Multinet1 ☐ Multinet2

Modem MAC Address:

Comment:

Save Cancel

Port Test

Switch Mode: 10Mbps

Time of Last Port Test: Never

Packet Loss: 100% - No Packets Transmitted

Initiate Port Test

NOTE: To run a port test, a client must be active on the port you wish to test.

86243

Figure 4-4 Port Control Port Settings Window Showing CMTS Data

Port Control - Port Settings

Port Settings

Remove Modem

Port ID: 0001000100003

Port Location: test-3033

Start Authorized Period: Oct 2 2002 Time 08:45 AM

End Authorized Period: Oct 2 2002 Time 08:45 AM

Bandwidth Per User: Full-Speed

Page Set: DailyHotel

Start Page: http://%iport%/ekgnkm/DailyHotelStart.asp

Uplink Port: ☐

Enable Port Hopping: ☒

Client IP Address Range (DHCP): ☐ Multinet1 ☒ Multinet2

Modem MAC Address: 00 a0 73 2c 7d 1f

Comment:

Save Cancel

Port Test

Switch Mode: 10Mbps

Time of Last Port Test: Never

Packet Loss: 100% - No Packets Transmitted

Initiate Port Test

NOTE: To run a port test, a client must be active on the port you wish to test.

86197

Step 4 Make the appropriate changes based on the information in Table 4-1.

- Step 5** If you want to test the port, click **Initiate Port Test** in the Port Test pane on the right. (This step is optional and the client must be active on the port for the test to work.) After port testing, the data shown in the Port Test pane is updated to reflect the test results.
- Step 6** To save the port changes, click **Save**. A confirmation dialog box appears to indicate that the changes were successful.
- Step 7** To close the dialog box, click **OK**. You are returned to the Port List web page.

^f
Table 4-1 Port Control Port Settings Field Descriptions

Field	Description
Port Settings	
Remove Modem (CMTS only)	Note This button appears only if the port is a CMTS (cable modem) port. Click this button to remove a cable modem.
Port ID	Displays the unique number automatically assigned to each port during the Network Elements port configuration. This number cannot be changed. The port ID incorporates the cluster, switch, and port number on the switch. The format is xxxxyyyyzzzzz, where xxxx is the cluster, yyyy is the switch, and zzzzz is the port.
Port Location	Enter the location (or room number) associated with this port. This location can be a number or text. Caution If you enter port locations the first time using this field, there is no way to verify that ports have been mapped to the correct room number. The only way to ensure that your port-room mapping is accurate is to use the Map Rooms option from the Dashboard. After locations have been mapped the first time, you can update the locations using this field.
Start Authorized Period (Subscription page set only)	If the port is configured for the Subscription page set, enter the starting date and time of the period that the port is authorized for use. The default is the time that the port was configured.
End Authorized Period (Subscription page set only)	If the port is configured for the Subscription page set, enter the ending date and time of the period that the port is authorized for use. The default is the time that the port was configured.
Bandwidth Per User	From the drop-down menu, choose the default bandwidth (in kbps) for all users who will be connected to the port. (Bandwidth is applied by IP address, not by port, and is effective only if Bandwidth Management is enabled.) The value is a number from 0 to 2000000 (for example, 2 Gbps), 0 representing the maximum bandwidth available. The default is <i>Full-Speed</i> . (For information on enabling Bandwidth Management, refer to the chapter on configuring the network and bandwidth management in the <i>Cisco BBSM 5.3 Configuration Guide</i> .)
Page Set	From the drop-down menu, choose the page set to be used by the port.
Start Page	Enter the complete URL of the Start page for your page set. The URL must be in the form <i>http://%iport%...</i> because BBSM translates <i>%iport%</i> to be either the BBSM internal IP address or the BBSM domain name, if applicable.
Uplink Port	Check this check box if the port is used as an uplink to another switch. BBSM ignores the MAC addresses on these uplink ports so it does not report that clients are connected to the ports.
Enable Port Hopping	Check this check box if you want to enable port hopping.
Client IP Address Range (DHCP)	If you are using multiple networks, click the default multinet number for clients connected to this network device: Multinet 1 or Multinet 2.
Modem MAC Address (CMTS only)	Note This field is blank and read only for switches and access points. For CMTSs, this field displays the cable modem MAC address. If you need to change the MAC address, the format is <i>xx xx xx xx xx xx</i> , such as <i>0 a0 73 2c 7d 1f</i> .
Comment	Use this field to enter additional information about this port.

Table 4-1 Port Control Port Settings Field Descriptions (continued)

Field	Description
Port Test	
Switch Mode	Displays the bandwidth rate.
Time of Last Port Test	Displays the last date and time that the port was tested.
Packet Test	Displays the percentage of packets that were transmitted.
Initiate Port Test	Click to begin testing the port.
Buttons	
Save	Saves the changes.
Cancel	Cancels the changes and returns you to the Port Control web page.

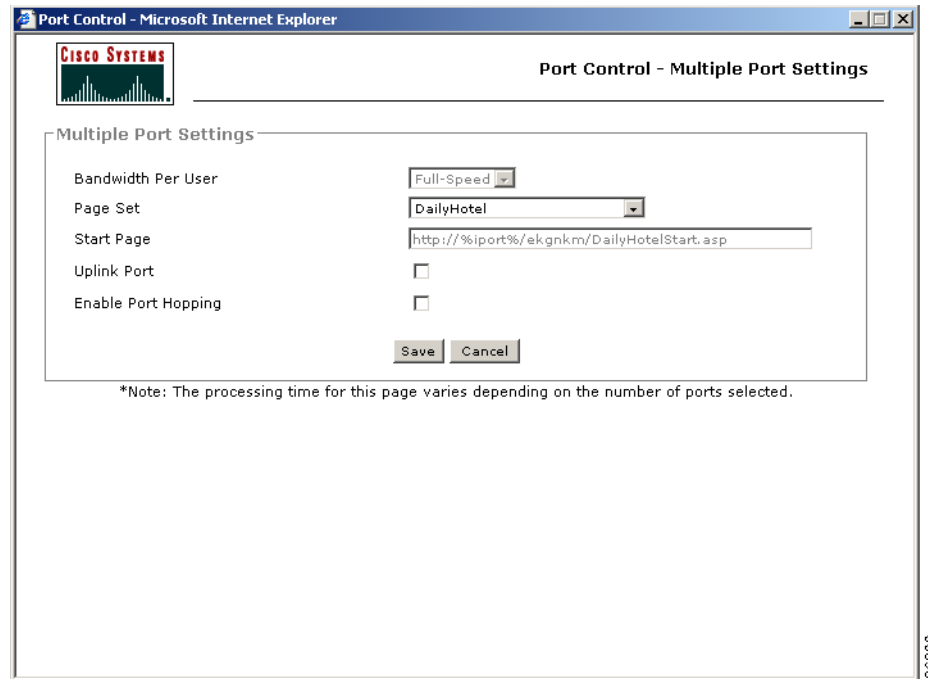
Changing the Port Settings for a Multiple Ports

Follow this procedure to change the port data for multiple ports and test the ports.

- Step 1** From the Dashboard, click **Port Control**. The Port Control web page appears. (See [Figure 4-1](#).)
- Step 2** In the left-hand column, check the ports that you want to update.
- Step 3** Click **Port Settings**. The Port Settings window for multiple-port changes pops up. (See [Figure 4-5](#).)



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

Figure 4-5 Port Control Port Settings Pop-up Window for Multiple Ports

- Step 4** Make the appropriate changes based on the field descriptions shown in [Table 4-1](#). This table also shows the fields that only apply to single-port changes. (Before making any changes, be sure that the Port ID and room or location number correspond to the port you want to change.)
- Step 5** Click **Save**. A confirmation dialog box appears to show that the changes were successful, what fields were changed, and the changed values.
- Step 6** Click **OK** to close the dialog box. You are returned to the Port Control web page.

Replacing, Adding, or Removing a Cable Modem

Follow this procedure to add, replace, or remove a cable modem.

- Step 1** From the Dashboard, click **Port Control**. The Port List web page appears.
- Step 2** In the left-hand column, check a cable modem port:
- If you are replacing or removing a cable modem, check the appropriate port. (See [Figure 4-2](#).)
 - If you are adding a cable modem, you must check a spare port. When a spare port is available, the port is designated by *Modem Removed* in the Modem MAC Address field.
- (To refresh the web page, click **Requery**.)

Step 3 Click **Port Settings**. The Port Settings window pops up (Figure 4-4):

- To add or replace a modem, enter the new MAC address in the Modem MAC address field and click **Save**. The format is *xx xx xx xx xx xx*, such as *0 a0 73 2c 7d 1f*. A confirmation dialog box appears to indicate that the changes were successful.
- To remove a modem, click the **Remove Modem** button. A confirmation dialog box appears to indicate that the changes were successful.

**Note**

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

Step 4 To close the dialog box, click **OK**. You are returned to the Port List web page.

**Note**

You can always add or replace a modem by using the dynamic CMTS port-room configuration. Refer to the section on dynamic port-room configuration for CMTSs in the *Cisco BBSM 5.3 Configuration Guide*.



Installing Service Packs or Patches (WEBpatch)

This section describes how to view, transfer, and install service packs or patches and view the patch log. (You must have administrative rights to install BBSM service packs or patches.)

You can install BBSM service packs or patches locally on any BBSM server or on multiple BBSM servers from another computer in a remote location. You can transfer multiple files to the BBSM server before you install them.



Note

As of BBSM 5.3, the FTP port on the internal network is blocked. Because WEBpatch transfer uses FTP, patches and service packs can be transferred only from the external network to BBSM. They cannot be transferred from within the BBSM network.

Before You Start

Before you begin transferring and installing files, read the following precautions

- Transfer and install only service packs or patches properly obtained from Cisco.
- Most BBSM service packs and patches are available over the Internet. Be sure that the file has been downloaded before continuing.
- Make sure that both the external and internal NICs are plugged in and enabled, or the service pack or patch will fail to install.
- Cisco strongly recommends that you terminate all client sessions during these installations.
- Install service packs or patches during low-use time periods to minimize service interruptions and ensure proper functionality.
- If you are using Windows 2000 Professional or XP Professional on your client, uncheck the **Client for Microsoft Networks** check box as described below. When you uncheck this check box, the ASP files load much more quickly. Be sure to re-check it after you install the patch.
 - Choose **Start > Settings > Network and Dial-up Connections**. The Network and Dial-up Connections window appears.
 - Right-click **Local Area Connection**, and from the drop-down menu, choose **Properties**. The Local Area Connection Properties window appears.
 - Uncheck the **Client for Microsoft Networks** check box.
 - To close the windows, click **OK** three times.

Patch Installation Procedure

Follow this procedure to view or install service packs or patches and view the patch log.

- Step 1** From the BBSM Hotspot Dashboard, click **WEBpatch**. The BBSM Patches web page appears. (See [Figure 5-1](#) and [Table 5-1](#).)

Figure 5-1 BBSM Patches

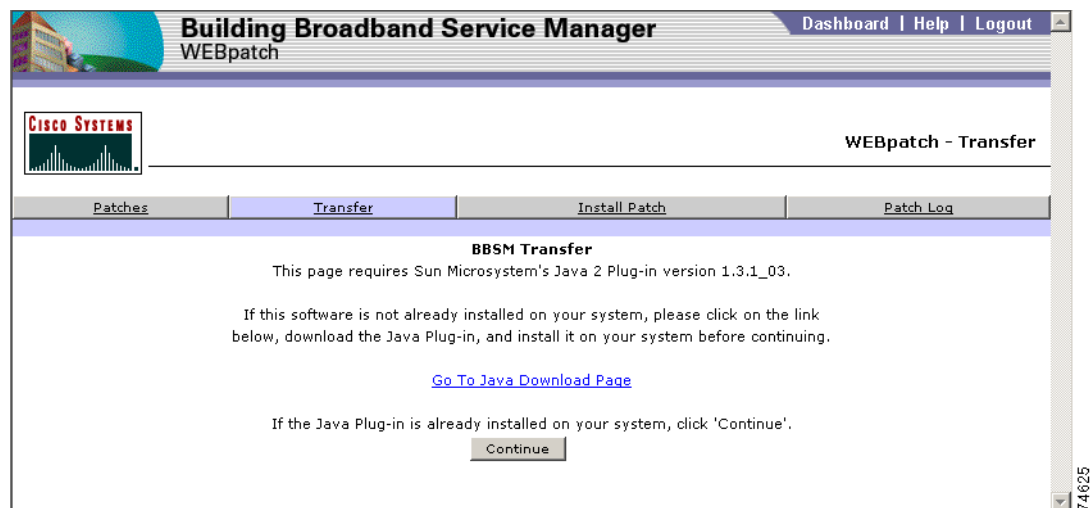
Table 5-1 BBSM Patches Fields

Field	Description
Installed patches	Specifies an installed service pack.
Install Date	Shows the date that the service pack was originally installed.
Release	Lists the BBSM release that the service pack was intended for.
Description	Briefly describes the service pack.
Release Dependencies	Indicates the BBSM release or range of releases that must be installed on the target server before you can install the service pack.
Patch Dependencies	Lists the previous service packs or patches that must be installed before you can install the current service pack or patch.
Hotfixes	Displays the names of batch files that are run during patch installation.
Database Commands	Displays the names of files containing database commands that the BBSM server sends to update its database when service packs or patches are being installed.

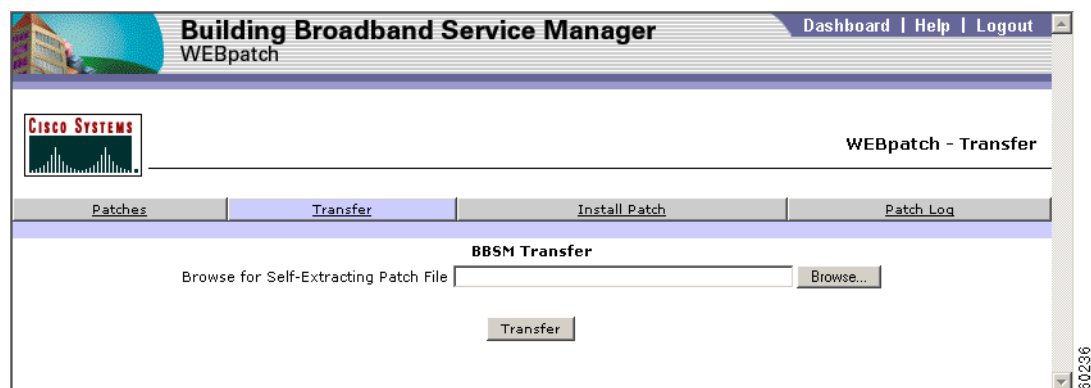
- Step 2** To view installed service packs, follow these steps:
- From the Installed patches drop-down menu, select a service pack. (The navigation buttons near the bottom of the page can also be used to select a service pack.)
 - Click **Go**. The BBSM Patches web page fields populate with the data for the specified service pack, and the View Log Entries button is enabled.
- Step 3** Transfer and install service packs or patches, as follows:
- Click **Transfer**. The BBSM Transfer web page appears. (See Figure 5-2.)

**Caution**

You must use the Java 2 plug-in, version 1.3.1_03, to transfer patches. Other versions will fail. The Java plug-in must be installed on the remote computer that you are using to transfer the file. If the plug-in is not installed already, click **Go To Java Download Page**, download the plug-in, and install it.

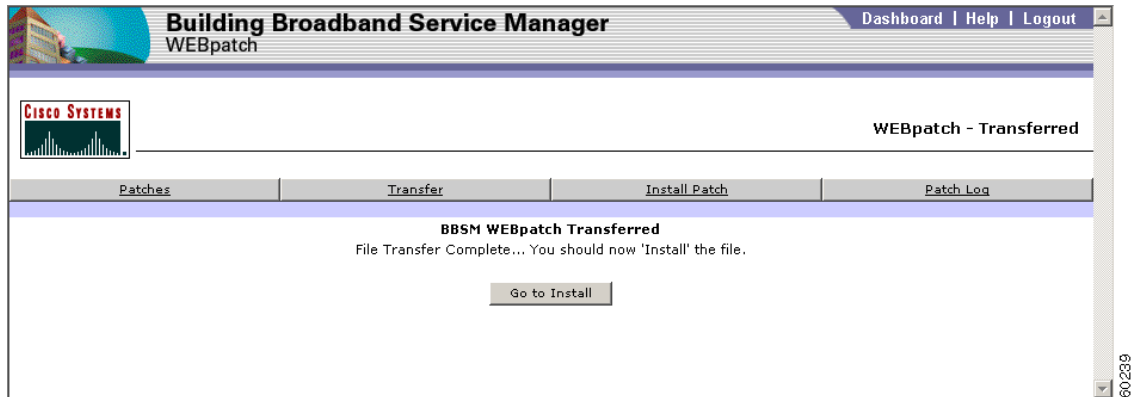
Figure 5-2 BBSM Transfer

- Click **Continue**. The BBSM Transfer web page appears. (See Figure 5-3.)

Figure 5-3 BBSM Transfer, Browse

- c. In the BBSM Transfer field, click **Browse** to navigate to the file being installed and then click **Open**. The file name now appears in the BBSM Transfer field.
- d. Click **Transfer**. The BBSM WEBpatch Transferred web page appears, prompting you to install the file. (See Figure 5-4.)

Figure 5-4 BBSM WEBpatch Transferred

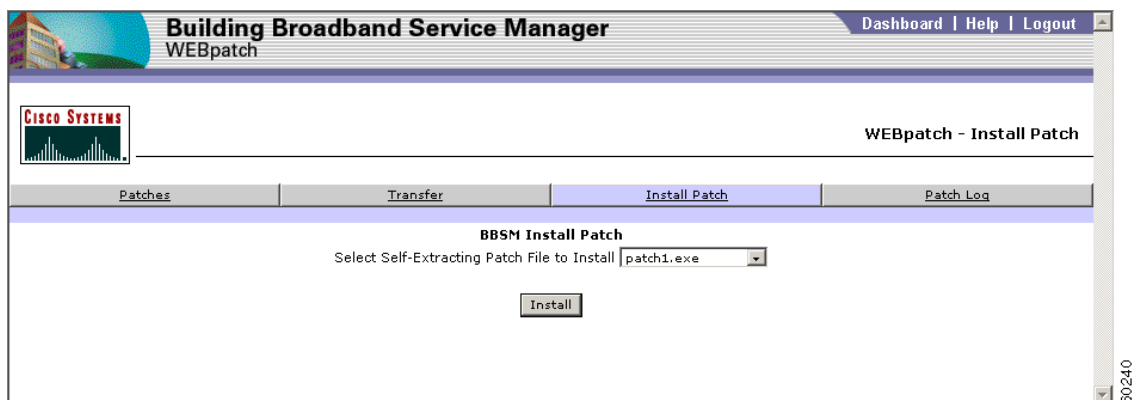


- e. To install another file at the same time, click **Transfer** again to continue transferring files to be installed. After all files are transferred, continue with the installation.
- f. Click **Go to Install** or **Install Patch**. The BBSM Install Patch web page appears. If you clicked Go to Install, the page displays the transferred patch in the Select Self-Extracting Patch File to Install drop-down menu. If you clicked Install Patch, select the patch from the Select Self-Extracting Patch File to Install drop-down menu. (See Figure 5-5.)



Note This step may take a few minutes, depending on the size of the patch and whether you are remote or local.

Figure 5-5 Install Patch



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

**Note**

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

- Step 4** To view the patch log to confirm that your patches installed successfully and to view any messages, follow these steps:
- Click **Patch Log**. The BBSM Patch Log web page appears. (See [Figure 5-6](#).) (This page can also be accessed from the Patches page by clicking **View Log Entries**.)

Figure 5-6 BBSM Patch Log

Building Broadband Service Manager
WEBpatch

Dashboard | Help | Logout

Cisco Systems

WEBpatch - Patch Log

Patches Transfer Install Patch Patch Log

BBSM Patch Log

Patches: All
Trace Level: Summary
Log Type: All

Go Default

Patch Log Data

Date Time	Patch#	Detail
03/11/2002 15:15:04	0	CPatchUtil::Transfer successfully invoked for [BBSM51SP1.exe]
03/11/2002 15:15:29	1039	CPatchUtil::InstallPatch started
03/11/2002 15:15:31	1039	CPatchUtil::InstallPatch successful for: BBSM51SP1.exe
03/11/2002 15:15:31	1039	CPatchUtil::Reboot successful
03/11/2002 15:18:47	0	CPatchUtil::Transfer successfully invoked for [Patch1042.exe]
03/11/2002 15:18:50	1042	CPatchUtil::InstallPatch started
03/11/2002 15:18:50	1042	CPatchUtil::InstallPatch successful for: Patch1042.exe
03/11/2002 15:18:50	1042	CPatchUtil::Reboot successful
03/11/2002 15:21:54	0	CPatchUtil::Transfer successfully invoked for [WEBPatch51SP1.exe]
03/11/2002 15:21:59	1044	CPatchUtil::InstallPatch started
03/11/2002 15:22:00	1044	CPatchUtil::InstallPatch successful for: WEBPatch51SP1.exe
03/11/2002 15:22:00	1044	CPatchUtil::Reboot successful
03/11/2002 15:25:24	0	CPatchUtil::Transfer successfully invoked for [BBSM51SP2.exe]
03/11/2002 15:26:50	0	CPatchUtil::Transfer successfully invoked for [BBSM51SP2.exe]
03/11/2002 15:27:54	1043	CPatchUtil::InstallPatch started

- From the drop-down menus at the top of the page, select your criteria or click **Default**, which selects all service packs and patches, the Summary trace level, and All log types. (See [Table 5-2](#).)
- Click **Go**. The messages are displayed in the Patch Log Data table.
- If no log information meets your criteria, a dialog box appears, stating that no records exist for the selected criteria. Click **OK** to return to the Patch Log page and change the search parameters.

Table 5-2 BBSM Patch Log Fields

Field	Description
Drop-Down Menus	
Patches	<ul style="list-style-type: none"> All (default setting)—Shows messages for all service packs or patches <service_pack_number>—Shows only PatchLog entries for the specific service pack
Trace Level	<ul style="list-style-type: none"> All—Shows all trace levels Summary (default setting)—Lists only the high level summary Detail—Shows all the messages for all actions performed during WEBpatch activities Debug—Not applicable (used by Cisco Support)
Log Type	<ul style="list-style-type: none"> All (default setting)—Shows all entries for all log types Transfer—Shows only entries for file transfers Install—Lists only installation related entries Other—Displays messages generated by Windows and other programs during WEBpatch activities
Table Columns	
Date Time	The date and time that the patch was installed
Patch #	The patch number
Detail	The patch description



Troubleshooting

Use this chapter to troubleshoot problems that may arise when using BBSM:

- [Clearing Pending Hotel Charges, page 6-1](#)
- [Troubleshooting Tips, page 6-3](#)
- [Using the Trace Debugging Utility, page 6-9](#)

In addition to the information in this section, you can also find tips and answers to common questions by accessing the BBSM website:

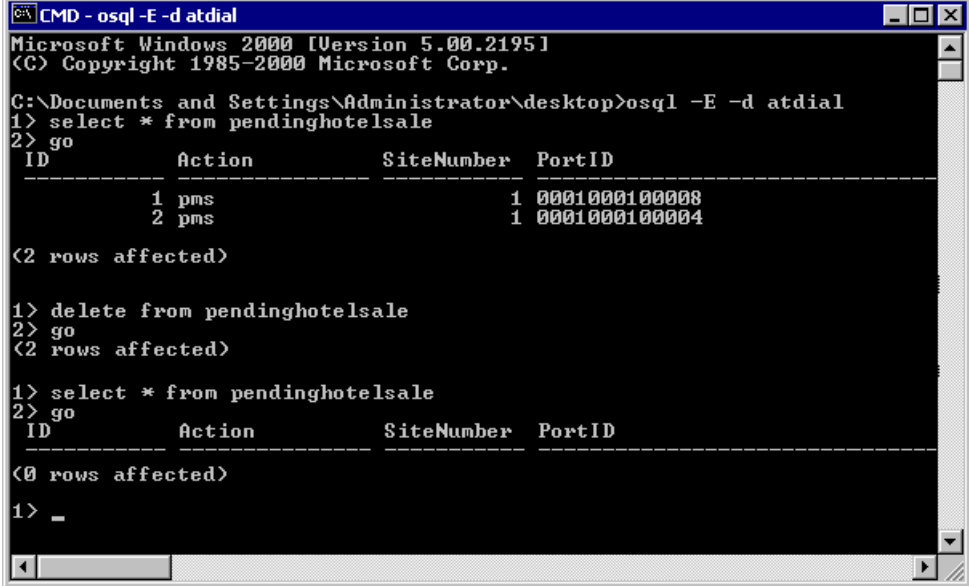
<http://www.cisco.com/en/US/products/sw/netmgts/ps533/index.html>

Clearing Pending Hotel Charges

Before room mapping, you must disable the PMS from the Billing PMS or Billing Printer web page in WEBconfig so guest room charges will not be posted to the PMS when you are mapping rooms. However, if charges are generated, they will probably need to be cleared from the pendinghotelsale database table before actual room charges start accruing. Follow these steps to clear the charges.

-
- Step 1** Open a DOS window.
- Step 2** Type the following commands to display any pending hotel charges:
- ```
osql -E -d atdial (at the 1> prompt.)
select * from pendinghotelsale
go
```
- Step 3** Type the following commands to clear these charges:
- ```
delete from pendinghotelsale
go
```
- [Figure 6-1](#) shows an example of pending hotel charges and the DOS commands that delete them.
- Step 4** Close the DOS window.

Figure 6-1 DOS Commands for Deleting Pending Charges



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

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

1> delete from pendinghotelsale
2> go
<2 rows affected>

1> select * from pendinghotelsale
2> go
  ID          Action          SiteNumber  PortID
  -----
<0 rows affected>

1> _
```

Troubleshooting Tips

The following sections describe problems that you or the end user might encounter when using BBSM and the suggested actions for resolving them.

No BBSM Start Page

The end user does not receive the BBSM Start page when opening the browser. The *Sorry, a network error has occurred* error message appears. This is also known as an RME 19+7 error.

Possible Cause	Suggested Resolution
The user is trying to connect to BBSM through an unsupported network device or through a network device that is not set up within BBSM.	<p>Follow these steps:</p> <ol style="list-style-type: none"> 1. Verify that all network devices on site are on the supported hardware list and that they are correctly set up in BBSM. 2. From the WEBconfig NavBar, click Network Elements > Site # (where # is the site number). Click the proper network device type to determine the IP address information of the various network devices. 3. Verify the connectivity to all network devices by pinging their IP addresses. 4. Verify the correct configuration of the network devices. 5. Correct any information and add any necessary network device information to the WEBconfig pages. Refer to the chapter on configuring network devices in the <i>Cisco BBSM 5.3 Configuration Guide</i>. <p>Note You may need to update the port map if any changes were made to the switch information.</p> <ol style="list-style-type: none"> 6. Attempt to connect a client to verify that the problem has been resolved.
Previously generated map settings have been corrupted, one or more network devices were added to this site and the settings were not updated, or port settings have never been configured for this site.	<p>Follow these steps:</p> <ol style="list-style-type: none"> 1. Update or generate the port configuration. Refer to the chapter on configuring network devices in the <i>Cisco BBSM 5.3 Configuration Guide</i>. 2. Attempt to connect a client to see whether the problem has been resolved.
The SNMP read-write community string on the switch does not match the BBSM server.	Change the SNMP read-write community string so that the server and the switch match. Refer to the chapter on configuring network devices in the <i>Cisco BBSM 5.3 Configuration Guide</i> .
A previously configured switch has lost its configuration.	<p>Reconfigure the switch with the correct IP and SNMP parameters. These parameters may be obtained from an up-to-date copy of the network diagram.</p> <p>Note An onsite technician must perform this step.</p>

No Internet Access

The end user receives the Start page but cannot access the Internet and receives the *you are connected but...* error message.

Possible Cause	Suggested Resolution
The client is using a private IP address and the router is not configured with a static route to the BBSM internal network.	Reconfigure the external router with a static route to the internal NIC.
The DNS server is not set to obtain DNS information from the Internet.	Enter the IP address of the ISP's DNS server. Refer to the section on configuring DNS forwarding in the <i>Cisco BBSM 5.3 Configuration Guide</i> .
The DNS server has cached bad information or is not started.	Restart the DNS server: <ol style="list-style-type: none"> 1. Select Start > Programs > Administrative Tools > Services. 2. Right-click DNS Server and choose Start (or Restart).
The Internet may be slow or the site may not be responding.	The user should try to log on later or try another Internet site.
The Internet connection (T-1 or T-3) from the ISP to the site may be down.	Submit a trouble call with the ISP.

Email Not Working

Users cannot send or receive email using their ISP account while connected to BBSM.

Possible Causes	Suggested Resolution
<p>The end user's ISP does not accept email from unrecognized sources or IP addresses to prevent its email server from being used as a spam gateway.</p> <p>Normally, the user's computer receives its IP address from the ISP itself, so the address is recognized as valid. When the user logs on to the BBSM network, the user's computer receives its IP address from the BBSM server, which the ISP sees as foreign.</p> <p>When the user tries to send email to this server, the server ignores the email because it does not recognize the source IP address as being on its own network.</p>	<p>If the BBSM network provider has set up an SMTP server to resolve this problem, the IP address of that server can be configured within BBSM. BBSM then intercepts all SMTP packets and forwards them to the IP address. This solution precludes the need for users to reconfigure their email program. Set the SMTP forwarding address as follows:</p> <ol style="list-style-type: none"> 1. From the Dashboard, click WEBconfig. The BBSM Server Settings web page appears. 2. Enter the IP address or FQDN of the SMTP server in the SMTP Forwarding IP Address field and click Save. <p>Note The ISP may have to add the external IP address of the BBSM server to the SMTP server list of allowed IP addresses from which to receive SMTP packets.</p>
The user normally connects to the Internet through his or her corporate network, which is behind a firewall.	<p>In this instance, users must tunnel into their corporate network to receive email. Refer to the resolution above to enable users to send mail only.</p> <p>The ISP may have to add the external IP address of the BBSM server to the SMTP server list of allowed IP addresses from which to receive SMTP packets.</p>

PMS Charges Not Posting

Charges are not posting to the PMS.

Possible Cause	Suggested Resolution
Locations (or rooms) may have been mapped incorrectly.	If you entered port rooms or locations the first time by using the Port Locations field in the Port Control window, you cannot verify that ports were mapped to the correct room number. The only way that you can ensure that your port-to-room mapping is accurate is to map rooms by using the Map Rooms option in WEBconfig. After the rooms have been mapped, you can update the port locations by using the Port Control window. (Refer to the section on mapping rooms in the <i>Cisco BBSM 5.3 Configuration Guide</i> .)
BBSM is not set up for PMS billing.	Turn on the PMS billing. To enable PMS billing, refer to the chapter on configuring site PMS billing or print billing in the <i>Cisco BBSM 5.3 Configuration Guide</i> .
The Athdmn service is not started.	As of BBSM 5.2, Athdmn is set to start automatically. If it has been turned off, you need to restart the Athdmn service: <ol style="list-style-type: none"> 1. Click Start > Settings > Control Panel > Administrative Tools. 2. Double-click Services. 3. Right-click athdmn and click Start. The charges should start to post. 4. Close all windows.
The PMS is not connected to the BBSM server.	Check the following: <ul style="list-style-type: none"> • Verify that the BBSM server is physically connected to the PMS. Refer to the chapter on connecting the PMS or local printer in the <i>Cisco BBSM 5.3 Configuration Guide</i>. • Verify that the correct communications port settings (COM and TCP) and PMS protocol are being used. • From the Dashboard, launch WEB PMS Test and send a test charge to the PMS to verify connectivity. (Refer to the WEB PMS Test section on testing the PMS interface in the <i>Cisco BBSM 5.3 Configuration Guide</i>.)
Some PMS systems require that a guest must be checked into a room before the charge can be accepted. This check-in can occur during the room mapping part of an installation when you test the charges that are being sent to a room.	Have someone at the front desk temporarily check the installer into the room being tested. After the PMS test charge is successfully completed, the installer can be checked out of the room.

RADIUS Problems

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

Possible Cause	Suggested Resolution
RADIUS is not correctly configured on the BBSM server.	<p>Check the following:</p> <ul style="list-style-type: none"> Verify that you can ping the RADIUS server IP address from the BBSM server: <ul style="list-style-type: none"> From the WEBconfig NavBar, click Billing > RADIUS > Server. Verify that the RADIUS servers are configured with the same shared secret (password) as the shared secret entered in WEBconfig. Verify that on the BBSM server RADIUS authentication is started and the authentication port is set to the same port that the RADIUS server is using. The default RADIUS port is 1645. Verify that the RADIUS server is configured to accept RADIUS requests from the BBSM server. Verify that the user account is set up and is active on the RADIUS server. Verify that the BBSM server is using the correct page set.

Software Download Failures

The patch or service pack transfer failed.


Possible Cause	Suggested Resolution
The Java plug-in may not be installed on the computer or the wrong version is installed.	<p>Install the Java plug-in that is provided on the software download page onto the computer that is doing the transferring:</p> <p>http://www.cisco.com/pcgi-bin/tablebuild.pl/bbsm53</p>
There is a bad or busy remote connection.	<p>If you can, access the BBSM server locally and transfer using WEBpatch.</p> <p>Another workaround is to place the file in the following folder directly into the folder to which the file is being transferred: c:\inetpub\patch</p>
You may be trying to transfer a very small patch from the BBSM internal network.	Install the patch directly on the BBSM server.

The install failed. You may receive various messages.

Possible Cause	Suggested Resolution
The file is corrupt.	Compare the size and Message Digest 5 (MD5) of the file against the size and MD5 that is listed on the software download page. If the file is not exactly the same, it may have become corrupt when it was downloading from the software download page. If the file is corrupt, download it again. In this case, the patch log will probably show a 0 for the patch number.
The patch may already be installed.	<p>If you have already installed a patch and try to install it again, a pop-up error message appears, stating that the installation was not successful.</p> <p>You can verify whether or not a patch was already installed by looking in two places:</p> <ul style="list-style-type: none"> • The Patches page lists the patch in the drop-down menu. • The Patch Log shows the details of all attempted patch installations. <p>Select the patch and look at the details to determine whether or not a patch has been successfully installed. If you tried installing the same patch a second time and the first install was successful, you do not need to take any further action.</p>
A patch dependency has not been met.	The Patch Log shows you if the patch has a dependency that has not been met. The release notes for the patch describe any dependencies that must be met before the patch can be installed.
For many of the Microsoft patch installers that we create, the connection to WEBpatch is lost during the installation. The installation then appears to fail and the page cannot be displayed.	<p>If you disturb the server while the patch is still installing, the installation may fail. (These patches are always described in release notes, so read the appropriate release note for the download instructions.)</p> <p>Check the following:</p> <ul style="list-style-type: none"> • Verify that the patch has been installed. It should appear in the drop-down menu on the Patches web page. If it is not listed, you can install it again. • Consult the Microsoft bulletin for a way to verify that the patch was installed successfully. • Very rarely, the patch shows that has been installed even though it is only partially installed. After trying all other workarounds, adjust the database manually. (You may want to contact the Cisco TAC. Refer to the “Obtaining Technical Assistance” section in the preface to this operations guide.)

BBSM Not Functioning

BBSM no longer functions.

Possible Cause	Suggested Resolution
The IP addresses, were not changed correctly.	<p>Verify with the customer that the Address Change Wizard was used to change the BBSM NIC IP addresses. If it was not used, use the Network Control Panel reset the IP addresses of the BBSM NICs back to the previous settings and run the Address Change Wizard to change the BBSM NIC IP addresses to the correct settings. Refer to the section on running the Address Change Wizard in the <i>Cisco BBSM 5.3 Configuration Guide</i>.</p> <p>Verify the WEBconfig information and, if necessary, change it. Launch WEBconfig. Change the IP address data on these web pages: IP Addresses, Routers, and Network Elements > Site # (where # is the site number). Refer to the chapters on changing the IP address ranges and configuring routers and network devices in the <i>Cisco BBSM 5.3 Configuration Guide</i>.</p> <p>Verify the DNS server address and change it if necessary. Refer to the section on configuring DNS forwarding in the <i>Cisco BBSM 5.3 Configuration Guide</i>. (All network hardware must have its IP address settings changed separately by a technician.)</p>
A network device has been disconnected. The problem could be a bad Ethernet cable, an unplugged Ethernet or power cable, or the switch itself might be malfunctioning. If a switch is merely misconfigured, traffic still passes through. The client would receive a DHCP address, and support staff could reach switches located downstream of the suspected switch.	<p>Using utilities such as ping and Telnet, along with the network diagram, follow these steps to determine the most probable location of the failure:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;">  <p>Caution If you are replacing switches or moving cables, return cables to the same port or the port configuration will be invalidated.</p> </div> <ol style="list-style-type: none"> 1. Determine which switches are not responding using the ping utility. 2. Telnet into a visible switch, if available, and try to ping the nonresponsive switches again. 3. An IT technician must perform these steps: <ul style="list-style-type: none"> – Check the unresponsive switches to ensure that all power and cable connections are good. – Check the lights for link status and ensure that the correct cables were used. – Power cycle the switch by unplugging the power cable, waiting 5 to 10 seconds, and plugging the power cable back into the switch. – Unplug the uplink cable from the suspected switch and plug it into a laptop configured for DHCP. Try to get an IP address. If you cannot get an IP address, the problem is probably upstream. If you can get an IP address, the problem is probably downstream. – Configure the laptop with the IP address of the BBSM internal NIC and plug it into the uplink port of the suspected switch. Try to ping the switch. 4. If the problem with a switch or switches cannot be resolved, replace the switches. <p>Note Switch-to-switch and router-to-computer connections require a crossover cable. Switch-to-computer connections require a straight-through cable.</p> <p>Use the network diagram to determine which, if any, switches are downstream of the suspected switch. (The network diagram may not reflect recent changes.)</p>

Using the Trace Debugging Utility

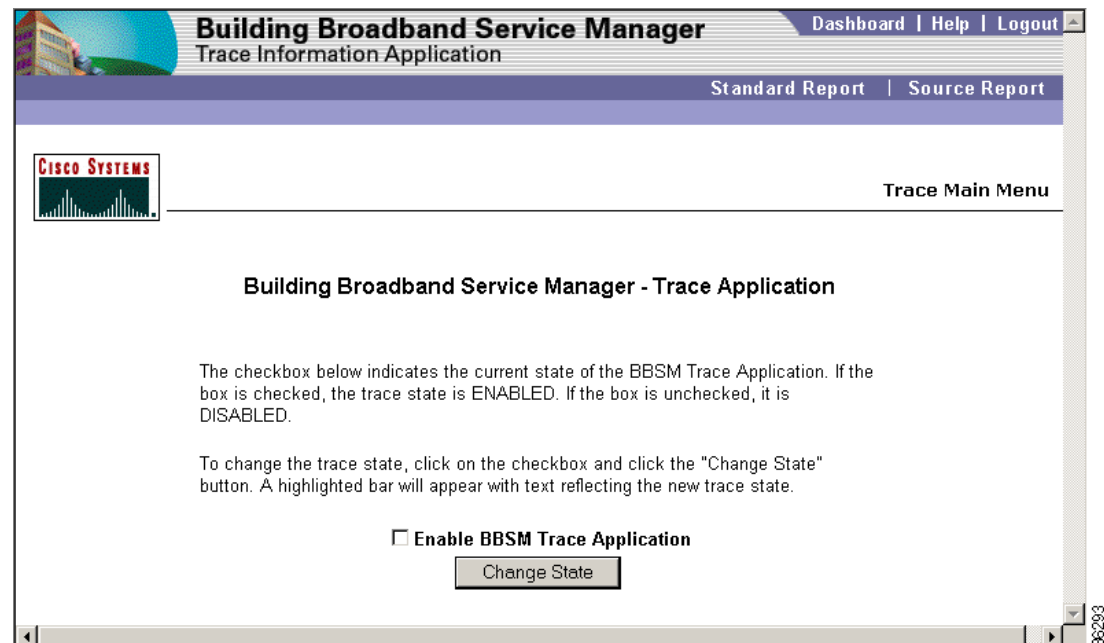
You can use the *Trace* BBSM debugging utility to debug problems. This section provides basic steps for using the Trace application. The *Cisco BBSM 5.3 SDK Developer Guide* provides additional information about using Trace that can be useful to developers.

**Caution**

Enabling Trace affects system performance, so Cisco recommends that you disable it after you have finished using the utility.

- Step 1** Open Internet Explorer.
- Step 2** Enter **http://<bbsm_server:9488>/trace/** where <bbsm_server> is the IP address of the BBSM server in the address field. If you are running the browser on the server, you can replace <bbsm_server> with *localhost* and then press **Enter**. The Trace Information Application web page appears. (See [Figure 6-2](#).)

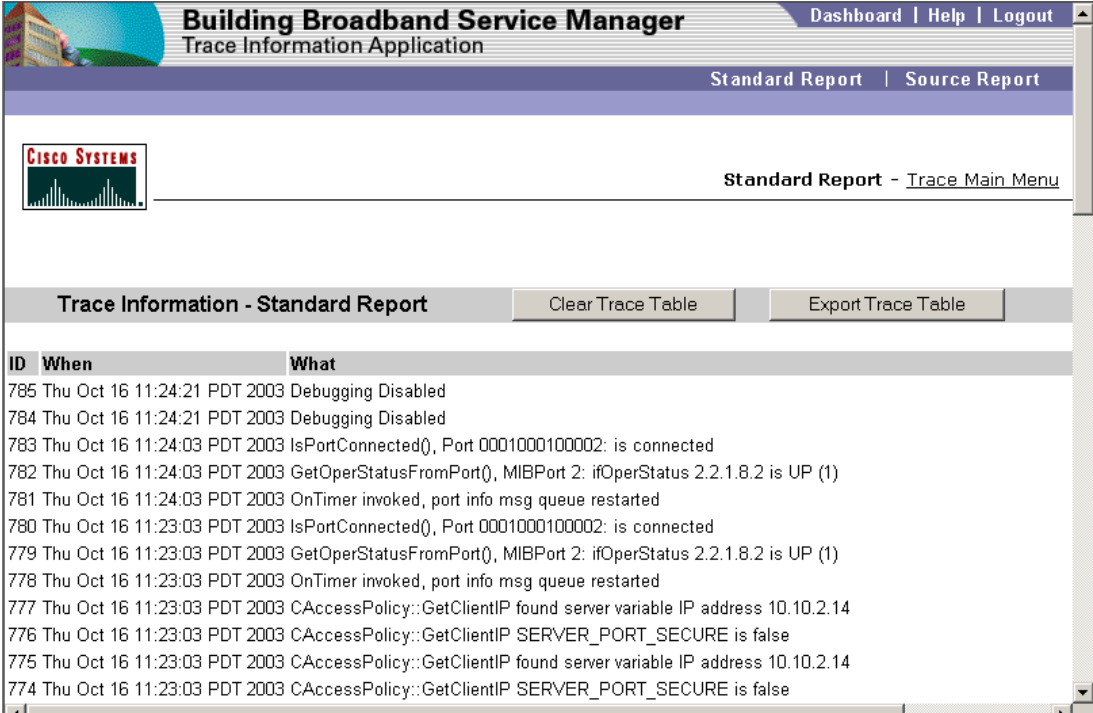
Figure 6-2 Trace Information Application Web Page



- Step 3** To enable the trace application (or trace logging), check the **Enable BBSM Trace Application** check box, and then click **Change State**.
- Step 4** To view the results of the trace, click the **Standard** or **Source** links.
- Step 5** To export the trace information table, click **Export Trace Table**.

Figures [6-3](#) and [6-4](#) show examples of the trace Standard and Source reports.

Figure 6-3 Trace Standard Report



Building Broadband Service Manager
Trace Information Application

Dashboard | Help | Logout

Standard Report | Source Report

CISCO SYSTEMS

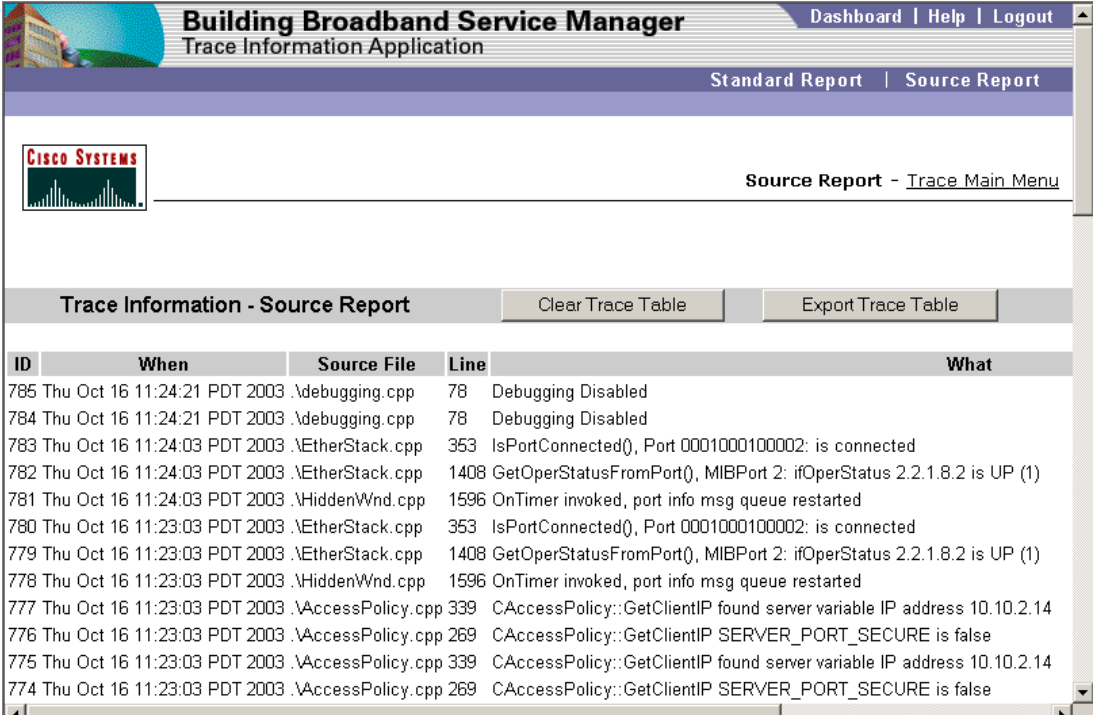
Standard Report - Trace Main Menu

Trace Information - Standard Report

Clear Trace Table Export Trace Table

ID	When	What
785	Thu Oct 16 11:24:21 PDT 2003	Debugging Disabled
784	Thu Oct 16 11:24:21 PDT 2003	Debugging Disabled
783	Thu Oct 16 11:24:03 PDT 2003	IsPortConnected(), Port 0001000100002: is connected
782	Thu Oct 16 11:24:03 PDT 2003	GetOperStatusFromPort(), MIBPort 2: ifOperStatus 2.2.1.8.2 is UP (1)
781	Thu Oct 16 11:24:03 PDT 2003	OnTimer invoked, port info msg queue restarted
780	Thu Oct 16 11:23:03 PDT 2003	IsPortConnected(), Port 0001000100002: is connected
779	Thu Oct 16 11:23:03 PDT 2003	GetOperStatusFromPort(), MIBPort 2: ifOperStatus 2.2.1.8.2 is UP (1)
778	Thu Oct 16 11:23:03 PDT 2003	OnTimer invoked, port info msg queue restarted
777	Thu Oct 16 11:23:03 PDT 2003	CAccessPolicy::GetClientIP found server variable IP address 10.10.2.14
776	Thu Oct 16 11:23:03 PDT 2003	CAccessPolicy::GetClientIP SERVER_PORT_SECURE is false
775	Thu Oct 16 11:23:03 PDT 2003	CAccessPolicy::GetClientIP found server variable IP address 10.10.2.14
774	Thu Oct 16 11:23:03 PDT 2003	CAccessPolicy::GetClientIP SERVER_PORT_SECURE is false

Figure 6-4 Trace Source Report



Building Broadband Service Manager
Trace Information Application

Dashboard | Help | Logout

Standard Report | Source Report

CISCO SYSTEMS

Source Report - Trace Main Menu

Trace Information - Source Report

Clear Trace Table Export Trace Table

ID	When	Source File	Line	What
785	Thu Oct 16 11:24:21 PDT 2003	.\debugging.cpp	78	Debugging Disabled
784	Thu Oct 16 11:24:21 PDT 2003	.\debugging.cpp	78	Debugging Disabled
783	Thu Oct 16 11:24:03 PDT 2003	.\EtherStack.cpp	353	IsPortConnected(), Port 0001000100002: is connected
782	Thu Oct 16 11:24:03 PDT 2003	.\EtherStack.cpp	1408	GetOperStatusFromPort(), MIBPort 2: ifOperStatus 2.2.1.8.2 is UP (1)
781	Thu Oct 16 11:24:03 PDT 2003	.\HiddenWnd.cpp	1596	OnTimer invoked, port info msg queue restarted
780	Thu Oct 16 11:23:03 PDT 2003	.\EtherStack.cpp	353	IsPortConnected(), Port 0001000100002: is connected
779	Thu Oct 16 11:23:03 PDT 2003	.\EtherStack.cpp	1408	GetOperStatusFromPort(), MIBPort 2: ifOperStatus 2.2.1.8.2 is UP (1)
778	Thu Oct 16 11:23:03 PDT 2003	.\HiddenWnd.cpp	1596	OnTimer invoked, port info msg queue restarted
777	Thu Oct 16 11:23:03 PDT 2003	.\AccessPolicy.cpp	339	CAccessPolicy::GetClientIP found server variable IP address 10.10.2.14
776	Thu Oct 16 11:23:03 PDT 2003	.\AccessPolicy.cpp	269	CAccessPolicy::GetClientIP SERVER_PORT_SECURE is false
775	Thu Oct 16 11:23:03 PDT 2003	.\AccessPolicy.cpp	339	CAccessPolicy::GetClientIP found server variable IP address 10.10.2.14
774	Thu Oct 16 11:23:03 PDT 2003	.\AccessPolicy.cpp	269	CAccessPolicy::GetClientIP SERVER_PORT_SECURE is false

- Step 6** To clear the trace information, click **Clear Trace Information Table**.
- Step 7** After running the trace, disable trace logging to prevent system performance from being degraded. On the Trace Main Menu, uncheck the **Enable BBSM Trace Application** check box and click **Change State**. (If you reboot the server, the trace is disabled.)
-



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	<i>See ASP.</i>
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. <i>See also Operator and Reports user.</i>
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	<ol style="list-style-type: none">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 <i>barred</i> 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 <i>0x0100</i> . 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 <i>0x0010</i> .

C

CA	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. <i>See also</i> CA.
certificate authority	<i>See</i> 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. <i>See also end user.</i>
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 <i>DHCP client</i> , 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 <i>www.ispemail.com</i> . 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 <i>user</i> .
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. <i>See internal network.</i>

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 <i>http://www.microsoft.com/default.asp</i> is <i>www.microsoft.com</i> .

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.

H

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.

I

ICMP	Internet Control Message Protocol. ICMP is a TCP/IP protocol used to send error and control messages. For example, a router uses ICMP to notify the sender that its destination mode is not available. A ping utility sends ICMP echo requests to verify the existence of an IP address.
IETF	Internet Engineering Task Force. The IETF is the main standards organization for the Internet. It is a large, open, international community of network designers, operators, vendors, and researchers concerned with identifying problems and opportunities in IP data networks and proposing technical solutions to the Internet community.
IIS	(Microsoft) Internet Information Server. IIS is Microsoft's web server that runs under Windows NT. You can install a certificate on the server to enable it to serve pages using Netscape's SSL security protocol.
Inetinfo	Inetinfo is the process in the Microsoft IIS in which the BBSM Access Policy ActiveX server components run.
integrator	A software developer that uses the BBSM SDK to extend the functionality of the BBSM.
internal adapter	The internal adapter communicates with the local area network (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. <i>See also external network.</i>
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 <i>consoles</i> (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. <i>See also bridged networks, fully routed networks, and mixed networks.</i>
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 <i>0x0100</i> .
network element	<i>See NE.</i>

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.
<hr/>	
O	
operator	A BBSM user who can perform some administrative functions on the BBSM server but does not have access to the full administrative interface. An operator is allowed to change entries in the port map and access code tables. Operator access is on a per-site basis. <i>See also Administrator and Reports user.</i>
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. <i>See also service restart and server reboot.</i>
<hr/>	
P	
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 <code>Connecting...</code> message. The post page calls the functions needed to connect the end user.
Property Management System	<i>See PMS.</i>
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. <i>See also Operator and Administrator.</i>
RFC	Request for Comments. An RFC is a series of notes on topics concerning the Internet. RFCs can be purely informational, or they can specify a proposed, draft, or approved Internet standard. Online versions of RFCs are available at the following URL: http://www.ietf.org/rfc.html

rogue user	An end user who attempts to access the BBSM server fraudulently or maliciously.
routed network	In routed networks, some computers cannot communicate with each other directly. Instead, they must send packets through one or more relays (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 <i>receive</i> , as contrasted with <i>transmit</i> .

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 <i>ToD server</i> .
TX	A communications abbreviation for <i>transmit</i> , as contrasted with <i>receive</i> .

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	<i>See end user.</i>

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. <i>See also XML device.</i>
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, <code><IP>192.168.10.1</IP></code> is an XML device. <i>See also XML.</i>



A

Access Code History reports [2-13](#)
access code reports [2-9](#)
Active Ports reports [2-7](#)

B

BBSM server, other documentation [vi](#)

C

Calendar Day Offset [2-2](#)
changing
 port settings [4-1](#)
clearing pendinghotelsale database table [6-1](#)
Client Deactivation option [1-1](#)
Client for Microsoft Networks check box, unchecking [5-1](#)
clients
 deactivating [1-1](#)
 reactivating [1-4](#)

D

Deactivate Clients web page [1-2](#)
deactivating clients [1-1](#)
debugging, Trace utility [6-9](#)
documentation, related [vi](#)

E

email, troubleshooting [6-4](#)
enabling, Trace debugging utility [6-9](#)
exporting trace debugging data [6-9](#)

I

installing service packs or patches using WEBpatch [5-1](#)
Internet access troubleshooting [6-4](#)

L

logging
 trace debug entries [6-9](#)

M

mapping reports [2-15](#)
monitoring system status [3-1](#)

N

network devices, monitoring [3-1](#)

O

operating system, monitoring [3-1](#)

P

patches, installing with WEBpatch [5-1](#)
pendinghotelsale database table charges, clearing [6-1](#)
PMS troubleshooting [6-5](#)
Port Control option [4-1](#)
ports
 testing [4-5](#)
 updating port settings [4-1](#)
problems [6-3](#)
publications, related [vi](#)

R
RADIUS

- reports [2-19](#)
- troubleshooting [6-6](#)
- Reactivate Clients web page [1-4](#)
- reactivating clients [1-4](#)
- remote access, unchecking Client for Microsoft Networks [5-1](#)
- Reporting Pages option [2-1](#)
- reports
 - Access Code History [2-13](#)
 - Active Ports [2-7](#)
 - Mapping [2-15](#)
 - RADIUS [2-19](#)
 - Transaction History [2-4](#)
 - Unused Code [2-10](#)
 - Usage [2-2](#)
 - Walled Garden [2-21](#)
- routed networks, Mapping reports [2-15](#)

S

- security, deactivating clients [1-1](#)
- service packs, installing with WEBpatch [5-1](#)
- services, monitoring [3-1](#)
- software downloads, troubleshooting [6-6](#)
- SQL, using with transaction history reports [2-4](#)
- Start page, troubleshooting [6-3](#)
- system status [3-1](#)
- System Summary web page [3-1](#)

T

- testing ports [4-5](#)
- Trace debugging utility [6-9](#)
- Transaction History
 - reports [2-4](#)
 - types [2-5](#)
- troubleshooting [6-1](#)
 - charges not posting to the PMS [6-5](#)
 - email not working [6-4](#)
 - no BBSM functionality [6-8](#)

- no Internet access [6-4](#)
- no start page [6-3](#)
- RADIUS problems [6-6](#)
- software download failures [6-6](#)
- Trace debugging utility [6-9](#)
- WEBpatch logs [5-5](#)

U

- unchecking Client for Microsoft Networks check box [5-1](#)
- Unused Code reports [2-10](#)
- uplink ports, configuring [4-5](#)
- Usage reports
 - Calendar Day Offset [2-2](#)
 - generating and viewing [2-2](#)

V

- viewing
 - WEBpatch logs [5-5](#)
- viewing installed patches or service packs [5-1](#)
- viruses, deactivating clients [1-1](#)

W

- Walled Gardens reports [2-21](#)
- WEBpatch web pages [5-1](#)

[Products & Solutions](#)[Ordering](#)[Technical Support](#)[Learning & Events](#)[Partners & Resellers](#)[About Cisco](#)

News

[Cisco Wireless Solution Helps UCSF Improve Patient Care](#) 01 Apr 2004

[Jakarta International School Deploys Cisco IP Tel and Security](#) 01 Apr 2004

[JARING Deploys Cisco IPCC](#) 31 Mar 2004

[Cisco Launches Intelligent Transportation Solutions Program](#) 30 Mar 2004

[New Networking Solution Suite for Transportation Industry](#) 30 Mar 2004

[More News](#)

Direct Access

Software Downloads

Industries

Resources For:

[Large Enterprise](#)

[Small & Medium Business](#)

[Home & Home Office](#)

[Service Provider](#)

[Investors](#)

[Government](#)

[Press](#)

Log In

→ [Log In](#) to access additional tools and content.

→ New User? [Register Now.](#)

Quick Links

[Technical Documentation](#)

[Partner Locator](#)

[Find a Service Provider](#)

[Security at Cisco](#)

[Career Certifications](#)

[Discussion Forums](#)



THIS IS THE POWER OF THE NETWORK. now.

→ [LEARN MORE](#)

BUSINESS INDUSTRIES AND SOLUTIONS +

BUSINESS INDUSTRIES

MANUFACTURING

Cisco Growing With Technology Awards

Manufacturing

Cisco Growing With Technology Awards

E-Commerce

Grand Prize Winner

By Howard Baldwin

Photographs by Emily Nathan

☐ Corrugated Supplies Company

☐ **Web Address:** www.csclive.com

☐ **Business Focus:** Manufacture of corrugated sheets to be used for boxes, displays, and other products

☐ **In Brief:** Lead times as low as 18 hours, with 50% of orders received, produced, and delivered in less than 24 hours

☐ **Location:** Bedford Park, Illinois

☐ **Employees:** 101

☐ **Executive Sponsor:** David G. Pung, Director of Information Services

Technology never moved fast enough for [Corrugated Supplies Company \(CSC\)](#), which produces corrugated paper that its customers use to create custom packaging and displays. Former majority owner Rick Van Horn envisioned a world where customers could access CSC's corporate systems long before the Web transformed business practices. As early as 1990, CSC took the extraordinary step of supplying its customers with PCs running a customer application that enabled them to dial in to CSC's corporate servers to place and track orders. In 1991, CSC employees were using wireless scanners running on a proprietary network and linked to a custom-built enterprise information system to track lading materials. The company was an e-commerce pioneer before most people had even heard the term.

This enthusiasm to embrace technology, while initially invigorating, eventually frustrated David G. Pung, a software developer for whom CSC was a client and who is now the company's director of information services. "As one of the suppliers, you'd get excited," remembers Pung, "but then the reality of what you could actually make happen with available technology set in."

Van Horn has moved into a supporting role at the company, but present majority owner John Potocsnak has continued CSC's focus on innovation and now, finally, technology has caught up. The Web and its networking standards have given CSC the flexibility it needs: Of the 600 orders CSC processes daily, roughly 85% are placed online through the company's extranet. CSC turns around the majority of those orders within 24 hours. That's important for CSC's customers, because they tend to be small "sheet plants" that compete with huge, vertically integrated companies such as [Georgia-Pacific Corp.](#) and Weyerhaeuser.

CSC uses its network to offer efficiency as well. Pung has developed software that enables CSC's customers to enter instructions from their clients into their systems, which then automatically generate orders for CSC. The customer receives an e-mail confirming the transaction.

"Our customers are now managing the flow of manufacturing raw material through our Web site, rather than just placing orders," says Pung. "It's a

Search:

Let Cisco Help You

[Contact](#) a Cisco Representative

Further Reading

First Runner-Up

Coastal Photography

☐ **Web Address:** coastal-photography.com

☐ **Business Focus:**

Professional photography

☐ **Location:** Greenville, North Carolina

☐ **Employees:** 5

☐ **Executive Sponsor:** Elbert Kennard, Owner

Second Runner-Up

Metrobank

☐ **Web Address:** metrobanker.com

☐ **Business Focus:**

Community banking

☐ **Location:** Farmington Hills, Michigan

☐ **Employees:** 65

☐ **Executive Sponsor:** Sherry Desbrough, Assistant Vice President, Information Services

transparent supply chain at its finest."

The Web site also enables CSC's customers to customize their orders more easily. If a customer wants its corrugated sheets stamped with a company logo instead of CSC's, it can specify so on the order-entry Web site. Changing an order prior to its completion—even if it's in the queue for a machine—simply requires that the customer click on an "edit" icon next to the order. (The icon and the ability to edit an order don't disappear until the order is actually on the machine.) The Web-based ordering system lets CSC offer more special requests. And because these are automated, CSC eliminates human error from the process. Finally, because CSC's own inventory information is integrated with the system, customers can see immediately—not days after they were expecting a shipment—whether an order can be fulfilled.

The Web site also incorporates shipping information. It tracks all products as they come off the manufacturing line and are loaded either into trailers or placed in a temporary inventory area. Customers can view not only the contents of the trailer but the sequence in which items were loaded, so they can move the corrugated paper to the designated packaging machinery more quickly once it has arrived at their facilities. In the end, says Pung, this reduces transaction costs because customers don't have to put the paper into inventory and then try to find it later. "This results in better production control, reduced inventory—a real just-in-time environment," he says.

Pung admits to one problem with being on the leading edge: All customers are different. "Some people let us manage their raw materials without their having to buy inventory software, while others have systems so archaic they'll never tie in to our purchase-order system," he says. "You have to accept that not everybody moves at the same pace. They have a whole list of problems, and my biggest problem may not be their biggest problem."

Nonetheless, being a small business has distinct advantages, one of which is the ability to create software specifically for your own needs, according to Pung. "You can buy someone else's software and live within the confines of it, but if you know how you want your business to run, you can build it to improve the value proposition for your customer," he says. "When you're dealing with commodity product, like a corrugated sheet, you have to add something more to it or you'll be in a pricing war. Technology makes you efficient enough to challenge that."

[Back to top](#)

iQ Magazine, First Quarter 2004

About the Author

Silicon Valley-based freelance writer Howard Baldwin has more than 20 years of experience as a business technology journalist. He is a regular contributor to *iQ Magazine*.

Rate this Article:

[See Readers' Top-Rated Articles](#)

[BUSINESS INDUSTRIES & SOLUTIONS](#) | [NETWORKING SOLUTIONS & PROVISIONED SERVICES](#) | [PRODUCTS & SERVICES](#) | [ORDERING](#) | [TECHNOLOGIES](#) | [TECHNICAL SUPPORT](#) | [LEARNING & EVENTS](#) | [PARTNERS & RESELLERS](#) | [ABOUT CISCO](#) |

[Home](#) | [Log In](#) | [Register](#) | [Contacts & Feedback](#) | [Site Help](#)

© 1992-2004 Cisco Systems, Inc. All rights reserved. [Terms and Conditions](#), [Privacy Statement](#), [Cookie Policy](#) and [Trademarks](#) of Cisco Systems, Inc. [Terms and Conditions](#), [Privacy Statement](#), [Cookie Policy](#), and [Trademarks](#) of Cisco Systems, Inc.