



Release Notes for Device Fault Manager 1.2 on Windows 2000

These release notes are for use with CiscoWorks2000 Device Fault Manager (DFM) 1.2 running on a Windows platform. The supported Windows version is Windows 2000 Professional and Server with Service Pack 1.

These release notes provide:


- [New Features, page 2](#)
- [Documentation Roadmap, page 3](#)
- [Additional Information Online, page 4](#)
- [Documentation Addendum, page 4](#)
- [Known and Resolved Problems, page 5](#)
- [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.

New Features

- All device support in the downloadable DFM 1.1 Incremental Device Support packages (available on Cisco.com) has been integrated into DFM 1.2. This includes:
 - Routers: Cisco Switching Access Concentrator MC3810-V3
 - Access Servers: Cisco Access Server AS5400, Cisco Universal Gateways AS5350 and AS5850
 - Switches:
 - Cisco Optical Network Switch ONS 15540 ESP
 - Cisco Catalyst 6513 and 6509-NEB
 - Cisco Catalyst 6000 Module Switch Feature Card WS-F6K-MSFC2
 - Cisco Catalyst 6000 Network Analysis Module WS-X6380-NAM
 - Cisco Catalyst 2980G
-
-  **Note** The DFM 1.2 device support table specifies whether DFM supports these switches running the IOS and/or the CatOS operating systems.
-
- IP Telephony Devices:
 - Voice Mail Gateway DPA7610 and DPA 7630
 - Cisco Catalyst 42000 Access Gateway Switch 4224
 - Third Party Servers: IBM Media Server x330, x340 and x342
- Bug fixes (listed in the [“Known and Resolved Problems”](#) section on page 5).

Documentation Roadmap

**Note**

Although every effort has been made to validate the accuracy of the information in the printed and electronic documentation, you should also review the Device Fault Manager documentation on Cisco.com for any updates.

The following documents are provided in PDF on your product CD:

- *User Guide for Device Fault Manager*
- *Installation Guide for Device Fault Manager on Windows 2000*
- *Installation Guide for Device Fault Manager on Solaris*

**Note**

Adobe Acrobat Reader 4.0 or later is required.

Use these publications to learn how to install and use DFM:

- *Installation Guide for Device Fault Manager on Windows 2000* (DOC-7814236=)—Provides instructions for installing DFM on a Windows 2000 system, and offers quick-start steps for using DFM. This publication is available on the CD-ROM in PDF format. The filename is dfm12_windows_install_guide.pdf.
- *Installation Guide for Device Fault Manager on Solaris* (DOC-7814237=)—Provides instructions for installing DFM on a Solaris system, and offers quick-start steps for using DFM. This publication is available on the CD-ROM in PDF format. The filename is dfm12_solaris_install_guide.pdf.
- *User Guide for Device Fault Manager* (DOC-7814235=)—Describes DFM, provides instructions for configuring, administering, and operating it, and answers DFM frequently asked questions. This publication is available on the CD-ROM in PDF format. The filename is dfm12_user_guide.pdf.

- DFM online help—Contains all of the information available in the *User Guide for Device Fault Manager*. This ensures you have complete information even if you do not have the manual readily available while using DFM.
- DFM Frequently Asked Questions—Answers common questions asked by DFM users, available from Cisco.com at:
<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/index.htm>

Use these publications to learn how to install and use CD One:

- *Release Notes for CiscoWorks2000 CD One, 5th Edition on Solaris* (DOC-78-14071-01)—Describes CD One, 5th Edition known problems, explains how CiscoWorks2000 handles time zone issues, and provides sources for additional general information.
- *Installation and Setup Guide for CD One on Solaris* (DOC-7814069=)—Describes installing and preparing to use CD One, and troubleshooting CD One installations.
- *Getting Started with the CiscoWorks2000 Server* (DOC-7814072=)—Provides an overview of the administrative functions provided by the CiscoWorks2000 Server, which is used by DFM and all CiscoWorks2000 applications.

Additional Information Online

For information about DFM supported devices, refer to the following URL, or check the documentation on Cisco.com for the correct location.

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev_sup/index.htm

Documentation Addendum

In the latest version of the *User Guide for Device Fault Manager*, Appendix A, “Device-Specific Information,” should include information explaining that for all Access Servers, serial interfaces are not managed by default. (The guide on Cisco.com does include this information.)

Known and Resolved Problems

Known problems (bugs) in DFM are graded according to severity level. These release notes contain descriptions of:

- All severity level 1 or 2 bugs.
- Significant severity level 3 bugs.
- All customer-found bugs (regardless of severity level).

You can search for problems using the Cisco bug tracking tool, Bug Navigator II. To access Bug Navigator:

-
- Step 1** Log into Cisco.com.
- Step 2** Select **Service & Support > Technical Support Help—Cisco TAC > Tool Index**.
- Step 3** In the Jump to: links at the top of the page, click the letter **S**, then select **Software Bug Toolkit**.
-

You can also access Bug Navigator by entering the following URL in your web browser: http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

[Table 1](#) describes the problems known to exist in this release; [Table 2](#) describes the problems resolved since the last release of DFM.

Table 1 DFM Known Problems

Bug ID (Severity)	Summary	Explanation
CSCdt76949 (1)	DFM occasionally reports erroneous HighUtilization events on interfaces	<p>When using DFM to view details of a HighUtilization event, the utilization shown is abnormally high (sometimes much higher than 100%).</p> <p>Fixed in the latest DFM 1.2.x IDU. To download the IDU, log in to Cisco.com and point your browser to: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm</p>
CSCsa07479 (2)	Uninstalling DFM renders VHM unusable	<p>If DFM and VHM are installed on the same Windows machine and you uninstall DFM, VHM will become unusable.</p> <p>If you have uninstalled DFM, you must do the following:</p> <ol style="list-style-type: none"> 1. Uninstall VHM. 2. Reinstall VHM, pointing the installer to a remote DFM installation.
CSCdv89796 (2)	Error when executing MailAction (com.smarts.mailexception)	<p>When sending a mail notification using the IIS 4.0 mail server running on a remote Windows machine, users may encounter errors and see this message:</p> <pre>error sending mail:com.smarts.store.SmStoreException</pre> <p>This occurs if the network is using a relay restriction access list and the user is not on the access list.</p> <p>The workaround is to have the administrator remove the access list.</p>

Table 1 DFM Known Problems (continued)

Bug ID (Severity)	Summary	Explanation
CSCdv50871 (2)	Getting duplicate IP address alarm even after the problem is fixed	<p>DFM displays duplicateIP alarms even after the problem is fixed and the duplicate IP address is no longer in the network.</p> <p>The workaround is as follows:</p> <ol style="list-style-type: none"> 1. Reconfigure your devices to use a unique IP address (making sure there are no duplicates). 2. From the Administration Console, delete the DuplicateIP object from the Inventory Browser: <ol style="list-style-type: none"> a. Right-click the object and select Browse DuplicateIP. If the DuplicateIP instance is not visible, right-click the object and select Show All. b. Expand and examine the view to locate all devices that have IPs marked as DuplicatedBy. c. Select the DuplicateIP instance and right-click Delete. d. Select the correct IP instance and right-click Rediscover. 3. Select Inventory > Reconfigure and Inventory > Save Inventory to save your changes.

Table 1 DFM Known Problems (continued)

Bug ID (Severity)	Summary	Explanation
CSCdx56993 (2)	Cat IOS devices: managed interfaces not shown under expected threshold group	<p>A switch interface/port on 355x/65xx Series devices can be configured as switch ports (L2) or as router ports (L3). DFM should to distinguish between the two scenarios and classify the instance to be a member of either of the following default groups:</p> <ul style="list-style-type: none"> • Interface group (if L3) • Access Ports group (if L2 and no trunking) • Trunk Ports group (if L2 and trunking is on) <p>There is currently no workaround. This is a enhancement request and there is not current timeline as to when this would be implemented. If you are a Cisco customer and come across this problem, please contact your Cisco account manager.</p>
CSCdx32239 (3)	Incorrect duplexity shown for router and switch interfaces and ports	<p>DFM was not always reporting the correct duplexity for router and switch interfaces. One reason this happened was because of the assumptions DFM made when the port or interface duplexity was reported as UNSPECIFIED.</p> <p>When DFM cannot correctly determine the duplex mode setting of a port or interface, it will disable all utilization and attribute rates, and duplexity will not be reported. This will eliminate HighUtilization alarms.</p> <p>This fix is provided in the latest DFM 1.2 IDU. The behavior is fully explained in the IDU Readme. To download the IDU, log in to Cisco.com and point your browser to:</p> <p>http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm</p>

Table 1 DFM Known Problems (continued)

Bug ID (Severity)	Summary	Explanation
CSCdx27739 (3)	DFM allows adding same device with two IP addresses	<p>If a device is in the Undiscovered class, it is possible to add the same device to DFM using two different IP addresses. This can occur if SNMP is not running on the device when the device is first added.</p> <p>This problem is fixed in the latest DFM 1.2 IDU. To download the IDU, log in to Cisco.com and point your browser to:</p> <p>http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm</p>
CSCdx17574 (3)	DFM manages Layer 2 ports on any devices it classifies as routers	<p>On any devices DFM classifies as routers—such as the Catalyst 4224 and Cisco 3700—DFM creates interface objects for all Layer 2 ports on the device. This is because DFM manages all router interfaces by default. (For example, on the Catalyst 4224, DFM creates interface objects for all FXS card ports.) This could create performance problems on enterprise systems.</p> <p>The workaround is to create a special group that does not manage these interfaces:</p> <ol style="list-style-type: none"> 1. From the Polling and Thresholds Console, select the Polling tab. 2. Click on the DFM domain to display the groups. 3. Right-click the Interface group and select New Group. 4. On the right column, select the Matching Criteria tab. 5. In the Value column, change Type and Mode to whatever is appropriate. 6. Click Apply. 7. Click Reconfigure. 8. From the Administration Console, select Inventory>Save Inventory.

Table 1 DFM Known Problems (continued)

Bug ID (Severity)	Summary	Explanation
CSCdx10326 (3)	Need better message for adapter with wrong username	<p>When the HPOV-NetView Adapter is installed on a remote system running HP OpenView, and the user enters an incorrect username and password on the remote server, Windows 2000 logs report “Waiting for Connection,” and ovstatus reports the process as running.</p> <p>The workaround is to verify that the username and password are correct, and change them if necessary:</p> <ol style="list-style-type: none"> 1. From the server, display the username and password: <code>DFMConnect.pl -s -show</code> 2. From the client, display the current username and password: <code>DFMConnect.pl -c -show</code> 3. From the client, change the username and password to match those of the server: <code>DFMConnect.pl -c -r <i>username password</i></code> 4. From the client, restart the necessary processes by doing <i>one</i> of the following: <ul style="list-style-type: none"> – Restart the CiscoWork2000 Server: <code>net stop crmdmgtd</code> <code>net start crmdmgtd</code> – Run ovstop and ovstart.
CSCdw19930 (3)	DFM reports HSRP implementation as duplicateIP	<p>HSRP virtual IP addresses are no longer reported as duplicate IP addresses when the latest DFM 1.2 IDU is installed. To download the IDU, log in to Cisco.com and point your browser to: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm</p>

Table 1 DFM Known Problems (continued)

Bug ID (Severity)	Summary	Explanation
CSCdu26398 (3)	Cannot disable polling on ports and interfaces	<p>If a Voice Gateway is added to VHM and performance polling for ports and interfaces is disabled, DFM should not poll the device. However, DFM continues to poll the device.</p> <p>The workaround is to also disable connectivity polling:</p> <ol style="list-style-type: none"> 1. From the Polling and Thresholds Console, select the Polling tab. 2. Click the DFM domain to display the groups. 3. Navigate through the device class (such as Router or Switch) to Settings>Connectivity Polling. 4. In the right column, set Analysis Mode to Disable. 5. Click Apply. 6. Click Reconfigure. 7. From the Administration Console, select Inventory>Save Inventory.
CSCdw88545 (3)	Access Servers: Missing supported alarms	<p>For an AS5400 or AS5350 with a large number of interfaces, DFM sometimes fails to subscribe to certain alarms on these interfaces (such as HighErrorRate and HighDiscardRate). These events are not displayed on the DFM consoles.</p> <p>There is no workaround.</p>
CSCdv28234 (3)	DFM show incorrect OperStatus for FXS and FXO interfaces	<p>An SNMP query on the FXS and FXO interfaces verifies that ifOperStatus is “dormant” (ifAdminStatus is “up”), which is expected when a call is not in progress. However, DFM reports the OperStatus as “other,” which is incorrect and conflicts with the what the OperStatus Description field should report (“Reflects the current operational status of the interface as reported by the instrumentation”). This problem was observed on DFM 1.1.</p> <p>There is currently no workaround.</p>

Table 1 DFM Known Problems (continued)

Bug ID (Severity)	Summary	Explanation
CSCdw64867 (3)	DFM periodically stops forwarding traps to HP OpenView/NNM after a few days	<p>DFM occasionally stopped forwarding traps to HP OpenView or NetView after a few days of normal operation. This occurred when subscription profile information was lost due to a lag between when the Trap Notifier Adapter process starts, and the adapter actually connected to the server. This lag occurred when:</p> <ul style="list-style-type: none"> • The Trap Notifier Adapter was configured to start upon system reboot. • The Trap Notifier Adapter was configured to start upon system reboot AND the DFM server had a large repository to restore. <p>This problem has been fixed in the latest DFM 1.2.x IDU. To download the IDU, log in to Cisco.com and point your browser to: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm</p>
CSCdw78953 (3)	DFMFileNotifier periodically stops writing to file log	<p>The DFM File Notifier Adapter occasionally stopped writing to the alarm log file. This occurred when subscription profile information was lost due to a lag between when the File Notifier Adapter process started, and the adapter actually connected to the server. This lag occurred when:</p> <ul style="list-style-type: none"> • The File Notifier Adapter was configured to start upon system reboot. • The File Notifier Adapter was configured to start upon system reboot AND the DFM server had a large repository to restore. <p>This problem was fixed in the latest DFM 1.2.x IDU. To download the IDU, log in to Cisco.com and point your browser to: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm</p>

Table 1 DFM Known Problems (continued)

Bug ID (Severity)	Summary	Explanation
CSCdx35118 (3)	Documentation does not specify that serial interfaces not managed on Access Servers	<p>The documentation does not specify that serial interfaces on Access Servers are, by default, not managed by DFM. Although Access Servers are classified as Routers, and router interfaces are normally managed by DFM, Access Server serial interfaces are not managed because of their sheer number.</p> <p>This information has been added to Appendix A, “Device-Specific Information” of the <i>User Guide for Device Fault Manager</i>, available from online help or Cisco.com.</p>
CSCdw91367 (3)	Monitoring Console reporting wrong event for ISDN status	<p>When an ISDN interface was configured to back up a primary link, the physical interface was up and the two B-channels are down (which is the correct behavior). However, because DFM interpreted ISDN interfaces to be set to BACKUP mode by default, DFM interpreted the physical interface backup as being activated, and the two B-channels (which are DS0) as operationally down (which was not correct).</p> <p>The latest DFM 1.2 IDU provides changes that correct the modeling. The changes are described in the IDU Readme. To download the IDU, log in to Cisco.com and point your browser to: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm</p>
CSCdt57822 (3)	Cat3548XL memory/processor not supported	<p>Certain IOS-based devices (such as the Catalyst 3548XL) are not fully supported in DFM 1.1 or DFM 1.2.</p> <p>Device support for the Catalyst 3548XL is provided in the latest DFM 1.2.x IDU. To download the IDU, log in to Cisco.com and point your browser to: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm</p>

Table 1 DFM Known Problems (continued)

Bug ID (Severity)	Summary	Explanation
CSCdx55371 (3)	File Notifier doesn't write to file after subsequent installations	<p>The File Notifier Adapter occasionally stops writing to the alarms log after subsequent installations on CiscoWorks2000. This can occur when subscription profile information is lost due to a lag between when the File Notifier Adapter process starts, and the adapter actually connects to the server. This lag occurs when:</p> <ul style="list-style-type: none"> • The File Notifier Adapter is configured to start upon system reboot. • The File Notifier Adapter is configured to start upon system reboot AND the DFM server has a large repository to restore. <p>The workaround is as follows:</p> <ol style="list-style-type: none"> 1. Make sure the DFM server is running and then stop and restart the adapters. 2. Consider disabling the adapters for automatic restart (by using the DFM GUI). 3. If you want the adapters to automatically restart, instead of using a subscription profile, use a choice subscription. For more information, refer to the <i>User Guide for Device Fault Manager</i> on Cisco.com.

Table 1 DFM Known Problems (continued)

Bug ID (Severity)	Summary	Explanation
CSCdx56957 (3)	Cat IOS devices: interfaces shown in both port and interfaces	<p>After adding a Catalyst device running IOS, Gigabit Ethernet GE1/1 and GE1/2 interfaces are displayed in both the Interface and Port groups.</p> <p>This behavior occurs because when you assign an IP address to a port on a Catalyst switch, and the Catalyst switch is running the IOS operating system, DFM creates an object in both the Port and Interface classes. The object in the Interface class represents a logical entity which DFM uses to maintain connectivity information. You should check the object in the Port class for expected fault and performance information.</p> <p>The latest DFM 1.2 IDU fixes this behavior. If the IDU is installed, 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. To download the IDU, log in to Cisco.com and point your browser to:</p> <p>http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm</p>
CSCdx54862 (3)	Insert card doesn't clear alarm	<p>After removing a device module from DFM, DFM generates an SNMP trap, but when the module is re-inserted, DFM continues to generate the alarm. This occurs because when DFM receives cold traps (along with warm start traps and module insertion traps), DFM places the module on the DFM pending list (to be rediscovered during inventory collection). DFM will continue to generate the alarms until the device is rediscovered. Thus the change is not known to DFM until inventory collection is performed.</p> <p>The workaround is to manually rediscover the pending list devices by selecting Inventory>Inventory Collection Pending.</p>

Table 1 DFM Known Problems (continued)

Bug ID (Severity)	Summary	Explanation
CSCdx30038 (4)	Error message does not report when broker passwords don't match	<p>When a remote VHM user attempts to attach to a DFM domain, and the user enters an incorrect username or password, this error message is displayed:</p> <pre>Could not connect with the broker named :172.20.121.31:9002. Is it running ?</pre> <p>This error message should be changed to something more helpful.</p> <p>If you encounter this message, check the following:</p> <ol style="list-style-type: none"> 1. Verify whether the broker is down; if it is, bring it up. 2. Verify whether the username and password are correct, and change them if necessary: <ol style="list-style-type: none"> a. On the DFM server, display the username and password: <pre>DFMConnect.pl -s -show</pre> b. On the remote VHM machine, display the current username and password: <pre>DFMConnect.pl -c -show</pre> c. On the remote VHM machine, change the username and password to match those of the DFM server: <pre>DFMConnect.pl -c -r username password</pre> d. On the remote VHM machine, restart the CiscoWorks2000 Server: <pre>net stop crmdmgtd net start crmdmgtd</pre>

Table 1 DFM Known Problems (continued)

Bug ID (Severity)	Summary	Explanation
CSCdw23386 (4)	BRI if/subif Mode change made in Admin Console does not persist	Changes made to interface modeling would not persist after the DFM inventory was rediscovered. This has been fixed in the latest DFM 1.2 IDU by improving the interface modeling for IDSN interfaces. The new modeling is explained in the IDU Readme file. To download the IDU, log in to Cisco.com and point your browser to: http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm

Table 2 *DFM Resolved Problems*

Bug ID (Severity)	Summary	Additional Information
CSCdv53955 (2)	DFM shows InsufficientFreeMemory for not having enough free flash	DFM no longer shows InsufficientFreeMemory for Catalyst switches (running CatOS) when switches have minimal flash space left.
CSCdt94677 (2)	Broker does not restart	DFM no longer fails to restart the broker if a broker.rps file already exists.
CSCdv25412 (2)	RSM interfaces generate erroneous collision information	DFM no longer generates erroneous collision information for RSM interfaces (DFM no longer classifies them incorrectly as “ETHERNETCSMACD”).
CSCdu56631 (3)	DFM shows bogus memory ExcessiveFragmentation faults for Catalyst switches	DFM no longer shows bogus memory ExcessiveFragmentation faults on Catalyst switches.
CSCdt95564 (3)	DNS name not displayed for Media Servers in the Inventory tree	DNS name is now displayed when Media Server is added to DFM (using Add Agent) and the user supplies the device's DNS name.
CSCdv56968 (3)	Fast memory is not a problem and should not be reported	DFM no longer reports a problem when an RSM running 11.2(15)P code is low in Fast memory. Fast refers to the 128 KB SRAM portion of MEMD for faster access, where MEMD is a two-port shared memory that stores the packet data and data structures used to control interface processors and packet buffers. Users have no control over the use of Fast and need not concern themselves with these numbers—a low number indicates an effective use of SRAM by the system.
CSCdu61181 (3)	Devices aren't imported to DFM using domain name	When Resource Manager Essentials devices are added to DFM, all devices are now reported with their Fully Qualified Domain Name (FQDN).

Table 2 DFM Resolved Problems (continued)

Bug ID (Severity)	Summary	Additional Information
CSCdv06863 (3)	DFM 1.1 install fails to find HPOV NNM6.2 with space in directory	When installing DFM 1.1 and HPOV NNM6.2 on the same machine, the installation would display an error if the HP OpenView NNM6.2 installation directory name contained a space (for example, "F:\HP Openview"). This error is no longer displayed.
CSCdw25330 (3)	AS5300 shows as Certified	The AS5350 and AS5400 devices were being displayed with a "Certified" device level, rather than a "Validated" level. These devices now show as "Validated."
CSCdt76654 (4)	Cannot add a job after removing it	For DFM 1.1 running with VHM 1.0, when a VHM job was removed, subsequent VHM jobs, such as inventory collection and device rediscovery, could not be added. This problem no longer occurs.
CSCdt76715 (4)	Multiple instances of job is created	For DFM 1.1 running with VHM 1.0, when a user would schedule VHM inventory collection and subsequently reschedule the collection, DFM created multiple jobs instead of modifying the schedule of the original job. This problem no longer occurs.

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

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 **Feedback** at the top 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 resellers 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 “[Documentation Roadmap](#)” 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 © 2002, Cisco Systems, Inc.
All rights reserved.