



Release Notes for Cisco BBSM 5.2

February 2004

These release notes describe features and caveats for the Cisco Building Broadband Service Manager (BBSM) 5.2. Updated upgrade installation instructions are also included.



Note

The most current Cisco documentation for released products is available on Cisco Connection Online (CCO) at <http://www.cisco.com>. Online documents may contain updates and modifications made after the paper documents are printed.

Contents

This release note contains the following sections:

- [Introduction, page 2](#)
- [New and Changed Information, page 2](#)
- [Upgrading BBSM from Software Release 5.1 to 5.2, page 3](#)
- [Before You Start, page 5](#)
- [Upgrade Procedure, page 7](#)
- [Important Notes, page 9](#)
- [Open Caveats, page 12](#)
- [Obtaining Documentation, page 15](#)
- [Documentation Feedback, page 16](#)
- [Obtaining Technical Assistance, page 16](#)
- [Obtaining Additional Publications and Information, page 17](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

Introduction

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

BBSM supports multiple authentication and billing options, including credit cards, property management systems (PMSs), and access code. A comprehensive software developer’s kit (SDK) is available that helps you customize interfaces. BBSM is available as a preloaded server appliance, or you can purchase the software separately and install it yourself.

New and Changed Information

BBSM 5.2 is built on the baseline functionality of BBSM 5.0 and 5.1 with the addition of new features and upgrades to some existing features. In addition, for BBSM 5.2, Microsoft Windows 2000 Service Pack 2 has been updated to Windows 2000 Service Pack 3.

The following are the new or upgraded features for BBSM 5.2.

Bandwidth reservation

Enables hotel guests to reserve minimum bandwidth for upcoming meetings and sets up classes of service (bandwidth rates) for these reservations. The feature adds a calendar interface for scheduling access codes and bandwidth management. The group bandwidth management does not affect the existing bandwidth throttling feature. Both can be used on the same BBSM server.

Two-way PMS

Expands the BBSM interface to the PMS to be bidirectional. This provides the ability for BBSM to retrieve guest data from the PMS. This data can then be used to enhance the end-user experience by providing customized content. This feature also provides an interface for viewing guest folios and guest checkout from the room.

Client selection between public and private IPs

Allows service providers to “upsell” their public IP addresses to VPN users as a premium service. Eliminates the VPN issues that occur with the use of private IP addressing. Enables service providers to confidently say that all VPN clients are supported.

Cable modem private IPs and client public IPs

Allows for a more cost-effective allocation of VPN-capable public IP addresses to clients and of private IPs to cable modems. Both devices are granted IP addresses from one central DHCP server located on the BBSM server.

Mapping cable modem ports and locations in one step

Allows the technician to map the cable modem port and the location at the same time. Does not require an active session.

RADIUS prepaid account support

Allows RADIUS end users to prepay for Internet service from their Internet service provider (ISP).

Support for Cisco switch clustering

Reduces the number of required IP addresses from one per switch to one per cluster (up to 16 switches). BBSM can recognize the entire cluster through one manageable IP address.

Broadband roaming

Allows BBSM to support broadband roaming by adding a new client-BBSM interface and changes to the BBSM-RADIUS interface, while maintaining backwards compatibility with existing BBSM applications. This BBSM release supports the iPass Smart Client.

Session deactivation feature

Allows a BBSM administrator or operator to terminate any active session through the Dashboard, which enables the administrator to have additional control to deactivate any malicious users.

New Page Set Wizard

Allows BBSM administrators to create their own custom DailyHotel page set by using a web-based wizard, which simplifies custom page set creation.

Improved Switch Discovery Wizard

Quicker and easier switch discovery to simplify configuration. Works with access points and switches in a bridged network topology.

MSDE “sa” and BBSD password changes

Provides a user-friendly way to change the Microsoft SQL Server Data Engine (MSDE) “sa” and BBSD login passwords.

New web API for posting PMS charges

Provides an interface for remote applications to post room charges to the PMS.

Improved GUI to simplify configuration and usability

Includes a new Start page for connecting to the Internet, improved port-mapping capabilities, improved navigation in WEBconfig, and the combination of two similar applications, Port Control and Subscription Port Control, into one application: Port Control.

Upgrading BBSM from Software Release 5.1 to 5.2

This section describes how to upgrade from BBSM software release 5.1 to 5.2.

All of the patches that you need to perform this upgrade are located on the BBSM 5.1 to 5.2 Upgrade Utility CD. Use one of the following procedures to obtain the upgrade package:

- If you have a Cisco service contract—Use the part number on the following Cisco Product Upgrade Tool website to request the Cisco BBSM 5.2 upgrade package:
<http://tools.cisco.com/gct/Upgrade/jsp/index.jsp>
- If you do not have a Cisco service contract—Contact your local Cisco account manager to place an order for the upgrade package (part number BB-SM-5.2-UPG=).

**Caution**

This upgrade can only be performed on a BBSM 5.1 server with all BBSM service packs and patches applied. You can access the required service packs and patches at the Cisco BBSM 5.1 Software Download website: <http://www.cisco.com/pcgi-bin/tablebuild.pl/bbsm51>. To determine the proper installation sequence, click **Read More** next to the note at the top of this web page.

Before you begin the upgrade, make sure that both the internal and external NICs are plugged in and enabled, or the upgrade will fail.

The upgrade consists of the following four separate patches that can be installed locally on a BBSM server or on multiple BBSM servers remotely from another computer.

Patch 5200 (WEBpatch51Upgrade.exe)

- Installs an upgraded version of WEBpatch.dll.
- Adds the necessary directory permissions to the c:\atcom\patch directory.
- Increases the default ISA timeout from 2 to 12 minutes.
- Reboots the BBSM server.

Patch 5201 (Upgrade51to52Part1.exe)

- Creates a temporary account and password.
- Sets up a registry for auto-login after reboot.
- Installs BBSM 5.2 c:\atcom files.
- Converts the BBSM 5.1 Atdial database to the BBSM 5.2 Atdial database and creates the Atdmn database.
- Removes these obsolete registry entries: Cisco2950, Cisco2950-48, Cisco3550-12, Cisco3550-24, Cisco3550-48, FidelioSerial.
- Reboots the BBSM server twice. After the server reboots the first time, the auto-login takes place, which causes the BBSM 5.2 DLL files to be registered. The temporary account and password are deleted, and the auto-login registry entry is cleared. Then the server reboots a second time.

Patch 5202 (Upgrade51to52Part2.exe)

- Installs Windows 2000 Service Pack 3 (SP3) if it is not already installed
- Reboots the BBSM server.

Patch 5203 (Upgrade51to52Part3.exe)

- Installs Microsoft Internet Explorer 6 (IE6) if it is not already installed and these Microsoft post-SP3 hotfixes for Q323255, Q326830, Q328145, and Q323759.
- Updates the Atdial database to reflect the BBSM 5.2 (1.0) release
- Removes the obsolete BBSM 5.1 c:\atcom\webconfig\help directory
- Reboots the BBSM server

Before You Start

Please read the following important information before you begin the procedure.

CSCdz57736

When you upgrade BBSM, the CMTS-specific router and switch configuration is not properly transferred. If you have a CMTS configured on your BBSM server, do not upgrade. This will be fixed in the next upgrade patch. There is no workaround.

CSCdz76629

If you are upgrading a BBSM 5.1 server with Patch 1069 applied, the BBSM server remains in the initializing state and does not move to the running state. Consequently, all clients fail to connect after the upgrade. In this case, the workaround is to install Service Pack 1 (SP1) to the BBSM server after the upgrade is complete.

Important Notes

- Before you begin the procedure, make sure that you have enough free disk space to complete the installation. The upgrade requires an additional 365 MB of hard disk space on your server.
- The patches must be installed in the order shown in the procedure. Otherwise, the upgrade will fail, and your BBSM server could become unstable. After installing each patch, verify that the previous patch was successfully installed.
- For additional information about using WEBpatch to install the patches and verify the installations, refer to the “Viewing and Installing Service Packs or Patches (WEBpatch)” section of the *Cisco BBSM 5.2 User Guide*.
- If you use the Site Controller and/or Building Broadband Service Director (BBSM) features, you must upgrade these features at the same time as the BBSM upgrade or BBSM will not function properly. Refer to the BBSM 5.2 website for the downloads and release notes.

Updating Custom DLLs

Update your custom dynamic link libraries (DLLs) by using the BBSM 5.2 SDK. For a customized switch DLL, use the BBSM 5.2 SDK to generate a new registry file and enter the DLL in the registry after the upgrade.

Restoring BBSM 5.1 Custom Page Sets

To restore custom BBSM 5.1 page sets that have the same default names as BBSM 5.2 page sets, go to the c:\atcom\Patch\backup5201 directory and copy them to the appropriate location.

Restoring Your Own TFTP Server

This caution applies only if you have installed your own TFTP server on BBSM. When you upgrade BBSM, the existing TFTP server is replaced by the Cisco TFTP server, and the existing registry entries are overwritten with the following values. After the upgrade, you will need to restore your original TFTP server:

```
[HKEY_CURRENT_USER\Software\Cisco Systems Inc.\Cisco TFTP Server\1.1\Options]
"LogFileName"="C:\\atcom\\TFTPServer\\Log\\TFTPServer.log"
"TFTPRootDirectory"="C:\\atcom\\TFTPServer"

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TFTP]
"Description"="Cisco TFTP Server"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TFTP\parameters]
"AppDirectory"="c:\\atcom\\TFTPServer"
"Application"="c:\\atcom\\TFTPServer\\TFTPServer.exe"
```

To save your original TFTP server and restore it after the upgrade, follow the steps below. The procedure explains how to export part of your Windows registry before the upgrade and then restore your TFTP server after the upgrade, or if you have already upgraded to BBSM 5.2 and did not export the TFTP registry settings before the upgrade, the procedure explains how to restore your TFTP server at this time.

-
- Step 1** Choose **Start > Run**. The Run dialog box appears.
- Step 2** Enter **regedit**, and click **OK**. The Registry Editor window appears.
- Step 3** Double-click **HKEY_LOCAL_MACHINE**:
- If you are exporting the TFTP registry settings before performing the upgrade, continue with [Step 4](#).
 - If you have performed the upgrade without exporting the TFTP registry settings and want to restore them, go to [Step 5](#).
- Step 4** If you have not performed the upgrade yet, export the registry file, install the upgrade, and reload the registry file, as follows:
- a. Navigate to **System > CurrentControlSet > Services > TFTP**, and select the TFTP folder.
 - b. Export the registry file. From the Registry menu, select **Export Registry File**, enter a file name, and click **Save**. (Do not enter a file extension. The file defaults to a .reg file.)
 - c. From the Registry menu, select **Exit** to close the registry application.
 - d. Install the BBSM 5.2 Upgrade. When you have finished installing the upgrade, the TFTP server running on BBSM will be the Cisco TFTP server.
 - e. To restore your original TFTP server as the default, double-click the .reg file you saved in [Step 4b](#) and click **Yes** to reload your settings back into the registry.
- You have completed this procedure.
- Step 5** If you have already performed the upgrade without exporting the registry file, restore your TFTP settings as follows:
- a. Navigate to **System > CurrentControlSet > Services > TFTP > Parameters**.
 - b. Double-click the AppDirectory text. In the Edit String window, change the Value Data text to the directory of your TFTP server and click **OK**.
 - c. Double-click the Application text. In the Edit String window, change the Value Data text to the name of your TFTP application and click **OK**.
 - d. From the Registry menu, click **Exit** to close the registry application.

You have completed this procedure.

Upgrade Procedure

Follow the steps below in the exact order shown to install the upgrade.

-
- Step 1** Load the BBSM 5.1 to 5.2 Upgrade Utility CD on your BBSM server.
- For a local BBSM installation, go to [Step 4](#).
 - For a remote BBSM installation, continue with [Step 2](#). Note the following about remote installations:
 - It usually takes about 5 or 10 minutes for the server to restart and for BBSM to initialize. If you are using Windows 2000 Professional (SP2 or later) or Windows XP Professional to install the patch remotely, the web pages will load very slowly unless you uncheck the **Client for Microsoft Networks** check box in the Windows NIC Properties window.
-
- Step 2** In the IE browser Address field, type **http://<external_NIC_address>:9488/www**, where <external_NIC_address> is the external NIC address of the remote BBSM server. For example, type **http://192.168.38.1:9488/www**, and press **Enter**. The Enter Network Password window appears.
- Step 3** Enter your username and password (leave the Domain field blank) and click **OK**. The remote BBSM Dashboard appears. Note that you must have administrator privileges to log on.
- Step 4** Install the first patch, Patch 5200, as follows:
- a. From the Dashboard, use the WEBpatch utility to install Patch 5200, Upgrade51to52Part0.exe. The patch usually takes about 10 minutes to install, including the automatic server reboot.



Note For details on how to uncheck the Client for Microsoft Networks check box, refer to the “Configuring Windows 2000 Professional or XP Professional” section of the *Cisco BBSM 5.2 User Guide*.

- Because of known issues with certain versions of Netscape Navigator, use Microsoft Internet Explorer 6 (IE6) for remote installations.



Caution The Java 2 plug-in, version 1.3.1_03, must be installed on the computer you are using to transfer the patches, whether you are installing the patches remotely or directly on the BBSM server.

- If you are installing patches using a remote computer, the Java plug-in must be installed on that remote computer.
- If you are installing directly on the BBSM, the Java plug-in must be installed on your BBSM server.
- You must use this version: other versions will fail.
- If the plug-in is not installed already, click **Go To Java Download Page**, download the plug-in, and install it. You can also go to the BBSM 5.2 Software Download web page and download the plug-in from there.

- b. Verify that the patch was installed. From the WEBpatch BBSM Patch Log web page, view the logs for Patch 5200. If the “InstallPatch successful for” and “Reboot successful” logs appear, the patch installed successfully. (See [Figure 1](#).)

Figure 1 WEBpatch BBSM Patch Log Web Page showing Patch 5200

Building Broadband Service Manager
WEBpatch

Dashboard | Help | Logout

CISCO SYSTEMS

WEBpatch - Patch Log

Patches | Transfer | Install Patch | **Patch Log**

BBSM Patch Log

Patches: 5200
Trace Level: Summary
Log Type: All

Go Default

Patch Log Data

Date Time	Patch#	Detail
04/13/2003 18:34:03	5200	CPatchUtil::InstallPatch started
04/13/2003 18:34:17	5200	CPatchUtil::InstallPatch successful for: Upgrade51to52Part0.exe
04/13/2003 18:34:17	5200	CPatchUtil::Reboot successful

88846

- Step 5** Install the second patch, Patch 5201, as follows:
- From the Dashboard, use the WEBpatch utility to install Patch 5201, Upgrade51to52Part1.exe. The patch usually takes 15 minutes to install, including two automatic reboots that occur during the installation.
 - Verify that the patch was installed, as explained in [Step 4b](#).
- Step 6** After installing the second patch, Patch 5201, using Microsoft Internet Explorer, delete cookies and other temporary Internet files on your computer, as follows:



Caution You must perform this step before installing Patch 5202 for the installation to be successful.

- From the Microsoft IE browser, choose **Tools > Internet Options**.
- From the Temporary Internet files area, do the following:
 - Click **Delete Cookies** and click **OK**.
 - Click **Delete Files**, check the **Delete all offline content** check box, and click **OK**.
 - Click **Settings**, click the **View Files** button, and verify that there are no temporary Internet files.
- Close the Temporary Internet Files window, and then click **OK** twice to exit the Settings and Internet Options windows.
- Close Internet Explorer and reboot your computer.

Step 7 Install the third patch, Patch 5202, as follows:

Note If Windows 2000 SP3 is not installed on your BBSM server, Patch 5202 takes about 20 minutes to install, including the reboot. If you have installed SP3, it takes about 3 minutes to install, including the automatic reboot.

- a. From the Dashboard, use the WEBpatch utility to install Patch 5202, Upgrade51to52Part2.exe.
- b. Verify that the patch was installed, as explained in [Step 4b](#).

Step 8 Install the fourth patch, Patch 5203, as follows:

- a. From the Dashboard, use the WEBpatch utility to install Patch 5203, Upgrade51to52Part3.exe. The patch usually takes about 10 minutes to install, including the automatic reboot.
- b. Verify that the patch was installed, as explained in [Step 4b](#).



Caution

If you performed a BBSM server upgrade from software release 5.0 to 5.1 and then to BBSM 5.2, clients can no longer connect; they receive an error message instead of the Start page. This is caused by a duplicate DLL file. To resolve this problem, delete the GenericSwitchNoLinkStatus.DLL file in the c:\atcom\install\switches directory. (The latest version of this file is in the c:\atcom\install directory. Do not delete the DLL file from this directory.) After you delete this file, you must restart the BBSM server.

If you do not have direct access to the BBSM server, you can delete this file remotely by installing Patch 5223 (BBSM5.0to5.2DLLPatch.exe), which is available for download at this Cisco website: <http://www.cisco.com/cgi-bin/tablebuild.pl/bbsm52>. After you install this patch, the BBSM server reboots automatically.

Important Notes

The following sections provide updated BBSM information.

Single-VLAN Configuration Note

If you are using a single-VLAN configuration and Cisco Ethernet switches and want to use a non-default management VLAN ID, you must change the Ethernet switch's VLAN ID. The switch's SNMP password configured in WEBconfig must be appended with @<management VLAN #>, which enables BBSM to discover ports in the VLAN. For example, if the switch's SNMP read-write community string is *private* and its management VLAN # is *100*, change the switch's BBSM SNMP password to *private@100*. You can also use the Switch Discovery Wizard to specify the management VLAN when you are adding switches to BBSM.

Indexed SNMP passwords are not supported on Cisco Aironet access points. Do not append @<VLAN ID> to the SNMP passwords of the access points on BBSM even if the access point management VLAN ID is not 1. If a non-default management VLAN ID is used on the access points, make sure that the management VLAN is set up as a native VLAN on the access points and on the switch trunk that the access points are connected to. For more information, see CSCed74734.

Access points are not configured automatically with a default VLAN. If you add, remove, or change any VLAN configuration from an access point, you must reconfigure the access point port settings by using WEBconfig. For additional information, refer to the *Cisco BBSM 5.2 User Guide*.

CyberSource Note

BBSM software includes a credit card accounting policy that invokes an application program interface (API) that is provided by CyberSource to interface with the CyberSource ICS credit card processing system. Included in the CyberSource API is a digital certificate, `CyberSource_SJC_US.crt`, which authenticates a CyberSource ICS server and a command line application, `Ecert`, to configure ICS merchant IDs from that ICS server. On January 16, 2004, the digital certificate expired and CyberSource changed its merchant ID configuration logic so that `Ecert` is now obsolete.



Note

BBSM servers that were previously configured with CyberSource ICS merchant IDs for BBSM credit card accounting still operate correctly. It is not necessary for existing customers that are using the ICS accounting policy to make any changes on their BBSM server.

BBSM administrators who want to use the BBSM ICS credit card accounting policy must configure an ICS merchant ID on the BBSM server before end users can use any of the BBSM ICS credit card accounting page sets. One of the steps in configuring the merchant ID is to run `Ecert` with the merchant ID as a command line parameter. `Ecert` communicates with a CyberSource server, authenticated with the previously mentioned digital certificate, and generates a public/private key pair and corresponding digital certificate for the BBSM server and the specified merchant ID. The CyberSource ICS API, when invoked from BBSM, uses the generated keys and certificate to communicate credit card information with a CyberSource ICS server.

Follow these steps to obtain and use the current versions of the CyberSource server digital certificate and the `Ecert` application:

-
- Step 1** From the BBSM server, go to `c:\opt\ics\keys`, and rename the `CyberSource_SJC_US.crt` file to **CyberSource_SJC_US.crt.old**.
- Step 2** Go to the CyberSource website (http://www.cybersource.com/support_center/management/keyupdate).



Note You need a CyberSource account to access this page.

-
- Step 3** Locate and download the following files to `c:\opt\ics\keys`:
- `CyberSource_SJC_US.cer`
 - `ecert-nt-3.4.10.exe`
- Step 4** Open a DOS window, and enter **cd c:\opt\ics\keys**.
- Step 5** Press **Enter**.
- Step 6** Enter **ecert-nt-3.4.10.exe <merchantID>**, where `<merchantID>` is your CyberSource merchant ID number, and press **Enter**.
- Step 7** Enter **copy c:\opt\CyberSource\SDK\<merchantID>.*** and press **Enter**.
- Step 8** Enter **copy c:\opt\CyberSource\SDK\CyberSource_SJC_US.crt** and press **Enter**.
- Step 9** Close the DOS window.
- Step 10** Configure BBSM to do credit card billing as described in the *Cisco BBSM 5.2 User Guide* using `<merchantID>` as the credit card billing Merchant ID.
-

Load Balancing Note

With the release of BBSM 5.2, load balancing is no longer supported on this platform.

Cisco Switches Note

The BBSM server does not support the Cisco Catalyst 2950 and 3550 switches with the 12.1(6) or 12.1(9) IOS release. (See CSCdy04210 for more details.) These switches must be upgraded to IOS release 12.1(11) and then configured to use 2950 12.1(11) or 3550 12.1(11) switch types on BBSM.

Two-Way PMS Note

Cisco BBSM v5.2 contains a powerful new feature allowing for two-way communications with a PMS of a hotel. To ensure proper functionality in BBSM v5.2 of the Two-Way PMS interface, you must install BBSM Service Pack 1 (BBSM52SP1.exe), which will be available for download at this Cisco website:

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

The release of this service pack will coincide with the release of the two-way PMS interface documentation in the BBSM software development kit (SDK).

Cisco BBSM 5.2 Quick Start Guide Note

In section 4, BBSM Server Setup, replace the text for Step 5-h with this sentence:

Right-click **BBSM**, and choose **All Tasks > Restart**.

Windows 2000 Regional Settings Note

BBSM 5.2 only supports English (United States) regional settings. Changing these settings adversely affects the functionality of the BBSM server.

Patch 5220 adds support for the English (United Kingdom) regional settings; however, if you do not use access codes, you do not need to install this patch.

Discontinuation of the Site Controller Feature Note

Effective immediately, support for the BBSM 5.2 Site Controller feature will end. This feature allowed one central BBSM server to regulate access to multiple hotels by placing separate Site Controller workstations on the actual site to allow in-room Internet usage charges to be sent to a PMS system or printer. BBSM servers can still support multiple sites, but PMS billing cannot be used.

Central BBSM deployments that currently use the Site Controller feature are affected. The workaround is to do one of the following:

- Do not charge for Internet access.
- Use the other billing methods, such as RADIUS, access codes, or credit card.
- At the remote site, replace the Site Controller with a BBSM 5.2 server.

Open Caveats

This section describes caveats that have not been resolved for BBSM 5.2:

- CSCdy25090

When you edit an existing page set with the Page Set Wizard, a Microsoft JScript runtime error occurs.

The workaround is to restart IIS. If a client has not used the page set to log into BBSM, then the editing works as designed and you do not have to restart IIS. If a client has used the page set, then IIS must be restarted before editing the page set. Use this procedure to restart IIS:

1. From the BBSM Start menu, choose **Programs > Administrative Tools > Services**.
2. From the Services window, right-click **IIS Admin Service**.
3. Click **Restart**.
4. From the Restart Other Services window, click **Yes**. You can now edit your page set with the Page Set Wizard.

- CSCdy45333

When a client connects with an iPass client and the browser has certain client proxy settings, the browser hangs, the browser page is blank, and BBSM shows the port as active. This occurs only when the iPass Dialer is used to connect to BBSM. These are some examples of affected proxy server settings:

- Client using DHCP IP address, proxy = http://www.nosuchname.com, Port 80
- Client using DHCP IP address, proxy = http://www.nosuchname.com, Port 8000
- Client using DHCP IP address, proxy = 10.10.10.50, Port 80 (or Port 8000)
- Client using DHCP IP address, proxy = http://10.10.10.50, Port 80 (or Port 8000)
- Client using static IP address with DNS, proxy = http://www.nosuchname.com, Port 80 (or Port 8000)
- Client using static IP address with DNS, proxy = 10.10.10.50, Port 80 (or Port 8000)
- Client using static IP address with no DNS, proxy = 10.10.10.50, Port 80 (or Port 8000)
- Client using static IP address with no DNS, proxy = http://10.10.10.50, Port 8000

The workaround is to set your browser to no proxy.

- CSCdy53542

When you use Netscape 7.0, the `iport_tools.asp` file can be closed without using the disconnect button.

The workaround is to install an earlier version of Netscape Navigator.

- CSCdy60290

If no network cables are connected when the Address Change Wizard is run, BBSM generates a script error and subsequently no clients can connect.

The workaround is to make sure that the network cables are connected when the Address Change Wizard is run.

- CSCdy61653

When you use PMS billing, an Athdmn error message randomly appears.

There is no workaround.

- CSCdy64795
 If CDP is used to discover switches and GBIC ports are used as uplinks, the Switch Discovery Wizard incorrectly marks ports 1 and 2 as uplink ports on those switches with GBIC ports.
 The workaround is to use the Port Control application to manually change the uplink port setting to false.
- CSCdy77529
 Transactions made after the calendar day offset time still appear in the Usage report. When the offset time is set to noon, transactions made after that time incorrectly appear in the Usage report.
 There is no workaround.
- CSCdy79765
 BBSM static clients cannot use FTP if they do not have DNS configured.
 The workaround, if using a static client, is to configure a DNS server address. This allows the static client to use FTP but affects the network settings of the end user. The end user must restore the network settings to their original state when they are done using BBSM.
- CSCdy88153
 When too many rows are selected on the Port Control web page and the Port Settings button is clicked, the client browser times out, the CPU continues to spike until the browser is closed, and a time out message appears.
 The workaround is to select a smaller number of ports at a time when changing settings through Port Control.
- CSCdz02586
 When the Radius or RadiusUband page set is used, and BBSM is configured for multinet, a phantom entry in the Port_State_Radius table may randomly appear.
 There is no workaround.
- CSCdz02597
 Internet Explorer 6.0 cache problems might cause the BBSM GUI to display incorrect values on the BBSM Port Control web page. When the page set value is changed, an incorrect room number and port ID could be presented to the user in the port settings web page each time the user changes the value on a port. Closing the browser may not fix the problem.
 The data on the port list web page might also be incorrect because current values may not appear on the port list. The Requery button can be used to update the list, but when the Port Control web page is closed and then reopened, incorrect values can still appear.
 The workaround is to click the Refresh button on the browser tool bar, or press the F5 key on the keyboard, if the web page content looks outdated or incorrect. Internet Explorer 6 has known issues with web page caching causing web pages to load from the cache displaying incorrect or outdated information.
- CSCdz03762
 When UNKNOWN is applied to a device with an unknown sysObjectID, the Switch Discovery Wizard generates an application error.
 The workaround is to manually add the switch from the Switches web page in WEBconfig by choosing a switch type from the Cisco Switch Type drop-down menu.

- CSCdz04652

When clustered switches are configured at sites 1 and 2, the WEBconfig GUI does not allow users to update the member switches of a cluster in site 2. A pop-up error message appears when a user tries to update the aging period or switch type of any member switches in site 2.

There is no workaround.
- CSCdz05331

Macintosh clients using Microsoft Internet Explorer can initially log on using the SubscriptionHome and SubscriptionHotel page sets, but after they disconnect, the next logon attempt fails. Clients can access the start page, but nothing happens when the Connect button is used. Clients using the DailyHotel page set cannot use the Connect button.

The workaround is for Macintosh clients to use Netscape Navigator 4.7 or 6.2.
- CSCdz06336

When using a bridged cable modem termination system (CMTS) and BBSM is configured for multinet with the cable modem scope being in a different multinet from the temp scope, if a cable modem is replaced by using dynamic port-room configuration, the new cable modem's IP reservation does not have the correct DHCP options set for the reservation.

The workaround is to use Port Control to replace the modem instead of using dynamic port-room configuration.
- CSCdz25098

If you connect and then disconnect from one Catalyst 2950 LRE switch with a single port CPE to another switch before the client MAC address ages out, BBSM incorrectly reports that you are still connected to the Catalyst 2950 LRE switch.

There is no workaround.
- CSCdz29993

When you use Internet Explorer 6.0 SP1, the browser fails to redirect to localhost/www.welcome.asp.

The workaround is to manually type **welcome.asp**.
- CSCdz31023

When using a Catalyst 2924 switch that is configured as a Cisco 2924 VLAN/Port Hub switch type, clients cannot connect to the Internet. They continue to be redirected to the BBSM start page each time they try to connect.

The workaround is to remove the VLAN/Port configurations from the switch and reconfigure the switch as a Catalyst 2924 Hub type in BBSM. If port-to-port security is required, the user can configure the protected port feature on the switch instead. The protected port feature is available on IOS release 12.0.5 XU or later.
- CSCdz49541

Under certain conditions, the Microsoft Internet Security and Acceleration (ISA) client filter DLL sometimes fails to load, but it reloads automatically when the service is restarted.

The workaround is to restart the Microsoft Internet Security and Acceleration (ISA) Server control service.

- CSCed74734

When the Switch Discovery Wizard is used to configure Cisco Aironet access points, and you specify a non-default management VLAN ID for access points, the wizard incorrectly appends @<management VLAN ID> to the access point's SNMP password on BBSM. Consequently, clients cannot connect because Cisco access points do not support indexed passwords.

The workaround is to rediscover Cisco access points with the Switch Discovery Wizard without editing the BBSM VLAN ID field (by leaving the BBSM VLAN ID as 1), or to use WEBconfig to edit and remove @<VLAN ID> from the access point's SNMP password on BBSM.

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.

Related Documentation

The following documents provide information about BBSM:

- *Cisco BBSM 5.2 User Guide* (order number DOC-7814689=)
- *Cisco BBSM 5.2 and BBSD Software Installation Guide* (order number DOC-7812741=)
- *Cisco BBSM 5.2 Quick Start Guide* (order number DOC-7814813=)
- *Cisco BBSM 5.2 SDK Developer Guide* (available on Cisco.com)

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from 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_inpck/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 submit e-mail 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, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

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

<http://www.cisco.com/tac>

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

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

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—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. Go to this URL to visit the company store:
<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 online at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. 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>
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the [Related Documentation](#) section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0705R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.