



Release Notes for Cisco BBSM 5.3 Service Pack 2

March 2005
OL-7303-01

These release notes describe the Cisco Building Broadband Service Manager (BBSM) 5.3 Service Pack 2 (SP2), which includes:

- Ten BBSM patches (see [Patches Included in BBSM 5.3 SP2, page 3](#))
- Thirteen Microsoft hotfixes (see [Microsoft Hotfixes Included in BBSN 5.3 SP2, page 3](#))
- Thirteen resolved caveats (see [Caveats Resolved By BBSN 5.3 SP2, page 4](#))
- All caveats resolved by Service Pack 1 (see [BBSM SP2 Caveats, page 6](#))
- Documentation enhancements (see [Changes to BBSM Documentation, page 7](#))

SP2 is released as a web patch on Cisco.com and is incorporated into the default image shipped with the HP/Compaq D530 and Quanta S19 platforms. SP2 is not dependent on any other BBSM patch or service pack, and can be installed on any BBSM 5.3 server. This service pack (BBSM53SP2.exe) is also known as *Patch 5325*.



Note

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

Contents

- [Installation, page 2](#)
- [Patches Included in BBSM 5.3 SP2, page 3](#)
- [Microsoft Hotfixes Included in BBSN 5.3 SP2, page 3](#)
- [Caveats Resolved By BBSN 5.3 SP2, page 4](#)
- [Changes to BBSM Documentation, page 7](#)
- [Important Dual VLAN Note, page 11](#)



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

- [Important Port Hopping Note, page 11](#)
- [Important IP Spoofing Note, page 12](#)
- [Obtaining Documentation, page 14](#)
- [Documentation Feedback, page 15](#)
- [Cisco Product Security Overview, page 15](#)
- [Obtaining Technical Assistance, page 16](#)
- [Obtaining Additional Publications and Information, page 17](#)

Installation

This service pack can be installed locally onto any BBSM 5.3 server with Internet access or remotely onto multiple BBSM servers from another computer.



Caution

We recommend terminating all client sessions during BBSM service pack and patch upgrades and installations. For additional information, see the *Cisco BBSM 5.3 Operations Guide*.

Follow these steps to install BBSM 5.3 SP2 onto your BBSM 5.3 server:

- Step 1** Using the Internet Explorer (IE) web browser, go to the Cisco BBSM 5.3 Software Download website:
<http://www.cisco.com/cgi-bin/tablebuild.pl/bbsm53>



Note

You must use Internet Explorer when using WEBpatch because of known issues and incompatibilities with Netscape Navigator.

- Step 2** Download **BBSM53SP2.exe** to a temporary location on your computer.
- For a local BBSM installation, go to [Step 7](#).
 - For a remote BBSM installation, continue with [Step 3](#).



Note

If you are using the Windows 2000 (SP2 or later) or Windows XP operating systems to install this patch remotely, the WEBpatch web pages load very slowly. To prevent this problem, uncheck **Client for Microsoft Networks** in the NIC Properties window on your remote computer.

- Step 3** In the IE browser field, enter **http://<external_NIC_address>:9488/www**, where <external_NIC_address> is the external NIC address of the BBSM server.



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.

Step 4 Press **Enter**. The Enter Network Password window appears.

Step 5 Enter your username and password. (Do not enter any information in the Domain field.)



Note You must have administrator privileges to use WEBpatch.

Step 6 Click **OK**. The remote BBSM Dashboard appears.

Step 7 From the BBSM Dashboard, use the WEBpatch utility to install this patch.



Note For instructions on transferring and installing BBSM patches and service packs, see the *Cisco BBSM 5.3 Operations Guide*. This service pack automatically reboots your BBSM server.

Patches Included in BBSM 5.3 SP2

These patches are included in BBSM 5.3 SP2:

Patch No.	Description
5301	SP1
5309	Microsoft security fix, MS04-007
5310	Dual VLAN
5311	Fidelio PMS, Date calculation
5314	Microsoft security fixes, MS04-11, MS04-012, MS04-14
5319	Packet Inactivity for 4x0x/6x0x Catalyst Switches
5321	Detecting Lost TCP/IP Connection to PMS
5322	Access Codes Fix
5323	Atdial Termination Fix
5324	Switch Support for 3560-24, 3560-48, 2912, 2924M

Microsoft Hotfixes Included in BBSN 5.3 SP2

The following Microsoft hotfixes are included in BBSM 5.3 SP2:

Table 1 Microsoft Hotfixes Included in BBSN 5.3 SP2

Hotfix No.	Topic
MS04-030	Vulnerability in WebDav XML Message Handler.
MS04-031	Vulnerability in NetDDE.
MS04-032	Windows security update.
MS04-037	Vulnerability in Windows shell; could allow remote code execution.

Table 1 *Microsoft Hotfixes Included in BBSN 5.3 SP2 (continued)*

Hotfix No.	Topic
MS04-039	Vulnerability in ISA Server 2000 and Proxy Server 2.0. Could allow Internet content spoofing.
MS04-040	Cumulative security update for IE.
MS04-044	Vulnerabilities in Windows kernel and LSASS.
MS05-008	Vulnerability in Windows shell; could allow remote code executions.
MS05-011	Vulnerability in server message block. Could allow remote code execution.
MS05-012	Vulnerability in OLE and COM. Could allow remote code execution.
MS05-013	Vulnerability in the DHTML editing component of ActiveX control. Could allow remote code execution.
MS05-014	Cumulative security update for IE. This update includes the cumulative security fixes in security update 867282 and the fixes for Internet Explorer that were released after the publication of Microsoft security bulletin MS04-040.
MS05-015	Vulnerability in Hyperlink Object Library. Could allow remote code execution.

Caveats Resolved By BBSN 5.3 SP2

This service pack includes caveats resolved in SP2. These appear below those resolved in SP1.

BBSM SP1 Caveats

This section describes the caveats that were resolved with BBSM 5.3 SP1.

- CSCec52226
When BBSM has an incorrect RADIUS shared secret (password), the RADIUS Authentication server now writes a warning message to the event log.
- CSCec72520
When configuring dual VLANs, BBSM no longer reboots continuously if a user forgets to unbind AtNat from the internal NIC.
- CSCec90048
In the ISA outgoing web requests configuration, the connection timeout is now set to 5 seconds.
- CSCed00939, CSCed00986, CSCed01481, CSCed01957, and CSCed02003
To be compatible with BBSM 5.3 SP1, the Cisco Catalyst 3750 with the earlier version of IOS must be upgraded to IOS release 12.1(14) EA1 or later. The port settings for the Cisco Catalyst 3750 switch are now generated correctly.

- CSCed01442
The BBSM 5.3 online help title bar and header have been updated to reflect the current BBSM version number.
- CSCed01446
When you click the “Configuring Dual VLAN's” link in the BBSM 5.3 online help, the correct web page now appears.
- CSCed01452
When you click the “Alerts” link in the BBSM 5.3 online help, the correct web page now appears.
- CSCed01462
When you click the “System Summary” link in the BBSM 5.3 online help, the correct web page now appears
- CSCed02440
The BBSM 5.3 online help Search feature now works as designed.
- CSCed03396
When examining DNS server replies to BBSM clients, BBSM no longer classifies certain normal replies from the DNS server as failure replies. This fix allows for FTP and Telnet applications from Macintosh and certain Unix clients to work properly.
- CSCed23220
Malicious browser clients can no longer use the BBSM web proxy server (ISA) from outside of BBSM.
- CSCed24140
The new RADIUSBlock page set and access policy are very similar to the existing RADIUS page set and access policy. The only difference is that the RADIUSBlock page set now passes a block duration parameter to the RADIUSBlock access policy in the SendActivateSession method invocation and the RADIUSBlock access policy automatically terminates any active sessions when this block duration has been reached.
- CSCed48316
For clients that use the Macintosh IE browser, the BBSM Page Set Wizard now generates page sets that work as designed.
- CSCed59320
When access codes by duration are created with the duration of 60 minutes or longer, the client session now expires and disconnects after the duration specified by the access codes.
- CSCed61653
When port hopping is turned on, clients can now port hop from one network device to another. BBSM no longer incorrectly deactivates the client sessions when clients port hop to another device after the port hop delay timer expires.

BBSM SP2 Caveats

This section describes the caveats that were resolved with BBSM 5.3 SP2.

- CSCee51547
The Page Set Wizard preview feature stopped functioning if the value for the descriptive text contains certain characters, including apostrophes, ampersands, and double quotation marks. The Page Set wizard now safely processes these characters.
- CSCef16148
The “Usage by room” report failed when the port location field contained an apostrophe. Several other reports display the port location field and have been updated to properly handle apostrophes.
- CSCef71288
The Port Test utility in BBSM, by default, set the bandwidth setting for Cable Modem Termination Systems (CMTS) to 10 MB. The default setting caused the utility to report an abnormally high number of errors. The default bandwidth setting for CMTS is now 1 MB.
- CSCef81970
When a network element was defined as “NULL:Clients connect to router” and the user enabled port hopping, clients never disconnected as a result of inactivity. Additionally, if the access code page set was used, access codes were never released. The administrative interface now disables the port hopping check box when the “NULL” switch type is set.
- CSCeg12118
When a Cisco Access Point is defined to use more than one VLAN, and the guest VLAN has an identifier higher than 254, it was assigned to Bridge Group 255. This occurred unless there was a VLAN identifier higher than the value assigned to the guest VLAN value. If the guest VLAN belonged to Bridge Group 255, clients were not redirected correctly to the splash screen. BBSM now correctly displays the splash screen.

In this scenario, BBSM sends improper SNMP queries to determine the MAC address of the client. Consequently, the clients cannot view the splash screen.
- CSCeg23273
During initialization of Atdial, each row in the port map table was updated. If a large internal range was specified (for example, 64K or larger addresses), CPU utilization could spike for an abnormally long period of time. BBSM now optimizes the initialization sequence to reuse SQL connections rather than creating a new connection for each row updated.
- CSCeg30007
When configuring access codes by date, if the ‘Set End Date’ button was clicked without selecting a day in the calendar, the end date was set to the month displayed in the calendar and the day to 31, regardless of whether 31 days were present for the selected month. BBSM now pulls the end date from a month with fewer than 31 days.
- CSCeg31227
When changing IP addressing after the initial configuration of DUAL VLAN, the RRAS Input filters for each VLAN were not changed or removed. The new IP address filter was added along with the old filter. BBSM now removes the old filters.
- CSCeg53266
When WebPatch was used to install a patch and the installation failed, the summary level message that appears in the patch install log indicated completion. BBSM now indicates unsuccessful patch in summary level with reasons in detail level.

- CSCeh14256
The **Dashboard > Port Control > Port Settings** feature failed when the port location field contained an apostrophe. This no longer happens.
- CSCdz57730
The WEBpatch install dropdown clipped off long filenames, particularly in multi-part x.x to y.y upgrade files, and the part number was not readable. This no longer happens.
- CSCed20809
The WEBconfig Software version sometimes displayed an incorrect (rollback) version after a new patch was installed. This no longer happens.
- CSCeh32156
BBSM rebooted if a client released the DHCP lease and certain timing conditions were met. This no longer happens.

Changes to BBSM Documentation

The *Cisco BBSM 5.3 Software Installation Guide*, the *BBSM Network Device Compatibility Guide*, and the *BBSM 5.3 SPI Configuration Guide* are changed by SP2.

Changes Affecting the *Cisco BBSM 5.3 Software Installation Guide*

Changes in this service pack affect the information in the *Cisco BBSM 5.3 Software Installation Guide*. This document currently is located at http://www.cisco.com/en/US/products/sw/netmgtsw/ps533/prod_installation_guide09186a00801d8cdc.htm.

Location	Change
Page 3	A note is added: “Third-party servers should have only two NICs.If platform has more than two NICs, BBSM will not function properly and will not correctly set up the routing from the internal to the external network.”
Location TBD	A caution is added: “Caution: Do not install a PIX firewall between BBSM and the PMS. The firewall must be configured to permit communication between the BBSM and PMS servers.”
Location TBD	A note is added: “Note: For two Ethernet interfaces, use third-party servers to create either two single-port network interface cards or a single dual-port interface card.”

Changes Affecting the *BBSM Network Device Compatibility Guide*

Changes in this service pack affect the information in the *BBSM Network Device Compatibility Guide*. This document currently is located at http://www.cisco.com/en/US/products/sw/netmgtsw/ps533/products_user_guide09186a00801a9752.html.

Changes to Table 4

Use the following updated table in place of Table 4. New and changed information is highlighted.

Table 4 Supported Cisco Catalyst Ethernet Switches

Cisco Catalyst Switch	Drop-Down Listing in the Cisco Switch Type Menu	Client Monitoring Type	BBSM Hotspot 1.0	BBSM 5.1	BBSM 5.2	BBSM 5.3
1900 <i>(does not support port-to-port security)</i>	Cisco 1900	Link status		X	X	X
2912 series	Cisco 2912	Link status		X	X	X
	Cisco 2912 Packet	Packet inactivity			X	X
	Cisco 2912M	Link status		X	X	X
	Cisco 2912 VLAN/Port	VLAN/Port		X	X	X
2916M	Cisco 2916M	Link status		X	X	X
2924 series	Cisco 2924	Link status		X	X	X
	Cisco 2924 Hub	Forwarding table			X	X
	Cisco 2924 Packet	Packet inactivity			X	X
	Cisco 2924M	Link status		X	X	X
	Cisco 2924M Packet	Packet inactivity			X	X
	Cisco 2924 VLAN/Port	VLAN/Port		X	X	X
	Cisco 2924 VLAN/Port Hub	Forwarding table				X
2940 series	2940	Link status			X	X
	2940 Packet	Packet inactivity			X	X
2948	Cisco 2948	Link status		X	X	X
2950 series ¹	Cisco 2950-12 (v. 12.0)	Link status	X	X	X	X
	Cisco 2950-12 (v. 12.1.11)	Link status	X	X	X	X
	Cisco 2950-24 (v. 12.0)	Link status	X	X	X	X
	Cisco 2950-24 (v. 12.1.11)	Link status	X	X	X	X
	Cisco 2950-48 (v. 12.1.11)	Link status	X	X	X	X
	Cisco 2950Packet-12 (v. 12.1.11)	Packet inactivity	X	X	X	X
	Cisco 2950Packet-24 (v. 12.1.11)	Packet inactivity	X	X	X	X
	Cisco 2950Packet-48 (v. 12.1.11)	Packet inactivity	X	X	X	X
2970 series	2970	Link status			X	X
	2970 Packet	Packet inactivity			X	X
3512 series	Cisco 3512	Link status	X	X	X	X
	Cisco 3512 VLAN/Port ²	Link status	X	X	X	X

Table 4 Supported Cisco Catalyst Ethernet Switches (continued)

Cisco Catalyst Switch	Drop-Down Listing in the Cisco Switch Type Menu	Client Monitoring Type	BBSM Hotspot 1.0	BBSM 5.1	BBSM 5.2	BBSM 5.3
•3524 series	Cisco 3524	Link status	X	X	X	X
	Cisco 3524 Hub	Forwarding table	X		X	X
	Cisco 3524 Packet	Packet inactivity	X		X	X
	Cisco 3524 VLAN/Port ²	Link status	X	X	X	X
3548 series	Cisco 3548	Link status	X	X	X	X
	Cisco 3548 Packet	Packet inactivity	X		X	X
	Cisco 3548 VLAN/Port ²	Link status	X	X	X	X
3550 series ¹ (including the 3550-PWR switch)	Cisco 3550-12 (v. 12.1.11)	Link status	X	X	X	X
	Cisco 3550-24 (v. 12.1.11)	Link status	X	X	X	X
	Cisco 3550-48 (v. 12.1.11)	Link status	X	X	X	X
	Cisco 3550Packet-12 (v. 12.1.11)	Packet inactivity	X	X	X	X
	Cisco 3550Packet-24 (v. 12.1.11)	Packet inactivity	X	X	X	X
	Cisco 3550Packet-48 (v. 12.1.11)	Packet inactivity	X	X	X	
3560 Series	Cisco 3560-24	Link status			X	X
	Cisco 3560Packet-24	Packet inactivity			X	X
	Cisco 3560-48	Link status			X	X
	Cisco 3560Packet-48	Packet inactivity			X	X
3750 series ³	3750	Link status				X
	3750 Packet	Packet inactivity				X
4000 series ⁴	Cisco 400x	Link status		X	X	X
	Cisco 4x0x Packet	Packet inactivity				X
4500 series ⁵	Cisco 4x0x	Link status	X		X	X
6509 ⁶	Cisco 6x0x	Link status	X		X	X
	Cisco 6x0x Packet	Packet inactivity				X

- For the Catalyst 2950 and 3550 switches, you must upgrade to Cisco IOS Release 12.1(11)EA1 or later if you are running Cisco IOS Release 12.1(6) or 12.1(9).
- This network device type supports VLAN per port (Switchport Multi command) for port-to-port security on Cisco Catalyst 2900 and 3500 XL series switches for running Cisco IOS Releases 11.2(8)SA3 through 12.0(5.1)XW. IOS releases later than 12.0(5.1)XW have a new method of implementing port-to-port security through private VLAN edge (port protected and switch port protected). Use Catalyst 2900 or 3500 link status switch types for switches with IOS releases later than 12.0(5.1)XW. For more information, consult the IOS guide for your software release.
- You must upgrade to Cisco IOS Release 12.1(14) EA1 or later to use the Cisco Catalyst 3750 switch with BBSM.
- BBSM was tested with Cisco Catalyst 4006, Supervisor III, Cisco IOS releases 12.1(12c)EW and 12.1(14)E1, and Supervisor IV, Cisco IOS Release 12.1(12c)EW.
- BBSM was tested with Cisco Catalyst 4507, Supervisor IV, Cisco IOS Release 12.1(12c)EW.
- BBSM was tested with Cisco Catalyst 6509, Supervisor I, Cisco IOS release 7.4(3).

Changes Affecting the *Cisco BBSM 5.3 SP1 Configuration Guide*

Changes to Figure 3-4 on Page 3-8

Refer to the following updated figure in place of Figure 3-4 on page 3-8.

Figure 3-4 Address Change Wizard IP Addresses Window (Singlenet, Dual VLAN)

BBSM Internal Network Address Ranges	
DHCP Start	192.168.100.21
DHCP End	192.168.100.230
Management Start	192.168.2.2
Management End	192.168.2.20
Foreign (Static) Start	192.168.100.231
Foreign (Static) End	192.168.100.254

BBSM TCP/IP Properties	
Clients VLAN IP	192.168.100.1
Clients VLAN Subnet Mask	255.255.255.0
Mgmt VLAN IP	192.168.2.1
Mgmt VLAN Subnet Mask	255.255.255.0
External NIC IP	10.10.1.2
External NIC Subnet Mask	255.255.255.0
Default Gateway	10.10.1.1

081980

Additional Changes to Text

Location	Change
Page 11-1, “Overview”	This warning was added: “Warning: Do not install a PIX firewall between BBSM and the PMS. The firewall must be configured to permit communication between the BBSM and PMS servers.”
Page 11-3, “Configuring PMS or Print Billing”	<p>This information on which Fidelio PMS versions are compatible with BBSM was added:</p> <ul style="list-style-type: none"> • Opera 2.0 and above • Fidelio Version 6 (all versions) • Suite 7 (version 13 and above) <p>Add note that the Fidelio PMS must use a specific interface module to communicate with BBSM. The interface details are as follows:</p> <ul style="list-style-type: none"> • Name: CISCO BBSM • Part: 5009-092 • FKT Logo: CIB
Page 11-2, “Two-Way PMS Interface”	<p>This note was added after the first paragraph: “To fully support the Bidirectional Daily Hotel page set, you must both enable bidirection communication and enable the View Folio option on the PMS [server?]. To use the bidirectional page without using the View Folio function, modify the page set to remove or hide the View Folio button.</p> <p>“To hide the View Folio button:</p> <ol style="list-style-type: none"> 1. Edit file C:\atcom\ekgnkm\BiDirectional_DailyHotelStart.asp. 2. Change the value for bBasicService from false to true: <pre>var bBasicService = false; ---> varbBasicService = true;</pre>

Important Dual VLAN Note

With this service pack, you no longer need to use the Intel PROset utility on the BBSM server to create management and client VLANs. VLANS are now fully created, configured, and deleted by using the Address Change and Switch Discovery wizards. For additional information, see the *Cisco BBSM 5.3 Configuration Guide*.

Important Port Hopping Note

Configuring port hopping on a “Null: Clients connect to router” or a packet type Cisco Aironet access point breaks packet inactivity functionality. When this happens, BBSM does not disconnect clients in time. The workaround is to disable port-hopping on those network elements. If the packet inactivity switch type is used, there is no need to turn on port-hopping since packet inactivity allows clients to port-hop.

Important IP Spoofing Note

As referenced in the *Release Notes for Cisco BBSM 5.3*, a new feature has been added in BBSM 5.2 SP2 that detects IP spoofing, which occurs when a second MAC address, such as a laptop, tries to use the same IP address. Consequently, the second MAC address is prevented from accessing the system.

Because the IP address spoofing feature blocks a DHCP client if its IP address is already associated with an existing active session, some DHCP clients cannot connect although they have IP addresses assigned through DHCP. The affected clients cannot ping BBSM's internal NIC address. They receive "The Page Cannot Be Displayed" error message on their browsers.

This problem can occur in these situations:

1. A link status switch type is used when a hub device is connected to a switch port.
2. A hibernating client is connected to a switch that is configured as a link status switch.
3. A long packet inactivity period is used.
4. A combination of long packet inactivity and port hopping is used.

In all of these cases, BBSM maintains a session although a client is no longer in the network or is not requesting to renew the IP address. Since the DHCP server is not aware of the existing session in BBSM, it assigns the IP address to another client when the default lease time expires. When this occurs, the IP address spoofing logic in BBSM blocks packets from the IP address because packets are from a different IP and MAC combination.

IP Spoofing Workaround for Switches

For situations 1 and 2 above, the workaround is either to remove the hub or other device from the port or to change the activity detection method, which is set through WEBconfig.

Otherwise, the switch type of the affected devices must be changed to the packet inactivity switch type, and the packet inactivity period must be configured to be less than 15 minutes. See the ("[Important Port Hopping Note](#)" section on page 11.) To do this:

Step 1 Go to the **Network Elements - Switches** web page in WEBconfig, and use the ">" button to navigate to the switch that needs modification.

Step 2 Click the **Switch Type** drop-down arrow, and change the selected switch type to the correct packet type. For example, if you are using the Cisco Catalyst 2940, you would choose Cisco Catalyst 2940 Packet. As soon as this change is made, the Packet Inactivity Period field is enabled.



Note If you need to use a long packet inactivity period or port hopping, you must increase the DHCP lease time. The minimum DHCP lease time is calculated by using the appropriate formula: $[(PIP \text{ or } PHD + 15 \text{ minutes}) * 2]$ or $[(PIP + PHD + 15 \text{ minutes}) * 2]$, where PIP equals *Packet Inactivity Period* and PHD equals *Port Hop Delay*. For example, if PIP equals 30 minutes and PHD equals 10 minutes, then the minimum DHCP lease time must be changed to 110 minutes $[(30 + 10 + 15) * 2]$. To configure the DHCP lease time, see the "[Increasing the DHCP Lease Time](#)" section on page 13.

Step 3 From the Packet Inactivity Period field, enter a value of time, in seconds, that is 15 minutes or less.

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

Step 5 Repeat for every switch needing this modification.

Only Cisco switches support Packet Inactivity switch types. If you are using other switch types, they are considered legacy devices and are not supported by TAC.

IP Spoofing Workaround for Access Points

For situations 3 and 4 above, the workaround is to reduce the packet inactivity period or the combined packet inactivity periods and port hop delay to be less than 15 minutes. See the [“Important Port Hopping Note” section on page 11](#). To do so, follow these steps:

- Step 1** Go to the Network Elements - Access Point web page in WEBconfig, and use the “>” button to navigate to the access point that needs modification.
- Step 2** Under Access Point Type, change the selected access point type to the correct packet type. For example, if you are using the Cisco Aironet 1100 AP, you would choose Cisco Aironet 1100 Packet.



Note If you need to use a long packet inactivity period or port hopping, you must increase the DHCP lease time, which is calculated by using this formula: $[(PIP \text{ or } PHD + 15 \text{ minutes}) * 2]$ where PIP equals *Packet Inactivity Period* and PHD equals *Port Hop Delay*. For example, if the PIP equals 30 minutes, then the minimum DHCP lease time would be 90 minutes $[(30 + 15) * 2]$. To configure the DHCP lease time, continue to the following section.

- Step 3** From the Packet Inactivity Period field, enter a value of time, in seconds, that is 15 minutes or less.
- Step 4** To save the changes, click **Save**.
- Step 5** Repeat for every access point needing this modification.

Only Cisco access points support Packet Inactivity switch types. If you are using other access point types, they are considered legacy devices and are not supported by TAC.

Increasing the DHCP Lease Time

Follow these steps to increase the DHCP lease time:

- Step 1** From the BBSM desktop, choose **Start > Programs > Administrative Tools > DHCP**. The DHCP window appears.
- Step 2** Right-click the **Scope** folder and choose **Properties**. The Scope BBSM53 Properties window appears.



Note If the Properties option is not visible, wait a few seconds, and right-click the **Scope** folder again.

- Step 3** In the Lease duration for DHCP clients area, enter the correct number of hours and minutes, and click **OK**.
- Step 4** Close the DHCP window.

Related Documentation

The following documents provide information about BBSM:

- *Cisco BBSM 5.3 Configuration Guide* (order number DOC-7815807)
- *Cisco BBSM 5.3 Operations Guide* (order number DOC-7816161)
- *Cisco BBSM 5.3 Software Installation Guide* (order number DOC-7815714)
- *Cisco BBSM 5.3 Quick Start Guide* (order number DOC-7816060)
- *Release Notes for Cisco BBSM 5.3* (available on Cisco.com)

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/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/>
- 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 1 800 553-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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

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>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

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 provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is 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/>

- *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>

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 Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Grow, 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 between Cisco and any other company. (0705R)