



# Polling

---

These topics describe the polling that DFM uses to collect device data:

- [ICMP Polling, page 9-1](#)
- [SNMP Polling, page 9-3](#)

DFM collects data for its analysis using a combination of ICMP and SNMP polling:

- ICMP polling is used to monitor device connectivity.
- SNMP polling is used to collect Fault and performance data (by getting the value of device attributes).

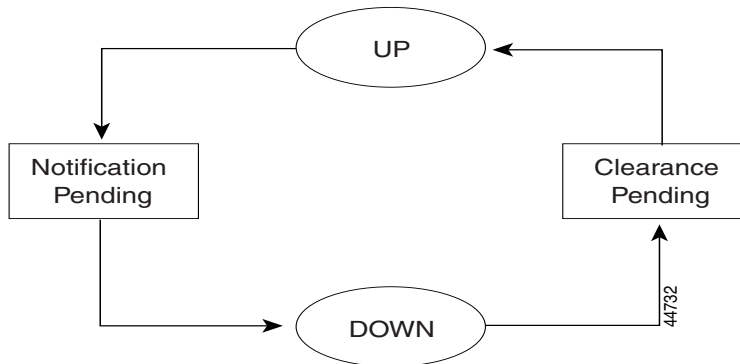
DFM implements SNMP and ICMP polling with cooperative adapters running within a domain manager, combining for a fast and reliable method of obtaining data.

## ICMP Polling

DFM uses a high-performance, asynchronous ICMP poller. The ICMP poller performs at a consistent rate that is independent of poll response times. DFM achieves this using two asynchronous threads; one thread sends polls and one thread receives polls. Because the send and receive threads operate asynchronously, slow response times or excessive timeouts do not affect the polling rate.

Figure 9-1 shows the four possible states of an element as determined by its response to an ICMP poll.

**Figure 9-1 The Four Possible States of an Element During a Polling Cycle**



The four states are: up, notification pending, down, and clear pending.

An element stays in the up state until it fails to respond to an ICMP poll. When it fails to respond, the element moves to the notification pending state until DFM can determine whether it is up or down. If the minimum stabilization period expires or the maximum failure retry count is exceeded before a successful ICMP poll occurs, the element moves to the down state. DFM does not poll the element again until the next scheduled polling cycle.

An element stays in the down state until it responds to an ICMP poll. When the element responds, it moves to the clear pending state. If the maximum success retry count is exceeded or the minimum clear pending time expires, the element returns to the up state.

IP addresses that are unresponsive to ICMP polls are added to a “do not poll” list. The SNMP poller checks this list before sending an SNMP request. For more information, see the [“SNMP Polling” section on page 9-3](#).

### Disabling ICMP Polling

If you have downloaded and installed DFM 1.2 Patch/IDU 1.2.9 or later, you can disable ICMP polling on an IP address without disabling SNMP polling. This means that ICMP will no longer ping the IP address for selected devices, but SNMP will continue to poll for availability monitoring. You can perform bulk unmanage (and manage) operations of this type by creating the appropriate groups in the default System Elements threshold group, and unmanaging those groups.

**Note**

---

Do not unmanage the management IP address (the IP address over which DFM talks to the SNMP agent on the device).

---

- To disable ICMP ping *for a single IP address*, from the Administration Console, select the IP address and right-click **Unmanage**.
- To disable ICMP ping *for a group of IP addresses*, do the following from the Polling and Thresholds Console:
  - a. Select the Thresholds tab.
  - b. Select **System Elements > All Managed IPs**.
  - c. Select the group and right-click **Unmanage**.
  - d. Select **Reconfigure** from the Group menu.
  - e. Select **Save Inventory** from the Inventory menu to update the DFM inventory.

**Note**

---

Managing and unmanaging IP addresses from the Polling and Thresholds Console controls ICMP connectivity polling; it does not affect the managed state of the device in the DFM system, as described in the “[Managing and Unmanaging DFM Inventory Elements](#)” section on page 6-12.

---

To download the latest patch/IDU from the DFM download site, go to <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-dfm>.

## SNMP Polling

The DFM SNMP poller is a synchronous, multi-threaded SNMP polling engine. By default, the SNMP poller uses 10 synchronous polling threads.

The SNMP poller supports SNMP V1 and SNMP V2, which enables the analysis model to use high-capacity 64-bit counters in its analysis. This is critical for performance analysis of high-speed data links where 32-bit counters may wrap between polls.

Polling for devices with multiple IP addresses is supported because the SNMP poller supports multiple IP addresses for each SNMP agent. The SNMP poller automatically switches to an alternate IP address during failures, ensuring the integrity of DFM's analysis during outages.

## Just-In-Time Polling Algorithm

The SNMP poller's MIB variable poll list is driven by a Just-In-Time polling algorithm. This ensures that only those MIB variables needed for analysis are polled. For example, if a port monitored for performance data is disabled, or goes down, the domain manager revokes the SNMP poller's request to monitor performance data for that port and the SNMP poller automatically removes the relevant MIB variables from the poll list. If the port is re-enabled, or comes back up, the variables are automatically put back onto the MIB poll list.

## Consolidated Requests

Issuing a single SNMP GET that requests 10 variables is more efficient than issuing 10 GET requests that each request a single variable. The SNMP poller consolidates as many attributes as possible into a single SNMP GET request. The consolidation is not restricted to variables from the same SNMP table. Polling consolidation continually adapts to changes in the MIB variable poll list.

If recoverable errors are encountered during a GET request, the SNMP poller suspends polling of the affected variable and continues to poll the other variables. For example, a MIB variable might become unavailable due to a configuration change. This enables the SNMP poller to operate efficiently during unexpected changes to a device's configuration.

## Fast ICMP Polling

Synchronous polling has one drawback: an attempt to poll a device that is down reduces polling throughput. This is because the poller must wait for the initial poll and the subsequent retry polls to timeout before polling the next SNMP agent. The problem is exacerbated by the large timeout and retry values that are often required to handle agents that are slow to respond.

DFM eliminates this problem by linking its SNMP and ICMP pollers. DFM avoids sending SNMP requests to agent addresses that are known to be unreachable. Remember, the DFM ICMP poller is asynchronous and does not slow down, even in the face of a total network outage.

IP addresses that are unresponsive to ICMP polls are added to a “do not poll” list. The SNMP poller checks this list before sending an SNMP request. If the SNMP agent address is on the “do not poll” list, the request is not sent. If the SNMP agent has multiple IP addresses, each address is checked against the list. If an alternate address does not appear in the list, the request is sent to that address. If all addresses for an agent are on the list, the agent is deemed unreachable, and all SNMP requests to that agent are temporarily suspended. As soon as an agent's IP address becomes responsive, the address is removed from the list, and SNMP polling resumes. The net effect is that DFM can support large SNMP timeout and retry values without suffering from polling slow-downs during network outages.

