



Release Notes for Device Fault Manager 2.0 on Windows

Revised: 5 July 2005

These release notes are for use with Device Fault Manager (DFM) 2.0 running on a Windows platform. Supported Windows versions are Windows 2000 (Professional, Server, and Advanced Server) with Service Pack 3 or 4, and Windows 2003 Server and Enterprise Edition.

New features in DFM 2.0 are described in the *User Guide for Device Fault Manager* (see [Product Documentation, page 2](#)). DFM 2.0 contains the device support provided by DFM 1.2 Patch/IDU 1.2.8. DFM 2.0 Incremental Device Updates (IDUs) and service packs can be downloaded from Cisco.com as they become available (refer to [Additional Information Online, page 5](#)).

These release notes provide:

- [Product Documentation, page 2](#)
- [Related Documentation, page 3](#)
- [Additional Information Online, page 5](#)
- [DFM 2.0 Upgrade Kit on Cisco.com, page 5](#)
- [Known and Resolved Problems, page 6](#)



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

Copyright © 2004-2005 Cisco Systems, Inc. All rights reserved.

- [Obtaining Documentation](#), page 22
- [Documentation Feedback](#), page 23
- [Obtaining Technical Assistance](#), page 23
- [Obtaining Additional Publications and Information](#), page 26

Product Documentation



Note

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

[Table 1](#) describes the product documentation that is available.

Table 1 Product Documentation

| Document Title | Available Formats |
|---|--|
| <i>Quick Start Guide for LAN Management Solution 2.5</i> | <ul style="list-style-type: none"> • Printed document that was included with LMS 2.5. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/lms/index.htm |
| <i>Release Notes for Device Fault Manager 2.0 on Windows</i> | <ul style="list-style-type: none"> • Printed document that was included with the product. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm20/relnotes/index.htm |
| <i>Installation and Configuration Guide for Device Fault Manager on Windows</i> | <ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm20/install/windows/index.htm • Printed document available by order (part number DOC-7816272=).¹ |

Table 1 Product Documentation (Continued)

| Document Title | Available Formats |
|---|--|
| <i>Installation and Configuration Guide for Device Fault Manager on Solaris</i> | <ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm20/install/solaris/index.htm Printed document available by order (part number DOC-7816268=).¹ |
| <i>User Guide for Device Fault Manager</i> | <ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dfm20/ug/index.htm Printed document available by order (part number DOC-7816266=).¹ |
| <i>Supported Devices for Device Fault Manager 2.0</i> | On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev_sup/dfm2_0.htm |
| <i>Status of DFM Device Agent Bugs (DFM 1.x and DFM 2.x)</i> | On Cisco.com at this URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev_sup/index.htm |
| Context-sensitive online help | <ul style="list-style-type: none"> Select an option from the navigation tree, then click Help. Click the Help button in the dialog box. |

1. See [Obtaining Documentation](#), page 22.

Related Documentation



Note

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

[Table 2](#) describes the additional documentation that is available.

Table 2 *Related Documentation*

| Document Title | Description and Available Formats |
|---|---|
| <p><i>Release Notes for CiscoWorks Common Services 3.0 (Includes CiscoView) on Windows</i></p> | <p>Describes Common Services 3.0 resolved and known problems. This document is available in the following formats:</p> <ul style="list-style-type: none"> • Printed document that was included with the product. • On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser30/index.htm |
| <p><i>Installation and Setup Guide for CiscoWorks Common Services (Includes CiscoView) on Windows</i></p> | <p>Describes installing and preparing to use Common Services 3.0 on Windows. This document is available in the following formats:</p> <ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser30/index.htm • Printed document available by order (part number DOC-7816497=). |
| <p><i>User Guide for CiscoWorks Common Services</i></p> | <p>Describes CiscoWorks Common Services, gives an overview of the applications that make up Common Services 3.0 and provides conceptual information about network management. This document is available in the following formats:</p> <ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser30/index.htm • Printed document available by order (part number DOC-7816398=) |

Additional Information Online

**Note**

We have adopted a new system for naming and numbering our patch/IDUs. For all releases after DFM 2.0 Patch/IDU 2.0.1, we will use the following conventions: *Patch/IDUs* will be called *Service Packs*, and instead of version *x.y.z*, it will be called version *z*. For example, instead of DFM 2.0 Patch/IDU 2.0.2, a release would be called DFM 2.0 Service Pack 2.

Incremental Device Updates (IDUs) or service packs contain updated files necessary for the latest device support and fixes to known problems that are not available in DFM 2.0. If you are a registered user, you can download IDUs/service packs for DFM from:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>

To determine which packages are installed on your CiscoWorks Server, from the Common Services home page, select **Software Center > Software Updates**.

You can also obtain any published patches from the download site.

DFM 2.0 Upgrade Kit on Cisco.com

A DFM 2.0 Upgrade Kit is available from Cisco.com. The Upgrade Kit is a collection of files needed by DFM 1.2.x users who wish to upgrade to DFM 2.0, but cannot use the standard upgrade procedure documented in the installation guides because:

- They plan to uninstall DFM 1.2.x (and all CiscoWorks applications) on a machine, and then install DFM 2.0 and CiscoWorks applications on the same machine, and/or
- They do not have a current installation of DFM 1.2.x.

The Upgrade Kit provides a script that saves the following data (which is not saved using the standard remote upgrade procedure documented in the installation guides):

- Device list—The migration procedure adds devices to Common Services Device and Credentials Repository and to DFM.
- Device managed state (managed or unmanaged).

- Some polling and threshold setting (refer to the installation guides for more information).

To use the Upgrade Kit, you must have a copy of the DFM 1.2.x DFM.rps (inventory) file. The Upgrade Kit is available from the DFM download page at <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>

Known and Resolved Problems

Table 4 describes problems known to exist in this release; Table 4 describes problems resolved since the last release of DFM.

For information on DFM bugs that result from device bugs, see *Status of DFM Device Agent Bugs* at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev_sup/index.htm.



Note

To obtain more information about known problems, access the Cisco Software Bug Toolkit at <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. (You will be prompted to log into Cisco.com.)

Table 3 Known Problems in DFM 2.0

| Bug ID | Summary | Additional Information |
|------------|---|--|
| CSCsa80715 | Notification Services hangs after 2 weeks | <p>Trap recipients do not receive traps from Notification Services; also, there is no response when you click a link on the Notification Services tab. This happens after the NOSServer process has been running continuously for about two weeks.</p> <p>The workaround is to stop and restart the NOSServer process weekly. From the CiscoWorks home page, select Server > Admin > Process; the Process page opens. For more information, click Help in the upper right hand corner of the Process page.</p> |

Table 3 Known Problems in DFM 2.0 (Continued)

| Bug ID | Summary | Additional Information |
|------------|---|---|
| CSCsa97047 | Remote upgrade completion message unclear | <p>When performing a remote upgrade using the DFMRestore.pl command from the Upgrade Kit, the upgrade appears to fail due to a problem with DM Broker:</p> <pre>dmquit: Cannot attach DM 'DFM': Domain Manager is not registered with the DM Broker Stopped DFM. Shutdown in process.....done! Shutdown of InCharge Broker at 'localhost:426' completed. Stopped Broker. >>> Exported files ICseed.txt, ICinventory.txt and ICptm.xml are located at /opt/CSCOpX/objects/smarts/conf >>> To complete this upgrade, run the /opt/CSCOpX/bin/DFM12x-DFM20-upgrade.pl after starting DFM2.0</pre> <p>The exported files are not actually created. This problem occurs when incorrect input has been provided to the DFMRestore.pl command.</p> <p>The workaround is to:</p> <ol style="list-style-type: none"> 1. Verify that the input path names to the DFMRestore.pl command are correct and that your copy of the DFM 1.2x DFM.rps file is in the location that you specified. 2. Run the DFMRestore.pl command again. |
| CSCsa97839 | Fatal errors migrating polling/threshold data | <p>Fatal errors are sometimes displayed while running the DFM12x-DFM20-upgrade.pl command and migrating polling and threshold data. This seems to occur after migrating Resource Manager Essentials data. If you look in the ptm.log file, you see an error in connection between the PTMServer process and the DFM Object Grouping Service Server (DFMOGSServer).</p> <p>The workaround is to re-enter the polling and thresholds settings.</p> |

Table 3 Known Problems in DFM 2.0 (Continued)

| Bug ID | Summary | Additional Information |
|------------|---|---|
| CSCsa97928 | Email and trap notifier data migrated but not displayed | <p>Although the email and trap notifier data is migrated from DFM 1.2.x to DFM 2.0, it is not displayed by DFM 2.0. This is because in the <i>NMSROOT/object/nos/config/nos.properties</i> file, TRAP_DEFAULT_FILE and EMAIL_DEFAULT_FILE are not defined.</p> <p>The workaround is to edit the nos.properties file (located in the <i>NMSROOT/object/nos/config</i> directory) and add the following two lines:</p> <pre>TRAP_DEFAULT_FILE=objects\smarts\conf\notifier\trap_notify.conf EMAIL_DEFAULT_FILE=objects\smarts\conf\notifier\mail_notify.conf</pre> |
| CSCsa91950 | restorebackup.pl displays incorrect instructions | <p>If you want to perform a remote upgrade to DFM 2.0 and you attempt to do so by running the restorebackup.pl command, the command displays upgrade instructions that are not up-to-date and not correct. If you use those instructions, some data does not get migrated.</p> <p>The workaround is to ignore the messages displayed by restorebackup.pl and perform a remote upgrade from DFM 1.2.x to DFM 2.0, as follows:</p> <ol style="list-style-type: none"> 1. Download the DFM 2.0 Upgrade Kit and Readme file for the DFM 2.0 Upgrade Kit. 2. Follow the instructions in the readme file for the DFM 2.0 Upgrade Kit. |
| CSCsa50868 | Device takes too long to move to Known state | <p>DFM sometimes requires up to 30 minutes to move a device from Learning to Known. This is due to the synchronization issues between two processes. This problem has been fixed in DFM 2.0 Patch/IDU 2.0.1 (or later), available on Cisco.com (see Additional Information Online, page 5).</p> |

Table 3 Known Problems in DFM 2.0 (Continued)

| Bug ID | Summary | Additional Information |
|------------|---|---|
| CSCsa50314 | DFM group administration windows should not show Common Services groups | DFM Group Administration allows users to create groups that contain Common Services groups, but users cannot perform any actions on those groups. The Common Services groups should therefore not be listed. This is due to a Common Services problem. A bug against Common Services has been opened (CSCsa50290). There is no workaround. |
| CSCef60937 | Fault History and Notification Services do not list groups from other LMS applications | In the Fault History and Notification Services windows, DFM does not display groups from other LMS applications (such as Campus Manager and Resource Manager Essentials). This is due to a Common Services problem. A bug against Common Services has been opened (CSCef59702). There is no workaround. |
| CSCsa49406 | Cannot launch drop-down tools from Alerts and Activities Detail page | When a remote instance of Cisco View or Campus Manager is registered with the CiscoWorks home page, and local versions of those applications are already registered, CiscoWorks cannot launch tools from the Alert and Activities Detail drop-down list. This is because CiscoWorks tries to open the remote link rather than the local link. This problem has been fixed in DFM 2.0 Patch/IDU 2.0.1 (or later), available on Cisco.com (see Additional Information Online, page 5). |
| CSCsa48916 | Alerts and Activities Detail page only refreshes events when they are cleared or they recur | The Alerts and Activities Detail page only refreshes event status when the event is cleared or when the event surpasses a threshold. If the event already surpassed the threshold, it is not refreshed if the value (still above the threshold) changes again. There is no workaround. |

Table 3 Known Problems in DFM 2.0 (Continued)

| Bug ID | Summary | Additional Information |
|------------|--|---|
| CSCsa45329 | DFM hogs CPU when DCR contains more than 5,000 devices | When the DCR contains more than 5,000 devices, the DFMOGSServer may hog CPU cycles due to processing issues. The CPU hogging may occur for four hours or more. This problem is less noticeable in dual CPU machines. This problem has been fixed in DFM 2.0 Patch/IDU 2.0.1 (or later), available on Cisco.com (see Additional Information Online, page 5). |
| CSCeg34129 | Sybase database error causes occasional lag in SNMP and e-mail notification delivery | A Sybase problem occasionally causes Notification Services to delay in delivering SNMP and e-mail notifications, with a delay up to five minutes. This occurs when the Solaris server is running in a heavy load environment (for example, when 50 events are received every polling cycle, and the polling cycle is every 4 minutes). It may be observed every 30 minutes. The Sybase database error that causes this problem is being tracked through a Common Services 3.0 defect (CSCef37746). There is currently no workaround. |
| CSCsa47936 | Alerts and Activities Detail tools fail if SSL is enabled on DFM server | If SSL is enabled on the DFM server, any of the tools that are launched from the Tools drop-down list (on the Alerts and Activities Detail page) will fail. This is because the tools path is hard-coded to http, and if SSL is enabled, the proper path is https. This problem has been fixed in DFM 2.0 Service Pack 2 (or later), available on Cisco.com (see Additional Information Online, page 5). |
| CSCsa45235 | Port analysis is provided even when analysis is disabled | If a port is connected to a layer 3 device (a router) and a user then disables analysis on the port, DFM will continue to analyze the port. This is due to an internal engine issue. This problem has been fixed in DFM 2.0 Patch/IDU 2.0.1 (or later), available on Cisco.com (see Additional Information Online, page 5). |

Table 3 Known Problems in DFM 2.0 (Continued)

| Bug ID | Summary | Additional Information |
|------------|---|---|
| CSCsa45801 | DFM reports interface OperationallyDown events even when analysis is disabled | If a user disables all interface/port analysis (using the Disable All Threshold Settings check box), DFM may continue to provide interface fault information. This is because DFM applies Reachability settings after applying Connector port and interface settings. This problem has been fixed in DFM 2.0 Patch/IDU 2.0.1 (or later), available on Cisco.com (see Additional Information Online, page 5). |
| CSCsa50045 | Memory ExcessiveFragmentation event not generated for some switches | By default, DFM generates memory ExcessiveFragmentation events for routers. For switches, the event is generated only when the enableFragmentAnanalysis flag is set to true. In DFM 1.2.x, users could enable this flag using the UI, but there is no mechanism to do this in DFM 2.0. There is no workaround. |
| CSCsa61612 | Need UI for bulk unmanage | DFM needs a function for performing bulk manage and unmanage operations, so that access ports (and other components) can be easily managed or unmanaged. The workaround is to manually manage or unmanage each component. |
| CSCsa49793 | Need popup message to remind user when to select Apply Changes | When a device or device component is resumed (or managed) after being suspended (or unmanaged), users must select Configuration > Apply Changes to resume polling. Although this is explained in the documentation, DFM should also display a popup message that reminds users to do this. |
| CSCsa49933 | Broken help links in Group Administration | In the Group Administration windows, some of the Help links were broken. This problem has been fixed in DFM 2.0 Patch/IDU 2.0.1 (or later), available on Cisco.com (see Additional Information Online, page 5). |

Table 3 Known Problems in DFM 2.0 (Continued)

| Bug ID | Summary | Additional Information |
|------------|---|--|
| CSCsa98634 | Windows: sm_nv_fwd process does not run after DFM 2.0 is installed | The sm_nv_fwd process is not running after installing DFM 2.0 on a Windows machine with Netview 7.1. The process won't start even if tried manually. There is no workaround. |
| CSCsa98010 | sm_ov_fwd process does not run after remote HPOV-NetView adapters are installed | After installing HPOV-NetView adapters on a remote host, error messages indicate that sm_ov_fwd is not running. Trying to start sm_ov_fwd manually does not work. There is no workaround. |
| CSCsa97997 | Windows: DOS window for sm_authority.exe opens on starting HP OpenView | Whenever you start HP OpenView on a system with DFM 2.0, a DOS window opens for sm_authority.exe. This happens when you install HP OpenView before installing DFM 2.0. Either leave the window open or minimize it. |
| CSCsa97721 | 120 dpi font resolution renders Alerts & Activities Display unreadable | Setting font resolution to 120 dpi on a high resolution monitor renders the Alerts and Activities Display unreadable. To work around this problem, select the default font and resolution settings for monitors. |
| CSCsa96361 | Device Update shows Device Fault Manager entry after DFM is uninstalled | After you uninstall DFM 2.0, DFM information is still displayed on the following Common Services windows: <ul style="list-style-type: none"> • Device Update • Licensing There is no workaround. |
| CSCsb06324 | "No disk" message during remote DFM migration | When migrating DFM 1.2.x data to DFM 2.0, after the user has performed all required steps (validated the installation and used the necessary scripts), DFM prompts the user to install a disk. This is an erroneous message. Ignore the message and click Continue , and the installation will proceed successfully. |

Table 3 Known Problems in DFM 2.0 (Continued)

| Bug ID | Summary | Additional Information |
|------------|--|---|
| CSCsa59632 | Uninstalling DFM does not remove all directories and files on Solaris and Windows | <p>When DFM is uninstalled, the <i>NMSROOT/log/dfmdb</i> directory is not deleted. In addition, the following files and parent directory are not removed:</p> <pre> NMSROOT/log/conf/aad.logConf NMSROOT/log/conf/ddv.logConf NMSROOT/log/conf/pm.logConf NMSROOT/log/conf/vgm.logConf NMSROOT/log/conf/adapters.logConf NMSROOT/log/conf/license.logConf </pre> <p>The workaround is to manually delete the directories and files.</p> |
| CSCsa90438 | Windows/Netscape 7.1: Alerts and Activities Detail drop-down tools will not launch | <p>For Windows clients using Netscape 7.1, if a user tries to launch any of the drop-down tools from the Alerts and Activities Details page, the tools are not launched.</p> <p>The workaround is to launch these tools from other CiscoWorks windows.</p> |
| CSCsa89419 | Netscape 7.1/Mozilla 1.7.1 on Windows: AAD and DDV resizing problem | For Windows clients using Netscape 7.1 or Mozilla 1.7.1, if a user reduces the size of either the Alerts and Activities Detail page or the Detailed Device View, the window will not expand to its original size. There is no workaround. |
| CSCin86753 | Issue regarding Duplicate IP address | When different IP addresses belonging to the same device are added as separate devices, due to a timing issue, they are discovered and listed as separate devices. This is incorrect and causes invalid DuplicateIP alarms. There is no workaround. |

Table 3 Known Problems in DFM 2.0 (Continued)

| Bug ID | Summary | Additional Information |
|------------|---|--|
| CSCsa55788 | DDV does not display other IP address for WLSE | <p>When the user adds a WLSE to DFM, and the WLSE is part of a redundant group of WLSEs, the DFM Detailed Device View does not show the other members of the redundancy group.</p> <p>The workaround is to log onto the WLSE device and check for the other members of the redundancy group (by selecting Admin > Appliances > Redundancy on the WLSE).</p> |
| CSCin86752 | DFM does not discover 4604 Access Gateway card in Catalyst 4506 | <p>DFM 2.x did not discover 4604 Access Gateway cards in Catalyst 4506 switches. This was because the Catalyst 4506 supports the CISCO-ENTITY-FRU-CONTROL-MIB, which did not have an entry that contains the IP address of the module. Catalyst 4000 switches did not have this problem because those switches supported the CISCO-STACK-MIB, which does have the appropriate entry.</p> <p>The parent switch and card are also discovered correctly in DFM 2.0. However, no card details are displayed in the Detailed Device View. There is no workaround.</p> |
| CSCsa56586 | Windows: Error when dfmimport used to import seedfile | <p>When a user tries to import a seed file using the dfmimport utility on Windows, they may see the following error message:</p> <pre>log4j:ERROR Could not connect to remote log4j server at [localhost]. We will try again later.</pre> <p>This message is spurious and should be ignored. The import will proceed.</p> |

Table 4 describes problems resolved since the last release of DFM.

Table 4 Resolved Problems in DFM 2.0

| Bug ID | Summary | Explanation |
|------------|--|---|
| CSCdx32239 | Incorrect duplexity shown for router and switch interfaces and ports | <p>DFM did not always report correct duplexity for router and switch interfaces. One reason this happened was because of assumptions DFM made when port or interface duplexity was UNSPECIFIED. DFM now uses DuplexMode to specify the duplexity (UNSPECIFIED, by default) and DuplexSource to track the source of setting duplexity (NONE by default). DFM now uses this new algorithm to determine duplexity:</p> <ol style="list-style-type: none"> 1. DFM checks the portDuplexity MIB attribute in the CISCO-STACK-MIB, and: <ol style="list-style-type: none"> a. If the value is set to either half duplex or full duplex, DFM uses that setting for DuplexMode and sets DuplexSource to ENTERPRISE_MIB. b. If the device is not a Cisco stack switch, the portDuplexity attribute is not present, or the portDuplexity attribute is present but its value is auto/disagree, DFM proceeds to Step 2. 2. DFM checks the dot3StatsDuplexStatus MIB attribute in the ETHERLIKE-MIB, and: <ol style="list-style-type: none"> a. If the value is set to either half duplex or full duplex, DFM uses that setting for DuplexMode and sets DuplexSource to ETHERLIKE_MIB. b. If the dot3StatsDuplexStatus attribute is not present, or it is present but its value is unknown, DFM proceeds to Step 3. <p>(continued)</p> |

Table 4 Resolved Problems in DFM 2.0 (Continued)

| Bug ID | Summary | Explanation |
|---------------------------|---|--|
| CSCdx32239 (continued) | Incorrect duplexity shown for router and switch ifs and ports | <p>3. DFM checks the <code>cdpCacheDuplex</code> MIB attribute in the CISCO-CDP-MIB, and:</p> <ul style="list-style-type: none"> a. If the value is set to either half duplex or full duplex, DFM uses that setting for <code>DuplexMode</code> (for both local and remote ports), and sets <code>DuplexSource</code> to <code>NEIGHBOR_MIB</code>. b. If the value is unknown, DFM proceeds to Step 4. <p>4. If DFM cannot correctly determine the duplex mode (because it was not set manually or set by MIBs), DFM will set <code>DuplexSource</code> to <code>ASSUMED</code> and do the following:</p> <ul style="list-style-type: none"> a. If the interface is a 10 MB Ethernet interface, DFM will assume the setting is half duplex. (DFM considers an interface to be a 10 MB Ethernet when its <code>Type="*ETHER*"</code> and its <code>MaxSpeed=10000000</code>.) b. For all other interfaces, DFM will assume the setting is full duplex. |
| CSCed27739 | DFM manages MPLS logical interfaces, causing duplicate alarms | <p>DFM generated duplicate alarms for Multiprotocol Label Switching (MPLS) interfaces. This occurred because DFM managed logical interfaces, and MPLS logical interfaces have a separate <code>ifIndex</code>.</p> <p>Logical interfaces with <code>ifType:166</code> (MPLS) are now unmanaged by default.</p> |

Table 4 Resolved Problems in DFM 2.0 (Continued)

| Bug ID | Summary | Explanation |
|------------|---|---|
| CSCsa03104 | DFM uses wrong OID to poll CPU utilization on PIX | <p>DFM did not report CPU utilization for PIX Firewalls because the algorithm used by DFM created the proper instrumentation when:</p> <ul style="list-style-type: none"> • cpmCPUTotalPhysicalIndex was nonzero, or • The OLD-CISCO-CPU-MIB was supported. <p>For PIX Firewalls, cpmCPUTotalPhysicalIndex is always 0, and PIX Firewalls do not support OLD-CISCO-CPU-MIB.</p> <p>DFM still polls cpmCPUTotalPhysicalIndex, but the value of cpmCPUTotalIndex is verified instead. cpmCPUTotalIndex is used as the index to make the processor.</p> |
| CSCea80669 | ovtrapd cannot start after reboot because DFM occupies port 162 | <p>If a user installed HP OpenView before DFM, HP OpenView used port 162 and DFM used port 9000. This is the correct behavior. However, if the user rebooted the device, the HP OpenView ovtrapd process could not start because DFM occupied port 162 as well as port 9000.</p> <p>Now, if DFM detects that HP OpenView or NetView is installed, DFM will only use port 9000. (However, if you want DFM to always use port 162 upon reboot—for example, if you remove HP OpenView and NetView—you can use the --privopen option to do so. Refer to the online version of <i>User Guide for Device Fault Manager</i>; see Product Documentation, page 2.)</p> |
| CSCeb12662 | Layer 3 device port/interface handling is incorrect | <p>When an IP address was assigned to a port on the Catalyst 4506 running Cisco IOS (with Sup III), DFM displayed it as both a port and an interface.</p> <p>All multilayer switch ports, to which IP addresses are assigned, are now properly modeled as interfaces.</p> |

Table 4 Resolved Problems in DFM 2.0 (Continued)

| Bug ID | Summary | Explanation |
|------------|---|--|
| CSCdx64809 | DFM should unmanage voice interfaces/ports | <p>In Cisco IOS devices running the Survivable Remote Site Telephony (SRST) feature, a VoiceEncapPeer interface (in ifTable) exists for each phone supported by SRST. These interfaces were operationally DOWN by default, since they were not being used while the local IP phones could reach their remote call manager. DFM generated an OperationallyDown event for these interfaces, which was incorrect, since this was the normal and expected state.</p> <p>DFM no longer generates an OperationallyDown event for these interfaces.</p> |
| CSCea11383 | DFM should not treat voice dial peers as regular interfaces | DFM treated dial peer interfaces as physical interfaces and was managing them. These interfaces are now not managed because DFM recognizes them (by their ifType) as voice interfaces. |
| CSCdy43753 | DFM cannot discover third power supply in Cat4000 switches | DFM could not discover the third power supply in Catalyst 4000 switches, even though the snmpwalk verified that the power supply was operational. DFM now correctly discovers the power supply. |
| CSCeb41000 | DFM should suppress flapping if device restarts | When a device restarted, all associated interfaces sent link up and link down traps. If the number of restarts exceeded the Link Trap threshold, DFM reported excessive restarts and flapping (depending on the interface type) for all associated interfaces. The flapping event is now suppressed if the device restarts. |
| CSCdz14890 | 1% error threshold is too high for critical interfaces | The minimum for the error threshold (ifInerror) in DFM was 1% of the total number of packets, which was too high for high-bandwidth interfaces (such as Gbic and other WAN interfaces). The threshold can now be changed, because DFM 2.0 adds a new ErrorTraffic threshold. Refer to the online version of <i>User Guide for Device Fault Manager</i> ; see Product Documentation, page 2 . |

Table 4 Resolved Problems in DFM 2.0 (Continued)

| Bug ID | Summary | Explanation |
|------------|--|---|
| CSCdz86886 | Cannot change PacketErrorRate threshold | The PacketErrorRate threshold could not be modified. The threshold can now be changed, because DFM 2.0 adds a new ErrorTraffic threshold. Refer to the online version of <i>User Guide for Device Fault Manager</i> ; see Product Documentation, page 2 . |
| CSCec42667 | CSS11150 and CSS11050 switches generate incorrect memory exception | On CSS11150 and CSS11050 switches, DFM generated erroneous memory exceptions because instead of monitoring only the SCFM module, it was monitoring other modules (such as the EPIF module). DFM no longer monitors any modules besides the SCFM module. |
| CSCec77687 | Filter out pass-through traps which are not related to managed devices | Whenever pass-through traps were received from unmanaged devices, they were displayed in the Monitoring Console. Pass-through traps for unmanaged devices are no longer displayed in the Monitoring Console. |
| CSCec30981 | VLAN for L3 switches not displayed | DFM did not display VLAN information for Catalyst 4500 switches that perform Layer 3 routing. DFM now displays the VLAN information. |
| CSCea30379 | DFM incorrectly reports CSS-11506 free memory | DFM reported insufficient memory alarms for the blades of some Content Switches because the cards are internal and had no memory on them. DFM will not report these errors (by unmanaging the cards) if it finds that no memory is configured in the module. This applies to modules 7 and 8 on the CSS11506 and module 4 on the CSS11503. |
| CSCdz71499 | DFM reports Catalyst 6000 IDSM blade as undiscovered | When a Catalyst 6000 with an IDSM blade was added to DFM, DFM reported the blade as Undiscovered. This error occurred because IDSM blades do not support SNMP. DFM no longer tries to discover the IDSM blade, which is shown as a card in the parent switch. |
| CSCea11379 | Memory not polled for 2948G | DFM did not poll memory components on the Catalyst 2948G. Memory components are now polled on the Catalyst 2948G. |

Table 4 Resolved Problems in DFM 2.0 (Continued)

| Bug ID | Summary | Explanation |
|---|--|--|
| CSCdw23386, CSCdy83378, CSCdv53038, CSCdw91367 | Improve ISDN modeling | These problems have been fixed through the improved ISDN interface model provided with DFM 2.0. Refer to the online version of <i>User Guide for Device Fault Manager</i> ; see Product Documentation, page 2 . |
| CSCea17909, CSCea15555 | Interfaces incorrectly displayed | <p>When a port on a device that supports both Layer 2 and Layer 3, such as a Sup card running Cisco IOS, was assigned an IP address, it was displayed in the DFM Administration Console under both interface and port. It is now displayed under interface.</p> <p>This fix also applies to the following devices:</p> <ul style="list-style-type: none"> • Catalyst C2955C-12 • Catalyst C2955T-12 • Catalyst C4506-with-Sup • Catalyst C4507-with-Sup • Catalyst C4503-with-Sup • Catalyst C3550-24-PWR • Catalyst C2955S-12 • WS-C2950ST-24-LRE |
| CSCdz09981 | DFM Name Resolution fails if devices are in different DNS domain | DFM was not using the fully qualified domain name entered in the Essentials Inventory Device Name and Domain Name fields for name resolution. This problem no longer occurs. |
| CSCdw19930 | DFM reports HSRP implementation as duplicate IP message | HSRP virtual IP addresses are no longer reported as duplicate IP addresses. |

Table 4 Resolved Problems in DFM 2.0 (Continued)

| Bug ID | Summary | Explanation |
|------------|--|---|
| CSCdx56957 | Cat IOS devices: interfaces shown in both port and interfaces | <p>After adding a Catalyst device running Cisco IOS, Gigabit Ethernet GE1/1 and GE1/2 interfaces were displayed in both the Interface and Port groups.</p> <p>This behavior occurred because when you assigned an IP address to a port on a Catalyst switch, and the Catalyst switch was running the Cisco IOS operating system, DFM created an object in both the Port and Interface classes. The object in the Interface class represented a logical entity that DFM used to maintain connectivity information.</p> <p>This behavior has been fixed. Now, when a port has an IP address assigned to it, DFM will only display it in the interface group. It will not be displayed in the ports group.</p> |
| CSCdv88878 | PPP interfaces were always classified as Backup and could not be unmanaged | DFM always classifies the PPP interfaces as Dial-on-Demand and thus generates a max-up-time event. DFM 2.0 provides a GUI feature through which users can disable interface and port analysis, thus suppressing event generation. Refer to the online version of <i>User Guide for Device Fault Manager</i> ; see Product Documentation, page 2 . |
| CSCdz49270 | DFM translates sysConfigChangeTime as date and time | <p>In sysConfigChange traps, DFM was incorrectly translating the sysConfigChangeTime, sometimes showing dates instead of a length of time since the last configuration change.</p> <p>Because there is currently no function that can map the MIB attribute SysConfigChangeTime to a time format consisting of hours/minutes/seconds, DFM will no longer display this MIB attribute in the sysConfigChange trap.</p> |
| CSCea24977 | 3725 SystemObjectID is incorrect | The SystemObjectID was incorrect for the 3725. The OID has been corrected. |

Table 4 Resolved Problems in DFM 2.0 (Continued)

| Bug ID | Summary | Explanation |
|------------|---|---|
| CSCdy27270 | DFM 1.2.1 shows false PowerSupplyException for Cat3550 | DFM displayed a power supply OperationalException for the Catalyst 3550, even though running the 'sh env all' command confirms that the power supply does not have any problems. DFM no longer displays this exception. |
| CSCdy77106 | DFM needs to add support of Layer 3 Cat4006-SUP3 (WS-X4014) | DFM did not support the Cisco Catalyst Supervisor Engine III on the Catalyst 4006. DFM 2.0 adds this support. |

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_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/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 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.

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/>
- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

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

- World-class networking training is available from Cisco. You can view current offerings at this URL:


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

This document is to be used in conjunction with the documents listed in the “Product Documentation” section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, the Cisco logo, and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, E-FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Re-MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet 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 trademarks between Cisco and any other company. (0705R)

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

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

