



# Overview

---

These topics provide an introduction to the CiscoWorks Device Fault Manager product:

- [Overview of DFM, page 1-1](#)
- [DFM Architecture, page 1-2](#)
- [Elements Monitored by DFM, page 1-10](#)
- [How DFM Collects Inventory Information, page 1-11](#)
- [How DFM Monitors Networks, page 1-11](#)
- [What DFM Reports, page 1-12](#)
- [Supported Devices, page 1-13](#)

## Overview of DFM

DFM reports faults that occur on Cisco devices, often identifying fault conditions before users of network services realize that the condition exists. DFM analysis technology differs from the traditional rules-based approach to event analysis. DFM analysis uses a top-down approach that starts by identifying the fault conditions that affect managed systems and are important to identify and analyze. Each fault condition causes a set of symptoms—a problem signature—that occur within the faulty element and in related elements. DFM creates a causality mapping between the fault conditions and the symptoms. After the fault conditions and their symptoms are identified, this information is coded in the analysis model.

Because the event information necessary to diagnose fault conditions is present in the analysis model, DFM monitors only the events necessary to diagnose the condition. DFM simplifies event analysis: there are no rules to write and the analysis model guarantees that critical fault conditions are always identified.

DFM can operate as an independent management system or can integrate with existing management applications to add fault management to the functionality already in place.

## DFM Architecture

DFM consists of three components:

- [DFM Domain Manager, page 1-3](#)

The domain manager, DfmServer by default, is the centerpiece of DFM, pinpointing the cause of Cisco device failures.

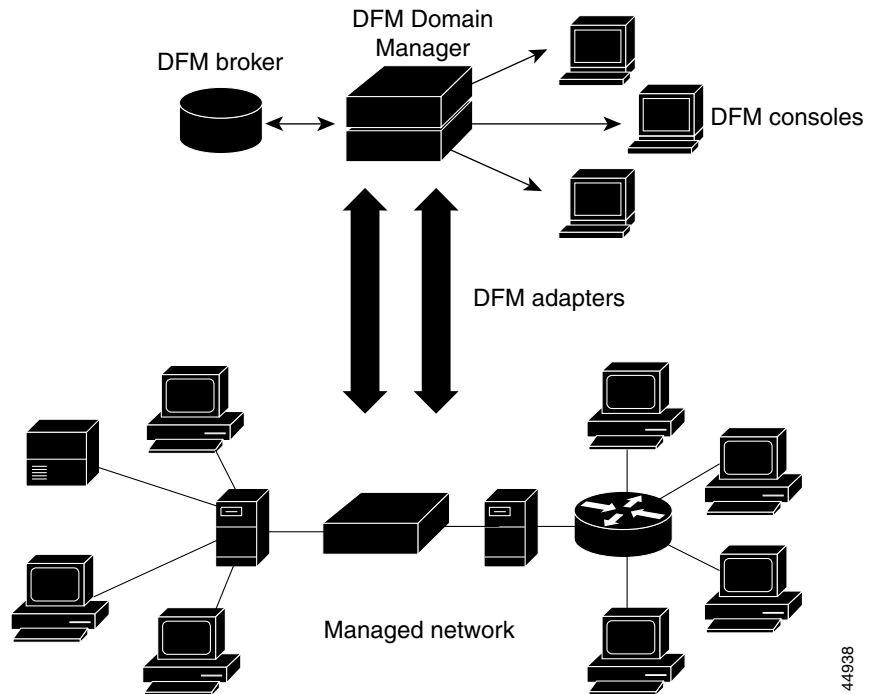
- [DFM Clients, page 1-8](#)

The consoles and adapters are examples of DFM clients. Adapters provide a means of communication between domain managers and the networked system. DFM consoles are graphical interfaces for interacting with domain managers. The Monitoring Console is used to view the results of a domain manager's analysis and the Administration Console, which also launches the Polling and Thresholds Console, is used to manage a DFM system.

- [DFM Broker, page 1-9](#)

The DFM broker facilitates communication between domain managers and clients.

Figure 1-1 Architecture of DFM Applications



44938

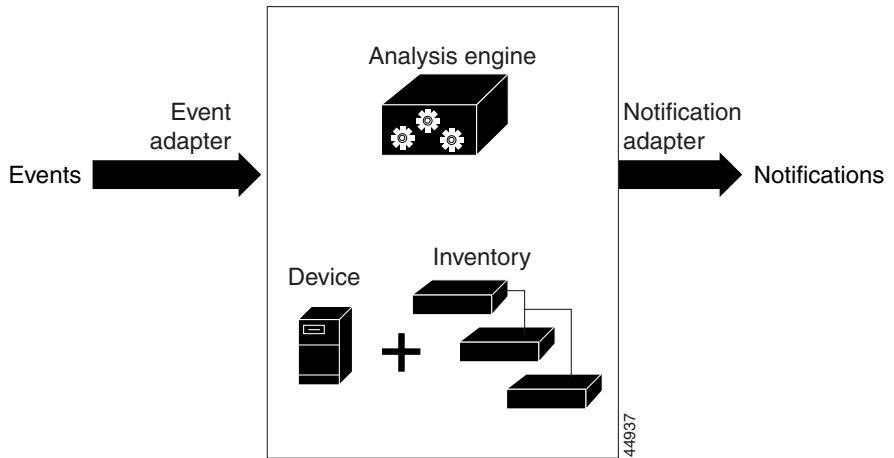
## DFM Domain Manager

A domain manager is a high-performance, multi-threaded application. It contains the Cisco *analysis model*, an in-memory repository of managed objects, and several adapters that interact with the managed domain.

The analysis model describes the types of elements managed by DFM, the fault conditions that can occur in those elements, and the symptoms that are caused by these conditions. In the DFM inventory, managed elements are represented by instances of the element types defined in the model.

For information on domain manager settings and properties, refer to the [“Domain Manager Settings”](#) section on page 11-10.

Figure 1-2 Domain Manager Architecture



## Analysis Model

The analysis model is an object-oriented data model that describes the managed domain. Each type of managed element in the managed domain is represented by a *class* in the analysis model.

A class consists of properties that describe a managed element. *Properties* include *attributes*, *relationships*, and *events*. Attributes describe a managed element, including its present state. Examples of attributes include an element's name and a counter that counts the number of packets traversing an interface.

Relationships define how managed elements are related to each other.

Events describe the failures that can occur in elements, the symptoms these failures cause, and the effect of failures. Symptoms can be local, observed in the element itself; or propagated, observed in elements related to the failing element.

## Event Notifications

Domain managers generate two types of event notification—*compound events* (also called exceptions or aggregates) and *symptomatic events*—which are displayed in the DFM Monitoring Console. When viewing the results of DFM's diagnosis, it is important to remember the differences between symptomatic and compound notifications.

**Note**

---

The depth of analysis performed on each network device depends upon the status information available via that device's Management Information Base (MIB). Not all devices support all MIB values.

---

## Compound Notifications

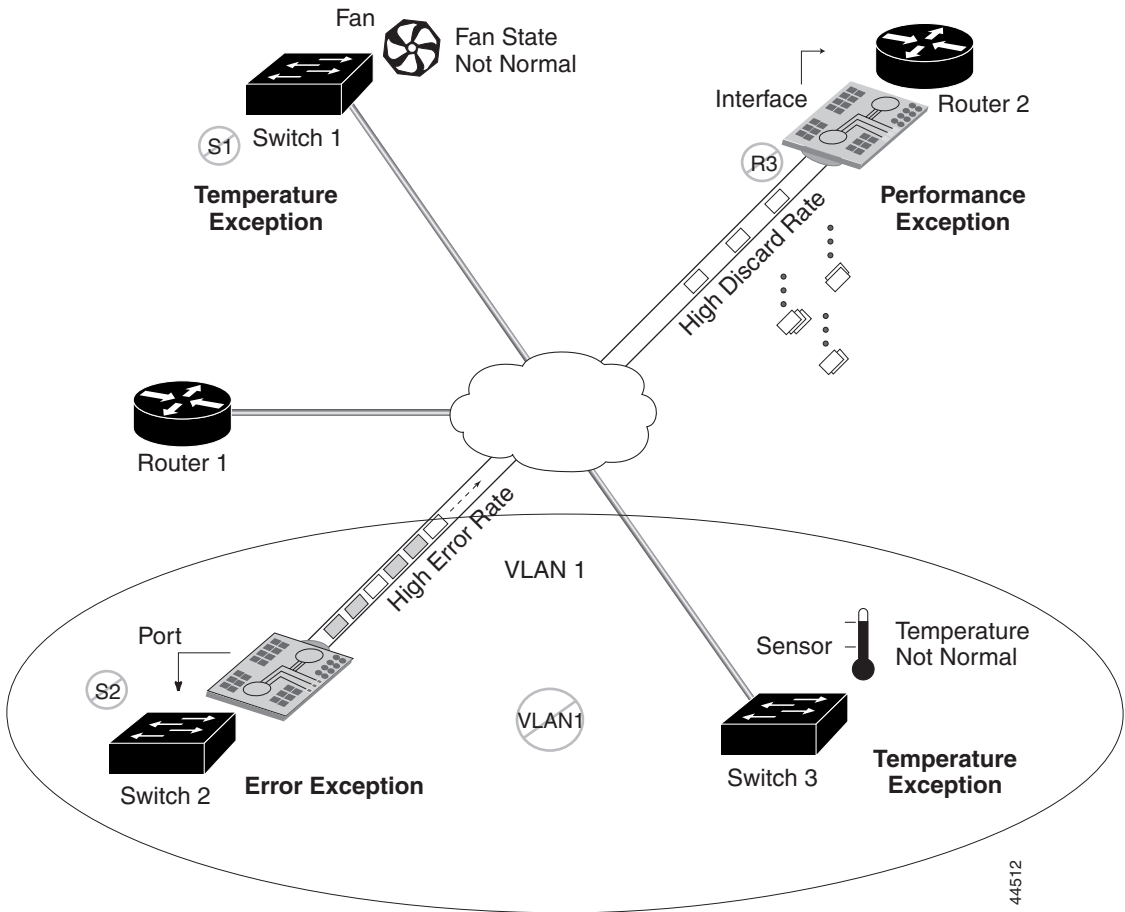
A compound notification (also referred to as an exception or aggregate) identifies a system or VLAN that is affected by one or more related faults. Exception notifications are displayed in purple on the console.

The properties of an exception notification list the faults that affect the managed element. Active faults are displayed in orange on the console.

## Symptomatic Event Notifications

A symptomatic event can also be called an *intra-device fault*, indicating an abnormal condition. One or more related faults occurring in a particular system or VLAN indicates an exception condition. These exceptions are displayed in yellow on the console.

Figure 1-3 Illustration of Faults and Exceptions



44512

## DFM Inventory

In the DFM inventory, managed elements are represented by *instances* of the classes defined in the model. An instance of a class represents a real-world managed element, such as an interface, a router, or a switch. The DFM inventory represents knowledge of the managed elements: how they are configured and how they are related to each other.

DFM performs inventory collection in the managed network. During collection, each managed device is probed to determine its configuration and its relationship to other managed elements. With this information, DFM creates instances and fills in the properties described in the analysis model.

The properties of a class serve as a template for all possible instances of that class, while the properties of an instance of a class describe a specific managed element in the managed domain.

Dynamic by nature, the DFM inventory is always changing as devices are added or taken offline, and other devices are configured or updated. DFM maintains a representation of the DFM inventory in memory and automatically updates it as the external DFM inventory changes.

## Analysis Engine

The analysis engine uses the analysis model and the DFM inventory to automatically build a *codebook*. The codebook is represented by a table. Each row represents a symptomatic event and each column represents a fault condition that DFM monitors for in the managed domain.

As the DFM domain manager monitors events, the analysis engine compares the set of monitored events with the problem signatures represented in the codebook. DFM diagnoses causes by finding the problems in the codebook that can best explain the observed events.

## DFM Clients

Any process that communicates with a domain manager is considered a client.

Examples of DFM clients include:

- [DFM Consoles, page 1-8](#)
- [DFM Adapters, page 1-9](#)

## DFM Consoles

The DFM consoles are multi-purpose interfaces that interact with the DFM domain manager. The *Monitoring Console* is the primary console, and it is used to display the results of a domain manager's analysis. Operators can filter alarms, view the effects of fault conditions on other managed elements, and initiate automated actions such as pages or e-mail in response to fault conditions. For information on the Monitoring Console, refer to [Chapter 13, "Common Monitoring Console Tasks."](#)

The *Administration Console* is also available for administrators. It enables them to manage and configure DFM applications by setting polling parameters, changing thresholds, and managing the DFM inventory. Some of these administrative tasks are performed using the *Polling and Thresholds Console*, which is launched from the Administration Console. For information on the Administration Console and the Polling and Thresholds Console, refer to [Chapter 5, "The DFM Administration Console and Polling and Thresholds Console."](#)

The DFM Console views can be customized for different users. For example, Alarm Log views in the console can be configured to filter out some events and to sort them based on other notification criteria.

## DFM Adapters

Adapters are applications that provide a means of communication between a domain manager and the networked system. Adapters can run as processes within a domain manager or as external applications.

DFM adapters perform a variety of tasks and are categorized according to function:

- Inventory adapters convey information about the managed Cisco elements. For example, when the DFM inventory adapter discovers Cisco elements, it creates instances to represent them in the DFM inventory maintained by the DFM domain manager. When the DFM inventory adapter discovers changes in Cisco devices, it automatically updates the domain manager's inventory. An example of an inventory adapter is the HPOV-NetView Adapter.
- Notification adapters receive event notifications from a domain manager and forward them to other applications. For example, when the Mail Notifier Adapter receives a cause notification from a domain manager, it sends an email message to designated recipients. Other examples of notification adapters are the Trap Notifier Adapter and the File Notifier Adapter.

For information on using these adapters, refer to [Chapter 10, "Using DFM Adapters."](#) For information on installing local and remote adapters, refer to *Installation and Setup Guide for Device Fault Manager*.

## DFM Broker

The DFM broker maintains a registry of information about a domain manager, including the following:

- Application name of the domain manager (by default, DfmServer).
- Hostname of the computer on which the domain manager is running.
- TCP port at which the domain manager is listening for client connections.

A domain manager notifies the broker when it shuts down and the broker removes its listing for the domain manager. Periodically, the broker connects to the domain manager to track its status.

When a DFM client needs to connect to a domain manager, it contacts the broker to determine the host that the domain manager is running on and the port on which the domain manager is listening.

For more information on the DFM broker, refer to the [“How the DFM Broker Works” section on page 11-8.](#)

## Elements Monitored by DFM

DFM diagnoses fault conditions on the following network elements:

- Bridges
- Chassis
- Cards
- Hosts
- Hubs
- Interfaces
- Module Switch Feature Card (MSFC)
- Ports
- Power Supplies
- Routers
- Router Switch Feature Card (RSFC)
- Route Switch Modules (RSM)
- SNMP Agents
- Switches
- System Fans
- System Memory Resources
- System Processor Resources
- VLANs

For more information on these elements, refer to [Chapter 2, “Network Elements Managed by DFM.”](#)

# How DFM Collects Inventory Information

DFM performs Simple Network Management Protocol (SNMP) polling to collect network inventory data from a variety of Management Information Bases (MIBs). Generic probes access standard MIBs and Cisco-specific probes access Cisco proprietary MIBs. DFM uses the information collected to create a representation of the managed elements within a domain manager's inventory.

For more information about the inventory collection process (including which MIB variables are queried), refer to [Chapter 7, “DFM Inventory Collection.”](#) Also, a complete list of MIBs polled is provided in [Appendix B, “MIBs Polled and SNMP Traps Processed or Passed-Through by DFM.”](#)

# How DFM Monitors Networks

After initial discovery, DFM continuously monitors the status of devices in your network using:

- SNMP polls
- SNMP trap message processing
- Internet Control Message Protocol (ICMP) polls

DFM gathers fault-related, intra-device information through SNMP polling and SNMP trap messages. DFM determines which devices to poll based on current polling configuration settings that you control. DFM also monitors device connectivity through ICMP polling.

For more information about the SNMP and ICMP polling process, refer to [Chapter 9, “Polling.”](#) For more information about SNMP traps, refer [Appendix B, “MIBs Polled and SNMP Traps Processed or Passed-Through by DFM.”](#)

By default, DFM monitors all Cisco devices and all ports that connect Cisco devices in your inventory. Such ports are referred to as *trunk ports* because they connect network infrastructure devices. *Access ports*, on the other hand, connect network infrastructure devices to host devices.

**Note**

---

By default, DFM manages trunk ports but does not manage access ports.

---

You can enforce a different management policy for your network elements by changing an element's managed state or by altering the polling and threshold settings associated with it.

For more information about changing the managed state of an element, creating new groups, and changing performance thresholds, refer to [Chapter 8, “Working with DFM Groups and Settings.”](#)

## What DFM Reports

DFM reports two types of notifications: faults and exceptions (or compound events).

Faults indicate abnormal conditions observed by the DFM. Examples of performance faults are:

- High error rate on a network adapter
- High utilization of a switch's backplane
- High buffer miss rate on a system's memory component

DFM uses the detection of faults to diagnose performance and operational problems. You can *drill down* on an exception notification to view the details about the faults that were detected to diagnose the fault condition.

Exceptions indicate that one or more related faults are occurring in a particular system or VLAN. For example, suppose that a switch in your network is experiencing performance faults on two of its ports. One port has a High Utilization fault while another port has both a High Broadcast Rate and a High Discard Rate. DFM generates one Performance Exception notification for the switch. You can determine the specific ports that are causing the switch problem by double-clicking on the exception notification to view the Notification Properties window.

Notifications are displayed in the alarm log view of the Monitoring Console. Symptomatic fault notifications are colored orange. Compound notifications are colored purple.

# Supported Devices

Device adapter packages for all supported devices are installed when you install DFM. Information about devices installed with DFM can be found at

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev\\_sup/dfm1\\_2.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev_sup/dfm1_2.htm)

You can download device packages for new devices from Cisco.com and find information about all supported devices by logging into Cisco.com at

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

Device packages are released cumulatively; that is, new device packages contain the contents of any previous packages.

To determine which packages are installed on your CiscoWorks Server, select **Server Configuration > About the Server > Applications and Versions**.

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

