



# Release Notes for Cisco BBSM 5.3 Service Pack 1

---

**February 2004**

These release notes describe the Cisco Building Broadband Service Manager (BBSM) 5.3 Service Pack 1 (SP1), which resolves caveats and problems in BBSM 5.3. This service pack (BBSM53SP1.exe) is also known as *Patch 5301*. BBSM 5.3 SP1 contains the Microsoft security update (MS04-003), “Buffer Overrun in MDAC Function Could Allow Code Execution (832483).” This service pack has no dependencies and can be installed on any BBSM 5.3 server.



**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

- [Installation, page 2](#)
- [Important Dual VLAN Note, page 3](#)
- [Important Port Hopping Note, page 3](#)
- [Important IP Spoofing Note, page 3](#)
- [Resolved Caveats, page 5](#)
- [Obtaining Documentation, page 6](#)
- [Documentation Feedback, page 7](#)
- [Obtaining Technical Assistance, page 8](#)
- [Obtaining Additional Publications and Information, page 9](#)



---

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

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

# 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, refer to the *Cisco BBSM 5.3 Operations Guide*.

Follow these steps to install BBSM 5.3 SP1 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/pcgi-bin/tablebuild.pl/bbsm53>


**Note**

Because of some known issues and incompatibilities with Netscape Navigator, you must use the IE browser when using WEBpatch.

- Step 2** Download **BBSM53SP1.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, refer to the *Cisco BBSM 5.3 Operations Guide*. This service pack automatically reboots your BBSM server.

## 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, refer to 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 to either 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 3](#). Follow these steps:

- 
- 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 5](#).

---

- 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 3](#). 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.

## Resolved Caveats

This section describes the caveats that are 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.

## 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 5.3 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)

## 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](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](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](mailto: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.