



CHAPTER 1

Introduction

These topics provide an overview of Device Fault Manager (DFM):

- [What Is DFM?](#), page 1-1
- [What's New in DFM 3.0?](#), page 1-3
- [Is DFM Ready to Use?](#), page 1-4
- [How Will I Use DFM for Day-to-Day Operations?](#), page 1-5
- [How Does DFM Work?](#), page 1-7

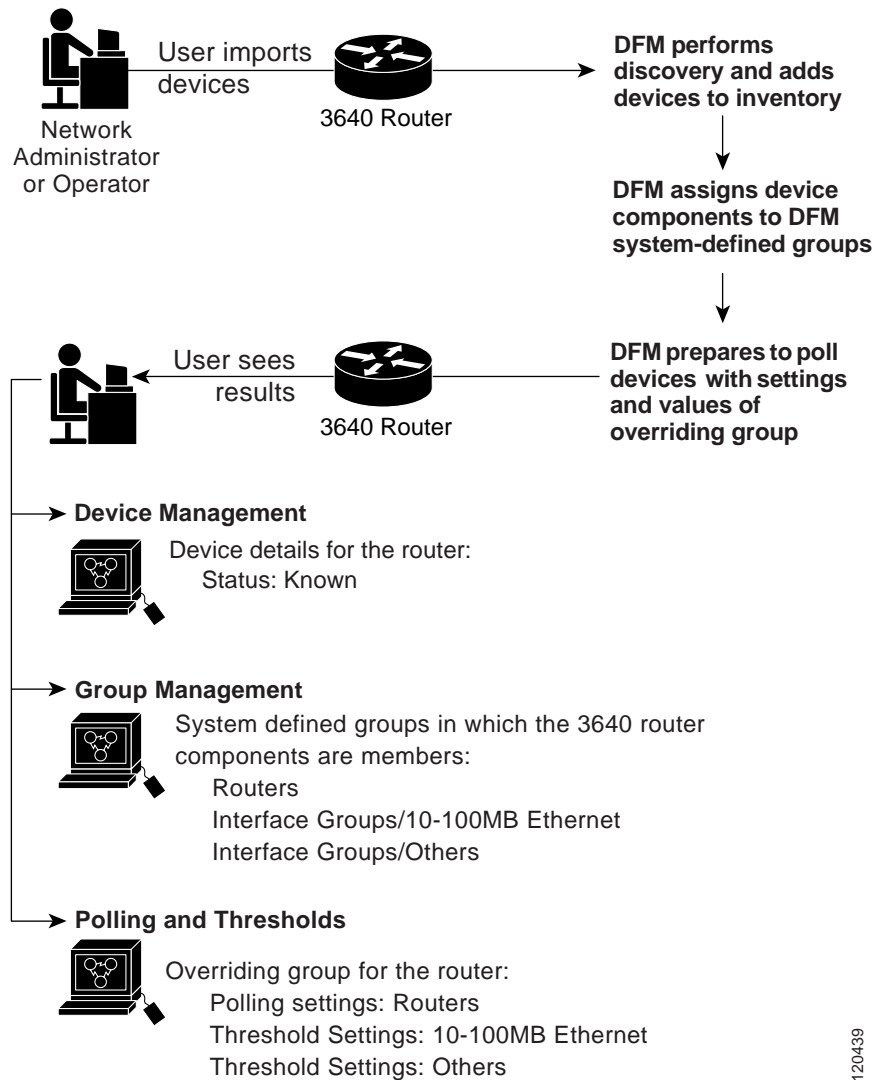
What Is DFM?

DFM offers the following real-time assistance to network operations personnel:

- Monitoring and displaying the operational health of the network
- Analyzing events that occur in these environments and determining when a probable fault has occurred
- Notifying users of alert conditions through an online display and through other notification services

[Figure 1-1](#) shows the series of activities that DFM performs when a user imports a Cisco 3640 router into DFM. The figure also shows how a user can confirm that these activities have occurred.

Figure 1-1 Importing a Router into DFM



DFM performs the following tasks after a user imports a device:

- DFM obtains basic information from the Device and Credentials Repository (DCR), which was supplied when the device was added to the DCR.
- DFM discovers the device—You can see the results of this discovery using Device Management.
- DFM assigns the device to system-defined groups—You can see which devices are members of each system-defined group using Group Management; the Membership Details page for any group will display them.
- DFM starts to poll the device—You can see alerts for a device on the Alerts and Activities display when events occur on the device. You can see the polling and threshold group that DFM uses for DFM polling parameters and threshold values for the device on the Polling Parameters Summary and Thresholds Summary pages.

When you first start to use DFM, you may be interested in the answers to the following questions:

- [What's New in DFM 3.0?, page 1-3](#)
- [Is DFM Ready to Use?, page 1-4](#)
- [How Will I Use DFM for Day-to-Day Operations?, page 1-5](#)
- [How Does DFM Work?, page 1-7](#)

What's New in DFM 3.0?

DFM 3.0 provides the following new features and enhancements:

- Enhancements to the AAD and AAD filtering—The Alerts and Activities display (AAD) has been enhanced to support up to 5,000 alerts. It is enhanced with paging tables so you can view all device issues. In addition, wildcard searches are now supported by Alerts and Activities display filters; see [Filtering Alerts and Activities, page 3-8](#).
- Integration with new CiscoWorks LMS Portal—The CiscoWorks LMS Portal replaces the CiscoWorks home page as the default home page for the LAN Management Solution. The portal provides quick status information on devices, the network, and the system. You can configure portal contents to fit your needs. The [User Guide for CiscoWorks Assistant 1.0](#) provides complete information on how to use the portal.
- Integration with new CiscoWorks Assistant—The CiscoWorks Assistant provides workflows that integrate key LMS application functionality. These workflows help you when you deploy, operate, and troubleshoot the LMS system. The [User Guide for CiscoWorks Assistant 1.0](#) provides complete information on this product.
- Enhancements to automatic device import—You can create customized filters that control device import. Devices must meet the filter criteria in order to be automatically imported. This feature is offered in addition to manual and bulk import, which were available in previous versions of the software. See [Importing Devices into DFM, page 4-9](#).
- Ability to selectively unmanage IP addresses—The Detailed Device View now lists IP addresses supported on all devices, and allows you to unmanage them one at a time. See [Suspending/Resuming a Single Device Component, page 3-18](#).
- Ability to perform bulk manage and unmanage operations—You can use ASL scripts to perform bulk manage and unmanage operations of interfaces, ports, IP addresses, processors, and memory. You must edit a file that is generated by the scripts to reflect the management state you want, and then apply the changes to the DFM inventory. See [Performing Bulk Manage/Unmanage Operations, page 3-19](#).
- New attributes support for creating User Defined Groups—The following attribute types are now supported when you create a user defined group:
 - Mib2ifType
 - DescriptionsSee [Working with Customizable Groups, page 8-4](#).
- Enhancements to Fault History—The Fault History screens have been reorganized to make them more intuitive. See [Starting Fault History, page 6-2](#).

Is DFM Ready to Use?

The person or team that installed DFM should have completed the initial configuration before you start working with DFM. The instructions for configuring DFM are included in *Installing and Getting Started with CiscoWorks LAN Management Solution 3.0*.

To use DFM, you must import devices into the DFM inventory as explained in [Importing Devices into DFM, page 4-9](#). Make sure that your devices are forwarding traps to DFM on port 162 (if port 162 is occupied, DFM uses port 9000). (The ports that are occupied by CiscoWorks are listed in *Installation and Getting Started Guide for LAN Management Solution 3.0*.)

Once you have imported devices, DFM is ready to monitor and analyze events, and provide notification of alerts on the Alerts and Activities display. DFM uses the default polling parameters and threshold values, default rediscovery and purging schedules, and default views. You should determine whether the default values are adequate for your use.

[Table 1-1](#) lists tasks that you may attend to, at your discretion, after the initial configuration. The table lists optional configuration tasks and some day-to-day tasks that you may want to address when you first start to use DFM.

Table 1-1 Tasks to Consider when Initially Setting Up DFM

Initial Setup Tasks	Explanation	Reference
Subscribe users to receive e-mail notification of alerts and subscribe hosts to receive DFM-generated SNMP trap, e-mail, and syslog messages.	DFM displays the operational health of the network on the Alerts and Activities display. In addition, you can subscribe users and hosts to receive e-mail, syslog, or SNMP trap notifications, in response to alerts.	How to Use the Alerts and Activities Display, page 3-1 Using Notification Services, page 5-1
Update polling parameters and threshold values.	DFM provides default values. However, you can update the values based on your experience with and knowledge of the network.	Configuring Polling and Thresholds, page 10-1
Update device rediscovery schedules.	DFM provides a single default schedule for device rediscovery. You can use that schedule or create additional rediscovery schedules (several can be active at the same time).	Configuring Rediscovery Schedules, page 7-5
Add Alerts and Activities views.	Alerts and Activities views control which groups of devices are the focus of the Alerts and Activities display. DFM provides two default view (All Alerts and Suspended Devices). You can add more views.	Configuring Views for the Alerts and Activities Display, page 9-1
Update the daily purging schedule.	By default, DFM purges the database at midnight. You can modify the schedule.	Configuring the Daily Purging Schedule, page 7-4
Configure DFM to forward traps to a Network Management System (NMS).	DFM can forward traps to other NMSs, such as HP OpenView and NetView.	Integrating SNMP Trap Receiving with Other Trap Daemons or NMSs, page 7-9

How Will I Use DFM for Day-to-Day Operations?

These topics briefly describe the DFM functions and how they are used, often on a daily basis:



Note

Your login determines the operations you can perform. For more information, refer to [Understanding Your User Role, page 2-7](#).

- **Alerts and Activities**—To monitor the network and assess its health.
- **Fault History**—To monitor the network and assess its health
- **Device Management**—To keep the inventory of devices that DFM monitors current.
- **Notification Services**—To ensure that the right users and systems receive e-mail, syslog or SNMP traps in response to alerts on selected devices.
- **Configuration**—To change polling and threshold settings, and perform system administration.

To make the most effective use of DFM on a day-to-day basis, users need to understand the impact of operations on configuration and administration tasks. An overview is provided in [Performing Scheduling Tasks, page 7-3](#).

The DFM functions that support day-to-day operations are further described in the following topics:

- [What Is Alerts and Activities?, page 1-5](#)
- [What Is Device Management?, page 1-6](#)
- [What Is Notification Services?, page 1-6](#)
- [What Is Fault History?, page 1-7](#)
- [What Is Configuration?, page 1-7](#)

What Is Alerts and Activities?

The Alerts and Activities display provides a consolidated real-time view of the operational status of your network. When a fault occurs in your network, DFM generates an event. All events occurring on the same device are rolled up into a single alert. You can also use Notification Services to change an event name to something that is more meaningful to you.

When an alert occurs on an element in your active view (a logical group of devices), it is displayed on your Alerts and Activities display. You, or a user with the necessary privileges, can customize your view to include only those device groups that are important to you.

From the Alerts and Activities display you can also:

- Drill down into an alert to see what events caused the alert, and add alert annotations for other users to read.
- Drill down into specific events for MIB attribute values.
- Open a Detailed Device View (DDV) to examine device components and suspend or resume monitoring them.
- Use tools such as CiscoView, User Tracking (if Campus Manager is installed), and Fault History.

You can see which components of the device are in the DFM manageable inventory as follows: After you locate the device on the Alerts and Activities display, you can click it and open a DDV. The DDV displays the manageable components of the device. From the DDV, a user with the necessary privileges

can suspend monitoring of a device component and, afterward, resume monitoring of the device component again. Suspended devices are moved to the Suspended Devices view. To launch a DDV for devices that currently have no alerts, use **Device Management > Device Details**.

What Is Device Management?

Device Management involves keeping the inventory of devices that DFM monitors up-to-date. Before devices can be in the DFM inventory, they must be added to the Device and Credentials Repository (DCR). The DCR is a centralized device repository for sharing device information across CiscoWorks. You can control whether all DCR devices are automatically added to the DFM inventory; whether DCR devices must match customized filters that you create, in order to be added; or whether you can manually add individual DCR devices to the DFM inventory. Synchronization is controlled using the Device Import page; by default, DFM is configured to use manual device import.

The DCR is the front-end for adding devices to and exporting devices from CiscoWorks, and modifying device credentials. DFM provides a user interface for performing the following operations on devices in the DFM inventory:

- Viewing device details
- Rediscovering devices
- Suspending and resuming DFM device management
- Deleting devices (*local delete*), when manual DCR synchronization is being used)

The following scenario describes the process for managing devices:

1. Devices are added from the DCR to the DFM inventory.
2. DFM gets basic information from the DCR.
3. DFM discovers a device and adds its manageable elements to its inventory, placing the device and its elements into the appropriate DFM system-defined groups. (The user can click View Discovery Status to see the status of the device import.)
4. By default, DFM performs rediscovery on a weekly basis. A user can update the default discovery schedule or add discovery schedules.

What Is Notification Services?

In addition to watching network conditions as they change on the Alerts and Activities display, you can use notification services to automatically notify users and other systems when specific changes occur on selected devices. To do so, you create subscriptions for e-mail notifications, DFM-generated SNMP trap notifications, or syslog notifications. You can also change event names to names that are more meaningful to you, and these names will be reflected in the DFM displays and notifications.

DFM subscriptions comprise:

- Alerts and/or events. For events, the subscription can contain an event set, which lists the specific events in which you are interested.
- A notification group, which lists the devices (or device groups) and alert/event severity levels in which you are interested.

You can add, modify, and delete subscriptions at any time as your need to disseminate the status and severity of alarm and event changes.

What Is Fault History?

Fault History provides the history of DFM events and alerts. The stored history includes alert information and annotations (informational text entered by DFM users), and event information and properties (component name and MIB attributes).

You can start Fault History in the following ways:

- From the DFM Alerts and Activities Display page. From here, you can generate a Fault History display with information about alerts and events from the last 24 hours.
- From the DFM home page by selecting **Faults > Fault History**. This method provides historical information about all alerts and events in the Fault History database. The Fault History database keeps information for the alerts and events that occurred within the last 31 days.
- From the LMS portal by selecting **Device Diagnostic Tools > Device Center**. From here, you can select a single device and generate a 24-hour or 31-day display.

You can use Fault History to generate customized tabular displays of specific alerts, specific events, event dates, and event severity.

What Is Configuration?

The Configuration pages provide a centralized location for all DFM configuration tasks. Configuration tasks are divided into two categories: Polling and Thresholds, and Other Configurations.

- The Polling and Thresholds category contains the functions that you can use to adjust polling and threshold settings on devices, ports, and interfaces.
- The Other Configurations category includes system administration tasks, such as configuring rediscovery schedules, logging levels, views for the Alerts and Activities display, trap forwarding and receiving; and selecting an SMTP server. In addition, you can perform group management from Other Configurations.

How Does DFM Work?

These topics provide a simplified view of DFM user tasks and DFM processing:

- [Users Perform Device Management and Configuration, page 1-8](#)
- [DFM Performs Ongoing Monitoring, Analysis, and Notification, page 1-9](#)
- [Users Respond to Notifications and Alerts, page 1-10](#)

Users Perform Device Management and Configuration

Users supply the information that tells DFM what to monitor. [Figure 1-2](#) shows a user importing devices, and performing optional configuration tasks to optimize DFM.

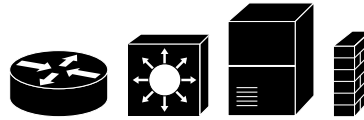
Figure 1-2 The Role of User Input

Create the DFM Inventory



Configure devices to forward traps to DFM.

Import devices.



Manage the Information (Alerts and Traps)



Manage polling and threshold settings.
Create e-mail, SNMP trap, and syslog notification subscriptions.
Configure SNMP trap forwarding to another NMS.
Customize the Alerts and Activities display.

Maintain the Data



Schedule database purging.
Configure the Rediscovery Schedule.
Adjust polling parameters.
Adjust thresholds.

120441

You must import devices and, as your network changes, you must add and delete them accordingly. DFM performs periodic rediscovery, refreshing the inventory of known devices and device components.



Note

DFM monitors supported devices only. To see the device support table for DFM, go to http://www.cisco.com/en/US/products/sw/cscowork/ps2421/products_device_support_tables_list.html.

You can decide how to manage the information about alerts, events, and traps that DFM produces. For example, you can:

- Create views, enabling users to monitor specific groups of devices on the Alerts and Activities display.
- Create subscriptions to send e-mail to users, or syslog and generated SNMP trap notification to systems.
- Determine where to forward traps by configuring the port to which DFM forwards them.
- Determine that DFM will send notifications if the application has been restarted.

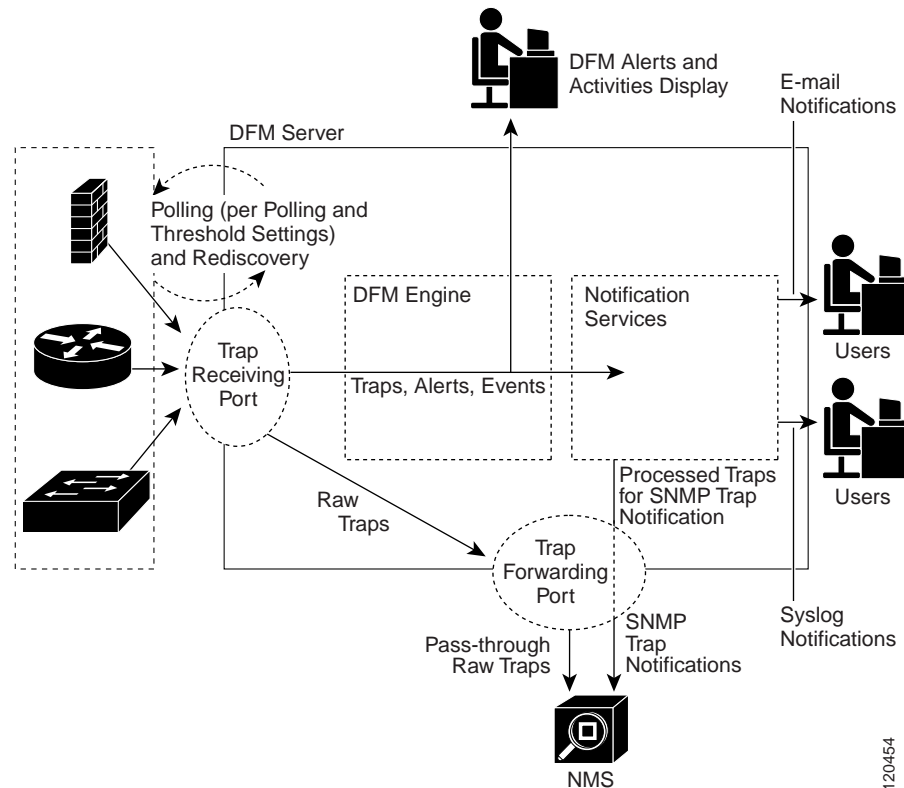
You can also control how often DFM gathers data. DFM receives traps in real time, but you can change the frequency with which DFM performs the following tasks:

- **Polling**—You can change the default polling parameters for device groups, altering the polling interval, timeout, and number of retries.
- **Rediscovery**—You can suspend the default rediscovery schedule and add different rediscovery schedules to fit your circumstances.

DFM Performs Ongoing Monitoring, Analysis, and Notification

DFM continuously gathers information from devices and device components, analyzing and prioritizing events, and raising alerts.

Figure 1-3 DFM Continuously Monitors the Network



DFM generates alerts based on the following activities:

- **Polling**—During polling, DFM identifies conditions that warrant generating an event, such as device unreachable or interface down.
- **Managing thresholds**—After polling, DFM compares the data it collected against threshold values for the devices. If threshold values exceed or do not meet limits, DFM generates the appropriate event.
- **Receiving SNMP traps**—DFM listens for traps on the default port or the port that you have configured for SNMP trap receiving. DFM will process the traps from known, supported devices.

As DFM generates alerts and alert conditions change, DFM determines when to send e-mail or syslog notifications to subscribers and when to generate SNMP traps to send to other systems.

For additional information, see the following topics:

- [MIBs Polled, page A-1](#)
- [Processed and Pass-Through Traps, and Unidentified Traps and Events, page B-1](#)
- [Events Processed, page D-1](#)
- [Polling—SNMP and ICMP, page E-1](#)
- [How DFM Calculates Repeated Restarts and Flapping, page F-1](#)

Users Respond to Notifications and Alerts

Most users will monitor the condition of DFM by using the Alerts and Activities display; others will respond to e-mail. External hosts will receive generated SNMP traps or syslog notifications. [Figure 1-4](#) shows how you can respond using Alerts and Activities.

Figure 1-4 *Users Respond to Alerts*

