



Release Notes for the Cisco Building Broadband Service Manager 5.1 Service Pack 2

January 2002

These release notes describe the Cisco Building Broadband Service Manager (BBSM) v5.1 Service Pack 2 (SP2), which resolves caveats and issues in BBSM 5.1, build 22. Subsequent releases of BBSM include these fixes, and many others, without the need to apply this patch.



Note

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

Contents

- [Special Building Broadband Service Director Note, page 2](#)
- [BBSM WEBconfig Note, page 2](#)
- [Increasing BBSM Virtual Memory Note, page 2](#)
- [Resolved Caveats, page 3](#)
- [Installation, page 19](#)
- [Related Documentation, page 20](#)
- [Obtaining Documentation, page 20](#)
- [Obtaining Technical Assistance, page 21](#)



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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

Special Building Broadband Service Director Note

Cisco Building Broadband Service Director (BBSD) is a feature that ships with BBSM 5.1. If you are using BBSD and you install the BBSM 5.1 SP1 on your BBSM Server, you must also install the BBSD 2.0 SP1 on your BBSD Server to get complete data backups.



Caution

BBSD will not correctly restore BBSM 5.1 SP1 data that was backed up before the date and time that the BBSD 2.0 SP1 was installed.

Although BBSD 2.0 is compatible with BBSM 5.1, once the BBSM 5.1 SP2 is installed on the BBSM Server, BBSD 2.0 SP2 must also be installed on the BBSD Server to maintain compatibility between BBSM and BBSD.

BBSD 2.0 SP1 includes a new web page, `Version.asp`, that displays current BBSD version information. To access the version page in BBSD, go to [http://\[ipaddress\]/BBSD/Version.asp](http://[ipaddress]/BBSD/Version.asp), where *ipaddress* is the IP address of the BBSD Server.

BBSM WEBconfig Note

After you install the BBSM SP2, a new check box, Enable Static Client Connections, appears on the Server web page in WEBconfig. Do not uncheck this check box. If you do uncheck it, BBSM 5.1 will only support clients who are configured for Dynamic Host Configuration Protocol (DHCP).

Increasing BBSM Virtual Memory Note

After BBSM 5.1 is installed, the default virtual memory settings need to be changed to increase the virtual memory. If the memory is not increased, Microsoft Internet Information Services (IIS) will fail. Follow this procedure to increase the virtual memory:

- Step 1 From your desktop, right-click **My Computer**.
- Step 2 Select **Properties**.
- Step 3 From the System Properties window, click the **Advanced** tab.
- Step 4 From the Performance area, click **Performance Options**.
- Step 5 From the Virtual memory area, click **Change**.
- Step 6 From the Virtual Memory window, change the **Initial size (MB)** text box to **384** and the **Maximum size (MB)** text box to **768**.



Note

Use these settings for a Dell server with 256 MB of RAM. If you are using a non-Dell server, you must check the amount of physical RAM your server has to calculate these settings. The Initial size equals the amount of RAM times 1.5. The Maximum size equals the amount of RAM times 3.

- Step 7 Click **Set**.
- Step 8 Click **OK** to close the Virtual Memory window.

- Step 9** Click **OK** to close the Performance Options window.
- Step 10** Click **OK** to close the System Properties window.
-

Resolved Caveats

This section describes resolved caveats that are included in BBSM 5.1 SP2.

CSCdt57418

Synopsis

In the RADIUS Servers web page of WEBconfig, when a user tried to update a RADIUS server name by modifying the Server Name field and clicking the Update button, a new server name was created instead of modifying the existing server name.

Cause

The code worked as designed.

Resolution

The Graphical User Interface (GUI) has been modified to be more intuitive for the user. A *New* button has been added to the RADIUS Servers web page of WEBconfig. To update the RADIUS Server parameters, the user modifies the existing form and then clicks the Update Button. To add a new RADIUS Server, the user clicks the New button to get a new form and then clicks the Update button after the new form is completed. When there is no RADIUS server, only the Update button is enabled.

CSCdt64894

Synopsis

A Microsoft JScript runtime error periodically occurred when updating switch information in WEBconfig.

Cause

Unknown. The Bug was inconsistent. It did not halt the performance of any BBSM actions.

Resolution

Three new C++ exception catches have been added to the Update method on the Switches.cpp page.

CSCdt75827

Synopsis

In the Walled Garden web page of WEBconfig, when a user tried to update a Walled Garden host name by modifying the Host Name field and clicking the Update button, a new Walled Garden host name was created instead of modify the existing one.

Cause

The code worked as designed.

Resolution

The Graphical User Interface (GUI) has been modified to be more intuitive for the user. A *New* button has been added to the Walled Garden web page of WEBconfig. To update the Walled Garden parameters, the user modifies the existing form and then clicks the Update Button. To add a new Walled Garden entry, the user clicks the New button to get a new form and then clicks the Update button after the new form is completed. When there is no Walled Garden, only the Update button is enabled.

CSCdt81214**Synopsis**

On the Port Control web page, the *Time of Last Sale* and *Time of Last Configure* is not read-only.

Cause

The code worked as designed.

Resolution

The portForm.asp page has been modified to make the *Time of Last Sale* and *Time of Last Configure* read-only.

CSCdt88911**Synopsis**

From the Call Types web page in WEBconfig, a user was able to edit the Site Number field, which caused confusion whether a record was actually being created or modified and affected WEBconfig.

Cause

The Site Number field could be edited.

Resolution

WEBconfig has been modified. The Site Number field on the Call Types web page has been changed to read-only. However, this fix created another issue regarding the deletion of call types. If the Site Number field cannot be edited and the customer deletes all call types, then a call type could not be recreated. This issue has also been resolved. The default call type can no longer be deleted.

CSCdt90843**Synopsis**

When the Address Change Wizard was used, it attempted to update the LAT table with new IP addresses. However, the LAT table is no longer used in BBSM 5.1. The Address Change Wizard must not affect the LAT table. Instead of updating the LAT table, the Address Change Wizard must update Microsoft Internet Security and Acceleration Server (ISA).

Cause

When Microsoft Proxy was used on the BBSM Server, it was necessary for the Address Change Wizard to update the LAT table. Now that Microsoft Proxy has been replaced with Microsoft ISA, the Address Change Wizard needs to update Microsoft ISA instead.

Resolution

Changes have been made to the Address Change Wizard to remove the update to the LAT table, and to update Microsoft ISA.

CSCdt90876

Synopsis

An administrator could not view codes for a single day by entering the same date into both the Start Date and End Date fields on the Access Code Report.

Cause

Client-side date validation did not allow for the start date and end date to be the same. The end date had to be later than the start date, which was not a user-friendly implementation.

Resolution

The validation has been modified to allow a same day query to take place. If a customer enters the same date in both the Start Date and End Date fields, the Active Server Pages (ASP) logic pulls information from the database with a start time of 12:00:00 AM and an end time of 11:59:59 PM.

CSCdu02442

Synopsis

When the administrator created two sites and tried to update a port on the second site from the Port Control web page, the page set for that port was switched to the Site 1 page set.

Cause

The Site 2 Port Control data was not getting set to the correct site or port ID. The Edit function was using the Site 1 page set information when the Update button was clicked.

Resolution

The portForm.asp page has been modified to correctly set the intended site number and port ID before data is updated.

CSCdu56779

Synopsis

From the Switches web page in WEBconfig, the Cisco 3548 VLAN port was missing from the Switch Type drop-down list.

Cause

There was no *Cisco 3548 VLAN/port* entry in the Switches registry.

Resolution

The GenericSwitch (switches.reg) file has been modified to include the *Cisco 3548 VLAN/port* registry entry.

CSCdu88111

Synopsis

When the client browser was configured to use the same proxy server for all protocols, the client was unable to view page sets using Secure Sockets Layer (SSL).

Cause

The ISAClientIP web filter modified requests by adding a private header to include the client IP. The web filter must not modify secure requests.

Resolution

The ISAClientIP web filter has been modified to ignore secure requests. Atnotify has also been modified to store the client IP in a session variable.

CSCdv20692**Synopsis**

BBSM could erroneously deactivate a session of the virtual private network (VPN) client behind the NULL switch.

Cause

This problem occurred because the NULL switch used an Internet Control Message Protocol (ICMP) echo and echo relay message to determine if the client was still active. If the client launched a VPN, the VPN software could alter the routing table on the client computer preventing the ICMP echo reply from reaching the BBSM. In this case, the BBSM assumed that the session was no longer active when in fact it was active with a VPN connection.

Resolution

ATNAT.sys, atnatcmd.exe, and the NULLSwitch.dll have been modified. They no longer use ICMP echo and echo reply to determine if the client is still active. Instead, ATNAT.sys now keeps track of packet activity from a given client, and the NULLSwitch.dll queries ATNAT.sys to determine how recent a client had activity. If the client has no activity within the aging time associated with the NULL switch, the NULLSwitch.dll reports that the session is no longer active.

CSCdv21688**Synopsis**

When a non-numeric value was entered into the price field, the group of codes was not successfully edited, and an SQL syntax error was returned.

Cause

The price field did not have any type of client-side validation to ensure that only numeric values could be submitted to the database.

Resolution

Client-side validation has been added to ensure that numbers, currency symbols, and periods are the only type of characters accepted. This fix also ensures that no blank entry in the price field is accepted.

CSCdv21702**Synopsis**

Entering a value into the price field on the GenerateCodeForm.asp page, such as 99999999999.999999999999, returned an out of range error from Microsoft Data Engine (MSDE).

Cause

MSDE cannot handle the conversion from a large number that is greater than 16 characters before and after the decimal point.

Resolution

A client-side validation has been added which limits the number of characters entered into the price field. The user can only enter up to 15 characters. If more characters are entered, the user is prompted to enter a smaller number.

CSCdv24274**Synopsis**

If the user left the price field blank when generating new access codes, a syntax error was displayed.

Cause

All fields displayed on the GenerateCodesForm.asp are required fields and pass information to the next page. No blank entries are allowed.

Resolution

Client-side validation was added to the GenerateCodesForm.asp to ensure that a blank entry is not allowed. If a blank entry is present when the form is submitted, a message box appears prompting the user to enter a value.

CSCdv25464**Synopsis**

Clients entered a continuous redirection loop to the start page when they clicked the Disconnect button without closing the browser and then used the browser's Back button to get to the start page. After trying to connect again, a loop occurred.

Cause

The code on the iport_tools.asp page needed updating.

Resolution (Partial)

The iport_tools.asp page has been modified to verify that clients are connected. If they are not connected, the web page closes itself. However, the first time clients try to connect after returning to the start page from the browser's Back button, they receive one redirection to the start page. If they try again, clients successfully connect.

CSCdv26034**Synopsis**

The portal did not open when clients used Netscape versions 4.51, 4.7 or 6.0. The xxxPost.asp page opened but did not close causing an error to appear in Netscape versions 4.5 and 6.0.

Cause

Versions of Netscape that have this problem POST with an invalid content-length header. The browser adds on an additional `\r\n` creating two extra bytes. Microsoft Internet Security and Acceleration Server (ISA) did not handle this, and the fix has an error in it. The ISA stops rejecting the POST and now treats the two extra bytes as part of the next message causing ISA to improperly parse the headers in the next message.

The issue with the client browser not automatically advancing to the portal was not related to ISA and W3Proxy. It pertained to the positioning of the OnUnload script function below the `<head>` tag.

Resolution

The pre-SP1 release of W3Proxy.exe from Microsoft was installed, which ignores the extra \r\n from Netscape. The DailyHotelPost.asp page has been modified causing the Netscape browser to automatically advance to the portal page from the post page.

CSCdv26090**Synopsis**

Users were required to enter a value into the SNMP Password field, which was disabled when the Router did not support SNMP.

Cause

The Community field in the Router table did not accept NULL values.

Resolution

The Router table has been modified to accept NULL values.

CSCdv26092**Synopsis**

There was an error updating the router if the SNMP password field was left blank.

Cause

The database did not allow null values.

Resolution

The database has been modified to accept null values.

CSCdv26752**Synopsis**

When editing access codes, changing the end date or start date to an invalid date, such as 9/31/2001, caused an SQL error.

Cause

MSDE cannot store or process invalid dates. September 31, 2001 is not a valid date string.

Resolution

Client-side validation has been added that prevents the acceptance of invalid dates.

CSCdv27685**Synopsis**

From the Generate Codes web page in Access Code Management, the "\$" sign was missing from the Price field when Bandwidth Manager was enabled.

Cause

The "\$" was missing from the code.

Resolution

The GenerateCodeForm.asp page has been modified to add a “\$” sign when Bandwidth Manager is enabled.

CSCdv27862**Synopsis**

From the Server web page in WEBconfig, after a user checked the Enable Maximum Active Sessions check box and then clicked Update, the Enable Maximum Active Sessions check box did not clear when the Defaults button was later clicked.

Cause

The default for Maximum Active Sessions check box was not set.

Resolution

The code has been modified. The default setting for Maximum Active Sessions has been changed to unchecked.

CSCdv27873**Synopsis**

From the RADIUS Servers web page in WEBconfig, when a user scrolled to any RADIUS Server other than the last RADIUS Server, the parameters of the last RADIUS Server were displayed instead of the current RADIUS Server when the Requery button was clicked.

Cause

The logic for the Requery button on the radius.asp page needed updating.

Resolution

The logic for the Requery button on the radius.asp page has been modified.

CSCdv27883**Synopsis**

From the RADIUS Servers and Walled Garden web pages in WEBconfig, the Requery and Delete buttons were disabled until data was saved. These buttons are enabled in other web pages in WEBconfig.

Cause

Worked as designed.

Resolution

The RADIUS Server and Walled Garden web pages have been modified to enable the Requery button when information is present. However, the Delete button is not active unless data is first saved.

CSCdv28353

Synopsis

The Access Code History report displayed Site 1 information in the Site 2 and Site 3 reports. The Access Code History report must only display information for each respective site.

Cause

There was a missing filter in the SQL Query Statement on the ACHistory.asp page, which allowed individual site information to be shown on all site reports.

Resolution

A filter has been added to the SQL statement that ensures that only Site 1 information displays in Site 1 reports and that only Site 2 information displays in Site 2 reports, etc.

CSCdv28892

Synopsis

The Access Code Report (ACReport.asp) and the Access Code History Report (ACHistoryForm.asp) did not verify that the starting and ending dates were in proper sequence.

Cause

There was no validation in place verifying that the starting date came before the ending date, which prevented information from being displayed on reports.

Resolution

Client-side validation has been added to both of the ACReport.asp and ACHistoryForm.asp pages, which ensures that the starting date is always before the ending date. Validation has also been added to stop invalid dates such as 9/31/2001 from being accepted.

CSCdv29282

Synopsis

During session activation, if the access policy's ActivateSession method failed (returns false), Atdial set the port state to Denied. This prevented the end-user from connecting on subsequent events.

Cause

If the access policy's ActivateSession method fails during session activation, the port state must be set to Inactive. A port state must be set to Denied as a result of accounting policy function errors. When the port state is set to Denied as a result of ActivateSession failure, the pre-connect logic failed when the end user attempted to access the start page.

Resolution

The code has been modified. The port state is now set to Inactive instead of Denied when the access policy's ActivateSession method fails.

CSCdv30748

Synopsis

All site transactions showed up on a selected site for the RADIUS History report.

Cause

The RADIUSReport.asp page did not display transactions according to the site selected.

Resolution

The RADIUSReport.asp page has been modified to display transactions for each selected site only.

CSCdv30892

Synopsis

The RADIUS Session report allowed invalid dates to be submitted, which caused MSDE to display an Out-Of-Date Range error to the client.

Cause

MSDE cannot handle invalid dates and did not allow them to be queried in the database. Dates such as 9/31/2001 or 11/31/2001 are not valid.

Resolution

Client-side validation has been added to verify that invalid dates are not allowed. When an invalid date is entered, a message box appears warning the user that the information is invalid.

CSCdv30938

Synopsis

On the EditCodes.asp page, when bandwidth is disabled, the Bandwidth drop-down selection box was still active. When Bandwidth Management is turned off, this option must be disabled.

Cause

No code was inserted to check for bandwidth management activation. Consequently, the page displayed the drop-down selection box for bandwidth regardless of whether the feature was turned on or off.

Resolution

Server-side code has been inserted into the EditCodes.asp page to ensure that the drop-down selection is enabled if the Bandwidth Management is turned on and disabled if the Bandwidth Management is turned off.

CSCdv32420

Synopsis

From the RADIUS web page in Reporting Pages, it was possible to successfully enter a start date that was later than the end date.

Cause

The Start Date and End Date fields did not have any type of client-side validation to ensure that an end date value was later than a start date value.

Resolution

Client-side validation has been added to ensure that the end date is later than the start date.

CSCdv35111**Synopsis**

From the Sites web page in WEBconfig, the value for the Max Price Per Job could be less than the value of the Price Per Page, which was incorrect.

Cause

Works as designed.

Resolution

In the sites.asp page, client-side validation has been added to verify that the value for the Max Price Per Job is greater than the value of the Price Per Page. If an incorrect value is entered, a warning message appears. The user cannot submit to the next page until the Max Price Per Job is greater than the Price Per page.

CSCdv37289**Synopsis**

The Mega page set credit card options were dependent on the old credit card billing server, IPORT Central Management System (CMS). Since this option is no longer being used, it had to be replaced with the Internet Commerce Suite (ICS) credit card billing option.

Cause

CMS is no longer a desirable option.

Resolution

Exchanged all references to CMS with ICS and updated the accounting information within the active server pages (ASP) for both Mega and the new MegaClear Page sets.

CSCdv40107**Synopsis**

When multiple router records existed, clients connecting through any router other than router 0 displayed the bandwidth selection option on the start page when the Bandwidth Manager feature was deactivated from the Servers web page in WEBconfig.

Cause

In previous releases of BBSM, Bandwidth Manager was set on a per-router basis. This feature is now set server-wide. Consequently, when the administrator enabled or disabled the Bandwidth Manager option from the Servers web page, only the record for router 0 was modified to reflect the configuration change.

When determining whether to display the bandwidth selection option in the start page, Atnotify looks at the specific router entry for the connecting client. If the administrator disabled Bandwidth Manager and a client was connecting through router 1, the check for the Bandwidth Manager feature that was performed by Atnotify incorrectly returned an enabled state. This caused the start page for the end user to incorrectly display the bandwidth selection option when Bandwidth Manager was disabled for the server.

Resolution

The NotifyBilling::GetManageBandwidth method has been modified to always look at the router 0 record when determining whether the bandwidth management feature is enabled or disabled.

CSCdv50031**Synopsis**

Simple Mail Transfer Protocol (SMTP) forwarding failed to redirect SMTP packets.

Cause

SMTP forwarding logic in BBSM was not functional.

Resolution

This problem has been resolved by correcting SMTP forwarding logic.

CSCdv55815**Synopsis**

The MEGA page set, which is a popular page set for trade shows and for subject matter experts doing demonstrations, had the Secure Sockets Layer (SSL) set for RADIUS and Credit Card.

Cause

Since BBSM does not have a SSL certificate installed, a MEGAClear page that does not require SSL was needed.

Resolution

A new MegaClear page set that does not require SSL has been created. The MegaClear page set user interface has RADIUSClear, AccessCode, Minute, Block, and Daily access policies for end users to choose from.

CSCdv56823**Synopsis**

A building was modified from a hotel to an office building with an enterprise LAN environment. This BBSM configuration has a large number of switches and a large base of users. When BBSM activates from 130 to 200-plus sessions, subsequent (but not all) connection attempts were delayed but are now redirected to the Connect screen. After 5 to 15 minutes, the initial request is processed, and users can access the Internet.

Cause

The server did not allow new user sessions to authenticate during the BBSM switch port status checks. On networks with a large switch fabric, this check can take some time. Consequently, BBSM determines where the clients are but does not finish the authentication process until the BBSM switch port status checks are finished.

Resolution

Code changes now interleave the connection process with the switch port status checks, which prevents the status checks from delaying the connection process.

CSCdv58101

Synopsis

When running the SwitchDiscovery.exe program, there was no warning message to inform the user that the existing port map would be wiped out once they clicked the Finish button. This caused some users to unintentionally wipe out their existing port map.

Cause

Warning contents were missing.

Resolution

On the SwitchDiscovery.exe program, a new warning message has been added that informs users that their existing port map will be wiped out when they click the Finish button.

CSCdv61553

Synopsis

From the Port Map web page in WEBconfig, the following error message sometimes appeared when the user unchecked the Clear Existing Port Map check box and then clicked the Generate button: *port map failed site n stack n*.

Cause

The logic for port mapping returns a false value if no new portmap is added. When the Clear Existing Port Map check box was unchecked, no new portmap was added to the first switch. Consequently, the port mapping logic returned a false value and caused an early exit even when there were more switches to portmap.

Resolution

The port mapping logic has been modified to return the correct status for AddPortMap().

CSCdv63341

Synopsis

When a connected client disconnected and then clicked the Back button on the browser to go back to the start page to enter and submit required data, BBSM continually sent the client back to the start page every time the client tried to reconnect. The active session count continued to increment, and the max active session was maximized even though the client was no longer connected.

Cause

BBSM detected that the client did not go through the pre-connect page and would not activate the session. BBSM redirected the client to the start page, but incremented the active session count. Eventually, this caused the active session count to reach the maximum number of active sessions that were set on the Server tab in WEBconfig.

Resolution

The BBSM code has been changed. The active session count is incremented only after BBSM successfully verifies that the client has gone through the pre-connect process. If the client did not go through this process, the active session count will not be incremented.

CSCdv65695

Synopsis

Not all 2950 series switches work successfully with switch discovery.

Cause

The 295024c and 295012 SysObjectIds were missing from the GenericSwitch (switches.reg) file.

Resolution

Two new switches have been added to the switches.reg file.

CSCdv66549

Synopsis

When there is a multiple stack configuration, the PortTest incorrectly assumed that it reached the end of the port map in the database.

Cause

The software did not test to see if it reached the end of the portmap for a specific portID (stack number) in the PortTests.cpp web page.

Resolution

The code in the PortTests.cpp and PortTests.asp pages has been modified to correct this problem.

CSCdv68179

Synopsis

In the WEBpatch application, the Browse button did not function if the client was using Microsoft Internet Explorer 5.5 or 6.0. This problem exists in both BBSM 5.0 and 5.1.

Cause

The FileUpload textbox used to transfer the file from the client's machine to the BBSM Server initially used a Read-only attribute to ensure that the user could not enter a fictitious file name and then try to upload it. However, it was discovered that the Read-only attribute is not supported for the FileUpload HTML tag. This caused the Browse button to be disabled and unusable in Internet Explorer 5.5 or 6.0.

Resolution

The Read-only attribute has been removed from the FileUpload HTML tag and replaced with two new Client-Side JavaScript functions. The two new functions now ensure that no keyboard entry is allowed in the FileUpload text box and that no right mouse clicks are allowed. Consequently, the user cannot paste a path. The user is now forced to click the Browse button and search for a valid executable file.

CSCdv81850

Synopsis

BBSM Secure Sockets Layer (SSL) page sets do not work correctly with SSL certificates issued by major certificate authorities (CA) such as Verisign.

Cause

Currently, BBSM SSL page sets only work correctly if the BBSM Server SSL certificate has an IP address for the server name in the certificate. Established certificate authorities, such as Verisign and Thawte, will only issue SSL server certificates for servers defined by DNS or LAN name. Therefore, SSL page sets do not work with real-world SSL server certificates.

Resolution

BBSM has been modified so that it can be configured to use the BBSM Server's DNS name instead of the internal NIC IP address in the hostname of page set URLs.

CSCdw01040**Synopsis**

During the BBSM installation, the Microsoft Internet Security and Acceleration Server (ISA) Web Proxy Service leaves web proxy logging enabled. With logging enabled, the proxy service can consume all disk space or virtual memory causing a system failure.

Cause

See the following Microsoft support URL:
<http://support.microsoft.com/support/kb/articles/Q305/7/12.ASP>

Resolution

A script is run that disables web proxy logging.

CSCdw10159**Synopsis**

The Room Mappings Report would give a user a divide-by-zero error when a port test was done and zero packets were sent.

Cause

The Room Mappings Report does the calculations for the pass-fail packet loss column in the SQL statement on the Reporting page. There was no divide-by-zero error check in place to catch this error if zero packets were transmitted.

Resolution

Error-checking code has been added to the Reporting page to check for a divide-by-zero error. If the packets transmitted are equal to zero, the page now returns a light blue box in the Pass or Fail column that says *Redo Port Test*. The Packet Loss column is empty, which alerts the user to redo the port test for that individual port.

CSCdw10938**Synopsis**

The SwitchDiscovery failed for Cisco 2948 switches.

Cause

There were three versions of Cisco 2948 switches, but only one of them, Cisco 2948gL3, could be discovered. Also, the Cisco 2948G has a different internal Management Information Base (MIB) port map. There was no port map logic for this switch.

Resolution

The switches.reg file has been modified to include all three switch types. The two new switch types are the Cisco 2948gL3DC and the Cisco 2948g. The Cisco2948 class has been added to the CiscoSwitch.dll that maps the MIB port correctly. The switches.reg file has also been modified to include *CreateStack = CreateCisco2948*.

CSCdw18623

Synopsis

A BBSM 5.1 Server with SP1 installed was configured with one site, 54 network elements, and 5800 ports (dhcp, foreign, and management). After running with no active clients for 6 to 8 hours, the server exhibited the following:

- Client browsers started timing out during yanking, or they were redirected to the error page.
- Attempts at viewing WEB reports on the server yielded *minimum query memory not available* errors.
- WEBconfig displayed garbage data or timed-out with a *max amount of time for a script to execute was exceeded* error message.
- Task Manager showed that CPU utilization is maximized by atdial.exe, sqlservr.exe, and LSASS.exe.

Restarting sqlservr along with atdial and msmq fixed the server (reports and client requests work). However, atdial, sqlservr, and LSASS quickly utilized close to 100% of the central processing unit (CPU). When sqlservr, atdial, and msmq are restarted, there is an initial spike in CPU utilization (30 seconds or so as atdial initializes) after which the system idle process shows 99% CPU time for exactly one minute. Consequently, 99 to 100% of CPU time was consumed by sqlservr, atdial, and LSASS.

Cause

Atdial creates a portinfo object for each entry in the port_state table. All portinfo objects are checked once-per-minute to see if clients are still connected, if sessions expire, etc. During each portinfo check, atdial performs a read from the server_configuration table to ensure that the portinfo object did not use outdated information.

For a debug server with 20 class C's (roughly 5100 ports), the server_configuration table reads were taking over two minutes for all portinfo objects. When atdial finishes checking the last portinfo object, it tests to see if one minute has elapsed since checking the first portinfo object. If so, it will start the portinfo check cycle again. In the case where it takes longer than 60 seconds to check all portinfo objects, atdial effectively never rests.

Consequently, msde was not able to handle the constant read requests, which was the main cause of this problem. Atdial was also performing this check for inactive as well as active ports. Atdial needs to pause between each portinfo check cycle.

Resolution

The outdated server_configuration check logic has been removed. When checking portinfo objects, atdial will skip ahead to the next active port so that messages are not posted and checks are not performed for inactive ports. Atdial always allows the ontimer function to invoke portinfo check cycles to avoid the constant barraging of the server.

CSCdw23310

Synopsis

The No MAC feature could fail if the system contained more than one client. An indication of this is when the active port report shows more than one active port while atnاتمcmd reports only one active report.

Cause

The client search algorithm incorrectly updated the port state table without sending an activate session request.

Resolution

The client search algorithm has been modified to prevent it from erroneously changing the port state table.

CSCdw27755

Synopsis

The new partially managed 4-port Long Reach Ethernet (LRE) customer premises equipment (CPE) device does not support link status on the four individual Ethernet ports. Therefore, the Cisco 2912 LRE and Cisco 2924 LRE switch DLLs did not support the 4-port CPE.

Cause

The new CPE hardware is not fully manageable and did not provide link status on individual ports.

Resolution

Two new switch DLLs have been created to support partially managed multi-port LRE CPEs. The Cisco 2912 LRE MultiPort CPE and Cisco 2924 LRE MultiPort CPE are now available switch types. These new DLLs use 2-way packet activity to timeout a client. The packet inactivity period is configured on the Switches web page in WEBconfig.



Note If a combination of one-port and 4-port CPEs is used on a 2912/2924 LRE switch, then all client status will be detected using packet activity. If only one-port CPEs are used on a LRE switch, then use the Cisco 2912 LRE or Cisco 2924 LRE switch type, which uses link status to detect client status.



Note There are known limitations with using 2-way packet activity to detect client status. If a client unplugs the Ethernet cable or shuts down to disconnect, there are situations where IP traffic can still be going to the client. In this case, the sessions do not timeout until the traffic stops.

CSCdw29582

Synopsis

A large telephone company wanted to deploy BBSM in hotels using Cisco 2924 LRE switches. They also wanted to put hubs in the rooms between the clients and the CPE devices. In this configuration, the current 2924 LRE switch dll never detected when the client was physically disconnected because the port's link status always showed connected status due to the hub being connected. The customer requested that Cisco provide a modified version of the 2924 LRE switch dll that detects client-connected status by pinging the client.

Cause

The existing 2924 LRE switch support in BBSM uses link status to determine if the client is physically connected.

Resolution

A new switch option, Cisco 2924 LRE Ping, has been added to the ciscoswitch dll and to the Switches web page in WEBconfig. This option pings the client to determine whether it is physically connected.

Installation

Use the WEBpatch option in BBSM to install BBSM 5.1 SP2, also known as BBSM51SP2.exe.



Caution

You *must* first use the WEBpatch option in BBSM to install the WEBpatch patch, also known as WEBPatch51SP1.exe, on the BBSM Server before you install BBSM 5.1 SP2. You must also install BBSM 5.1 SP1 before you install BBSM 5.1 SP2.



Note

A memory exception window might momentarily appear at the beginning of the reboot process. This exception does not affect the functionality of your BBSM Server, and you will not see this error message again during subsequent patch installations.



Note

The *Cisco Building Broadband Service Manager WEBpatch User Guide* provides instructions to install, transfer, and remove BBSM service packs (or patches).

Related Documentation

The following documents provide additional information:

- The *Cisco Building Broadband Service Manager WEBpatch User Guide* provides instructions to install, transfer, and remove BBSM service packs (or patches).
- The *Cisco Building Broadband Service Manager Hardware Assembly Guide* provides instructions for connecting your BBSM Server.
- The *Cisco Building Broadband Service Manager Quick Start Card/CD Sleeve* provides information on how to access documentation on the BBSM v5.1 CD for installing and configuring BBSM.
- The *Cisco Building Broadband Service Manager and Director Installation Guide* provides instructions (if your system is customer-installed) for installing BBSM software.
- The *Requires Immediate Attention Card for Cisco BBSM Server* provides instructions for changing passwords and accessing documentation on the BBSM v5.1 CD.
- The *Cisco Building Broadband Service Manager Software Configuration Guide* provides instructions for configuring BBSM software.
- The *Cisco Building Broadband Service Director Software Configuration Guide* provides instructions for configuring Cisco Building Broadband Service Director (BBSD) software.

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

<http://www.cisco.com>

Translated documentation is available at the following URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

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

All customers, partners, and re-sellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

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

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, FrameShare, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, ScriptBuilder, ScriptShare, SMARTnet, TransPath, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and Discover All That’s Possible are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0110R)

Copyright © 2002, Cisco Systems, Inc.
All rights reserved.