

# CiscoWorks Device Fault Manager

Device Fault Manager (DFM) provides real-time fault analysis for Cisco devices. Through a variety of data collection and analysis techniques, DFM generates “intelligent Cisco traps,” which can be forwarded to other multi-device, multi-vendor event management systems installed in the network, sent to e-mail/pager gateways, or displayed in the DFM alarm window.

## Device Fault Manager

DFM provides real-time, detailed fault analysis, designed specifically for Cisco devices. This focus on Cisco devices enables DFM to monitor Cisco technology-based networks for variety of fault conditions, analyze these conditions, and only notify the user via intelligent Cisco traps when a problem has occurred requiring their attention.

DFM is designed to work out of the box, with support for more than 100 of the most common Cisco routers, switches, access

servers, and hubs already designed and included in the product. For each of these supported devices, DFM will automatically look a for range of common problems at the device and Virtual LAN (VLAN) level—all without requiring users to write rules or set polling or threshold values—ever. As the network grows and changes, DFM is engineered to detect any changes with the Cisco devices and will adjust its analysis accordingly.

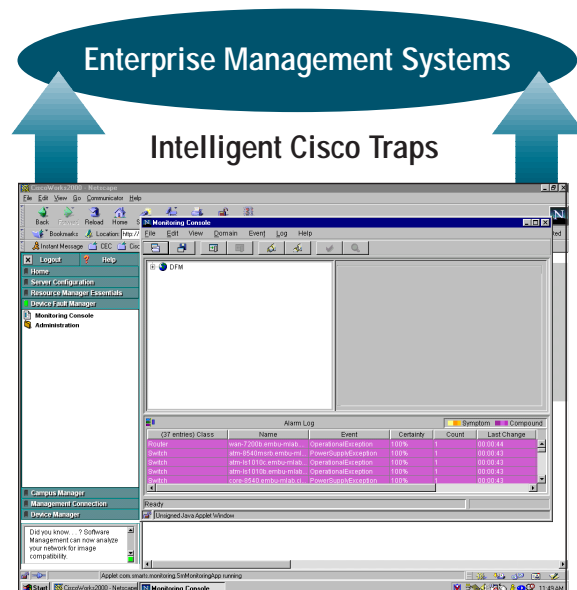
## DFM Features Include:

- Problem focused fault analysis
- Integration with CiscoWorks
- Integration with enterprise management systems
- Support for Layer 2 and Layer 3 network devices
- On-going device support (incremental device updates)

## Problem Focused Fault Analysis

DFM actively monitors a wide range of Cisco internetworking equipment, at the device and VLAN levels. Depending on the type of device, DFM will actively monitor different conditions via Internet Control Message Protocol (ICMP) polling, Simple Network Management Protocol (SNMP) Management Information Base (MIB)

Figure 1  
Device Fault Manager





interrogation, and SNMP trap reception. DFM will track and analyze conditions known to cause higher level problems in that particular device.

If DFM receives information from the device that is not a known condition of a higher-level problem, DFM will ignore the information, minimizing the need for IT managers to look at every network event. This provides the opportunity for IT managers to proactively manage Cisco device faults.

DFM can easily recognize if a series of events from a device are related. For example, if a series of ports on a switch are down, instead of flooding your event screen with a multiple port-down traps, DFM will recognize that these ports are on the same module and tell the user that the module is down. If the condition continues, users will not receive separate notifications, DFM will increment the existing module down problem.

As part of its analysis, DFM continually analyzes the availability of Cisco devices and ports on the devices, but it also looks for specific problems within the device, including:

- *Chassis*—backplane utilization
- *Fan*—fan state not normal
- *Memory*—excessive fragmentation, buffer miss rate, buffer utilization, free memory
- *Network adapters*—backup activated, error rates at the system and VLAN level, broadcast rates, collision rates, discard rates, flapping, maximum uptime, queue drop rates, and utilization
- *Power supplies*—voltage out of range
- *Processors*—utilization
- *SNMP Agent*—unresponsive
- *System*—excessive restarts
- *Temperature*—temperature out of range

### **Integration with CiscoWorks**

DFM is designed to work with the entire family of CiscoWorks products. DFM integration with the CiscoWorks family includes:

- New Device Fault Manager folder on CiscoWorks desktop
- Leverages CiscoWorks security roles
- Utilizes CiscoWorks Server process and backup management services
- Automatically imports Cisco devices from Resource Manager Essentials (RME), for both local and remote installations of DFM and RME

### **Integration with Enterprise Management Systems**

DFM can be utilized as a Cisco fault subsystem; generating intelligent Cisco traps to other multi-device, multi-vendor event management systems installed in the network. Cisco has worked closely with a range of enterprise management systems, enabling these intelligent Cisco traps to be displayed properly in their respective event systems.

### **Support for Layer 2 and Layer 3 Network Devices**

DFM analyzes both Layer 2 and Layer 3 devices, monitoring the them individually, but also recognizing which ports are members of specific VLANs, and automatically monitoring each VLAN as a group of devices.

## On-Going Device Support Updates (IDU)

As new Cisco devices are added to the network, DFM can easily be updated via an incremental device update capability of the Cisco Software Center. Just like the existing device support in DFM, all new devices added through incremental updates do not require any rules to be written by the user for DFM to analyze and report faults in your Cisco network.

## Specifications

A single copy of DFM can monitor a network with up to 30,000 Cisco ports when installed on its own sever.

## System Requirements

The server, client and web browser system requirements can be found in the Product Overview documents for the IP Telephony Environment Monitor LAN Management solutions and on Cisco's main on-line documentation site, under each CiscoWorks solution.

Please refer to these and other Product Installation documentation for more detailed information on setting up and configuring these solutions

## Supported Cisco Devices

The current supported device list is located at <http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/index.htm>

## Availability

Device Fault Manager is available in the LAN Management Solution. If you plan to install DFM with the full contents of the CiscoWorks LAN Management Solution see the LMS Product Overview documentation and other product installation documentation for more detailed information on setting up and configuring these solutions. See the Read Me First document for the appropriate bundle for additional information.

To place an order, contact your local Cisco sales representative.



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the  
**Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo 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.  
(0303R) 203046/ETMG\_04/03