



DFM Inventory Collection

These topics detail how DFM's inventory collection process works:

- [Standard and Cisco MIBs, page 7-1](#)
- [DFM Inventory Collection Probes for Standard MIBs, page 7-2](#)
- [DFM Inventory Collection Errors, page 7-9](#)
- [Discovery Error and Devices Not Supporting SNMP, page 7-11](#)
- [Duplicate IP Address Error, page 7-12](#)

DFM inventory collection creates a representation of the managed inventory within a domain manager's repository. Data is collected using SNMP to create instances of the managed devices and their internal components. Internal components can include chassis, cards, ports, interfaces, power supplies, and environmental test points.

See [Appendix B, "MIBs Polled and SNMP Traps Processed or Passed-Through by DFM"](#) for additional information.

Standard and Cisco MIBs

It is often necessary to use Cisco MIBs in order to fully inventory a device. In some cases, standardized MIBs, such as MIB-II, do not contain tables for representing certain elements that DFM is able to manage. For example, MIB-II does not represent processor or memory elements. In these cases, Cisco MIBs offer more detailed information.

For example, the MIB-II ifTable in a Cisco Catalyst 5500 contains an entry for each port. However, the duplex setting for each port is only available from the proprietary portTable within the CISCO-STACK MIB.

**Note**

When a device is imported into DFM, basic polling information is obtained, and displayed when you refresh the display. However, if the device belongs to a group without any settings, the device is not polled, so the device information is not updated.

DFM Inventory Collection Probes for Standard MIBs

DFM's inventory collection is performed by a multi-threaded adapter that runs within a domain manager. Inventory collection is divided among several probes, each of which is responsible for collecting a piece of the overall inventory:

- [System Information Probe, page 7-2](#)
- [Containment Probe, page 7-7](#)
- [IP Network Probe, page 7-8](#)
- [VLAN Probe, page 7-8](#)
- [Neighbor Probe, page 7-8](#)

For a complete list of MIBs polled, refer to [Appendix B, “MIBs Polled and SNMP Traps Processed or Passed-Through by DFM.”](#)

System Information Probe

The main tasks of the System Information Probe are to determine whether a device is certified and to uniquely identify the device. The System Information Probe accesses the device to retrieve the following MIB-II attributes: sysObjectID, sysName, sysLocation, sysContact and ipAdEntIfIndex.

If the device does not respond to the probe's SNMP query, the domain manager classifies the device as Undiscovered and does not perform any further discovery for the device. The domain manager also sets the status of the device to

unmanaged, meaning that the device will not be monitored. For information regarding the managed/unmanaged status of a device, see the [“Managing and Unmanaging DFM Inventory Elements”](#) section on page 6-12.

If the SNMP query returns successfully, the System Information Probe checks if the sysObjectID of the device is present in the oid2type.conf configuration file. The oid2type.conf file lists the types of device that DFM has knowledge of. The domain manager classifies each device according to the level of support DFM provides, as indicated by the oid2type.conf file. This is referred to as the device’s certification, which can be determined by checking the status of the device’s Certification attribute. There are five levels of certification:

Table 7-1 Levels of Device Certification

Level of Certification	Description
Validated	The highest level of certification. A validated device is listed in the oid2type.conf file and is a device with which DFM has been field tested.
Certified	The device is listed in the oid2type.conf file. DFM will use the information in the publicly available MIBs to perform discovery.
Template	The device is listed in the oid2type.conf file but that DFM has no information about the MIBs this device supports.
Undiscovered	DFM has not fully inventoried this device because an inventory collection error occurred. For information regarding inventory collection errors, see the “DFM Inventory Collection Errors” section on page 7-9.
Uncertified	The device has a sysObjectID that is not listed in the oid2type.conf file. Uncertified devices are displayed in the Polling and Thresholds Console under the Uncertified Systems groups.

Validated and certified devices are supported by DFM.

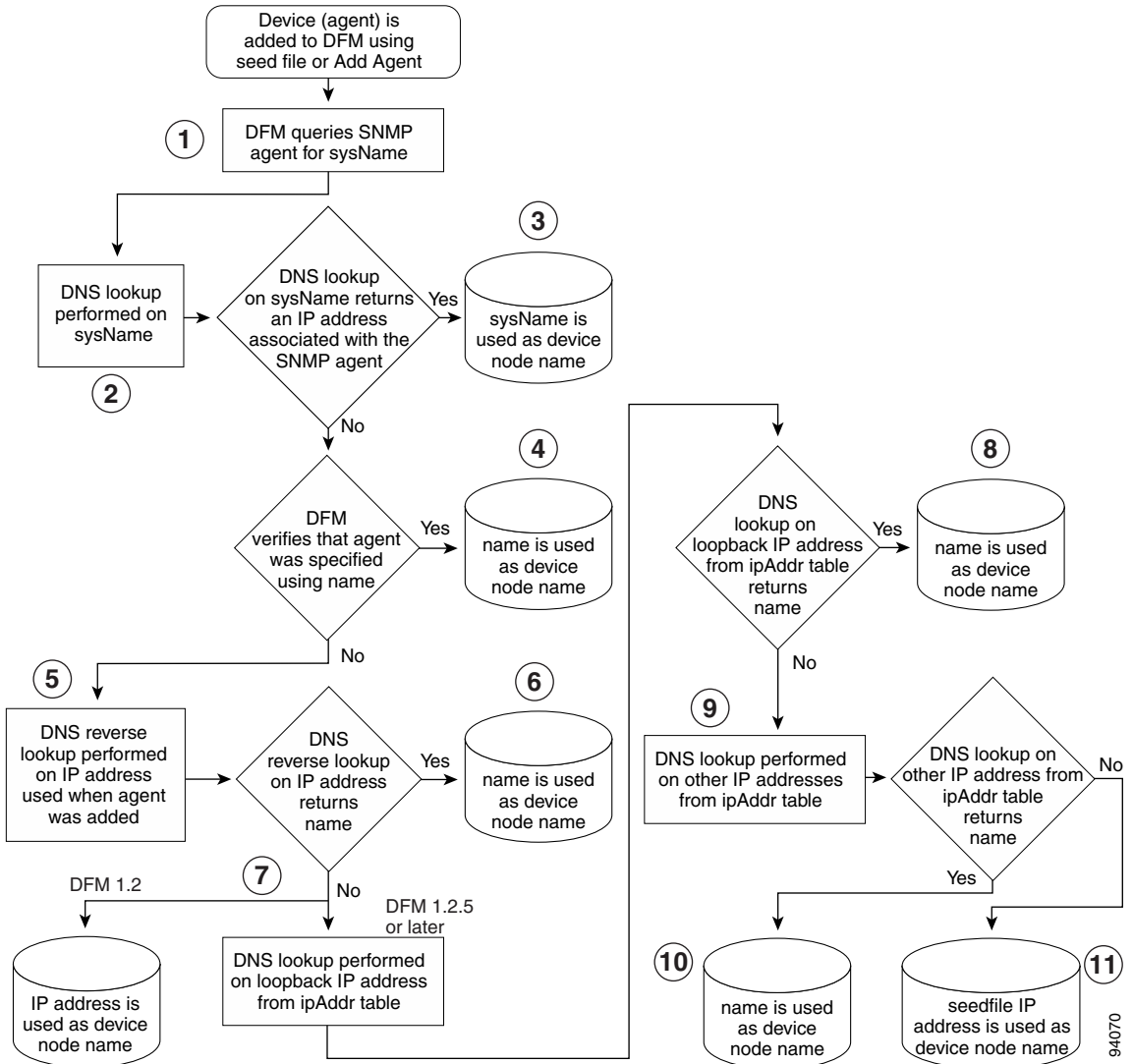
The `oid2type.conf` file also specifies how DFM should classify a recognized system (switch, router, hub, bridge, or host). The System Information Probe uses the class specified in the `oid2type.conf` as the device type. For example, DFM classifies a device as a Router if the `oid2type.conf` lists Router as the class for that device's `sysObjectID`.

DFM Name Resolution

The System Information Probe is also responsible for providing a unique identifier for the device. A device can be discovered either from a seed file or by using Add Agent from the DFM consoles.

[Figure 7-1](#) illustrates the algorithm used to assign a name (*node name*) to a discovered device. The goal of this algorithm is to provide DFM with a unique identifier that is always DNS-resolvable. [Figure 7-1](#) also illustrates why it is important that when devices are added to DFM, they should be specified using DNS-resolvable names, whether it is a seed file name, an Add Agent dialog value, or `sysName`.

Figure 7-1 DFM Name Resolution Algorithm



94070

As illustrated in [Figure 7-1](#), DFM resolves names as follows:

1	DFM obtains a value of sysName for the device SNMP agent.
2	DFM tries to resolve sysName and obtain the IP address from DNS:
3	If the DNS lookup for sysName succeeds and returns an IP address (or addresses) associated with the SNMP agent, sysName becomes node name.
4	If the DNS lookup for sysName fails, DFM checks to see if either the seedfile or the Add Agent procedure specified the device as a name. If either of them did, the seedfile name becomes node name.
5	If the DNS lookup for sysName fails and the device was not specified as a name, DFM checks to see if either the seedfile or the Add Agent procedure specified the device as an IP address. If either of them did, DFM tries to resolve the IP address using DNS:
6	If the DNS lookup for the IP address succeeds and returns a name, this name becomes node name.
7	If the DNS lookup for the IP address fails: <ul style="list-style-type: none"> • For DFM 1.2, the seedfile IP address becomes node name. • For DFM 1.2 with IDU 1.2.5 (or later), DFM tries to resolve a loopback IP address from the ipAddr table (as described in the next step).
8	If the DNS lookup for loopback IP address from the ipAddr table succeeds, the DNS name for the loopback IP address becomes node name.
9	If the DNS lookup for the loopback IP address from the ipAddr table fails, DNS attempts to resolve a different IP address from the ipAddr table.
10	If DNS resolves a different IP address from the ipAddr table, the DNS name for the resolveable IP address from the ipAddr table becomes nodename.
11	If DNS cannot resolve any other IP addresses from the ipAddr table, the seedfile IP address becomes node name.

DFM Name Resolution for Windows Devices Using NetBios

As [Figure 7-1](#) illustrates, after a device is added, DFM queries the SNMP agent for sysName, and a DNS lookup is performed on sysName (indicated by an asterisk in the diagram). Windows can be configured to use NetBios over TCP/IP. If NetBios over TCP/IP is used and a DNS lookup fails, the Windows name resolver continues searching using NetBios name resolution. As a result, certain hosts (either Windows-based hosts or Windows-based router cards, such as the Cisco CallManager) might be named according to their NetBios names. These names might not immediately correspond to any IP address or DNS name, which could lead to initial confusion. Additionally, in certain cases the NetBios name resolution might depend on device status; for example, if a device is up and responding to NetBios name queries, its name will be resolved.

To avoid confusion on Windows, disable NetBios over TCP/IP on any Windows servers running DFM. If this solution is unacceptable, make sure NetBios names are consistent with the DNS naming scheme.

DFM Name Resolution for Devices Using Aliases

Under certain circumstances, DFM will resolve a device name to the device alias rather than the DNS name. This occurs in the following scenarios:

- On Solaris, if a Solaris machine has been configured to use the hosts file before using DNS. (This would be specified on the Solaris `/etc/nsswitch.conf` file, which determines precedence for the name resolution method.)
- On Windows, if a machine alias is specified in the Windows hosts file. In this case, the alias will always take precedence over the DNS name.

Containment Probe

The main task of the Containment Probe is to discover the components of a device, including: interfaces, ports, MAC addresses, and cards or modules.

The Containment Probe queries the following MIB variables: `ipAdEntIfIndex`, `ifType`, `ifDescr`, `ifSpeed`, `ifMtu`, `ifPhysAddress`, and `ifName`. If the Containment Probe has access to proprietary MIBs, it queries additional variables. For switches or bridges, the probe also queries the `dot1dBasePortIfIndex` MIB variable. Again, if the probe has access to proprietary MIBs, it queries additional variables.

The probe creates an interface in the domain manager's inventory for each `ifName` it discovers and fills out information about the interface using the corresponding `ifType`, `ifDescr`, `ifSpeed`, and `ifMTU` MIB variables. The probe also creates relationships between a device and its interfaces.

The Containment Probe creates a MAC managed element to represent the `ifPhysAddress` and to establish the relationship between an interface and its MAC address. For each `ipAdEntIfIndex` associated with an interface, the probe creates an instance of the class IP and the relationship between the interface and its IP addresses.

IP Network Probe

The main task of the IP Network Probe is to discover IP network connectivity and to find IP addresses configured on a system. The probe queries the following MIB variables: `ipAdEntAddr`, `ipAdEntIfIndex`, and `ipAdEntNetMask`.

VLAN Probe

The VLAN Probe Collects VLAN information from switches including VLAN identifiers, VLAN trunks, and VLAN port memberships.

Neighbor Probe

The Neighbor Probe collects additional inter-device connectivity information using proprietary topology MIBs such as the Cisco CDP MIB.

DFM Inventory Collection Errors

When DFM discovers your network at runtime, the process is monitored to record errors that occur during the probe. If an error is encountered, DFM is unable to inventory the device and a `DiscoveryError` notification is sent for that device. There are two types of errors that can occur during inventory collection:

- The request to the SNMP agent times out. The device may be busy, the link to the system may be too slow, the Read Community string for the agent may be incorrect, or the device may not support SNMP. (For information on changing a device community string in DFM, refer to the [“Adding Devices to the Managed Inventory”](#) section on page 6-2. For more information regarding devices that do not support SNMP, see the [“Discovery Error and Devices Not Supporting SNMP”](#) section on page 7-11.)
- The SNMP agent has an improper MIB implementation, which causes SNMP requests to loop over a table.

Inventory collection errors are displayed in the Monitoring Console. To view more information about a `DiscoveryError`, double-click on the event in the alarm log to open the Notification Properties window.

**Note**

Once a device is successfully discovered, the domain manager attributes errors in reaching the device’s SNMP agent to other causes, according to the set of available symptoms. Other causes include: the SNMP agent is unreachable because of network problems, the SNMP agent is down, or the system hosting the agent has failed.

The following table describes the actions taken by the inventory collection probe for different scenarios. The term “Initial inventory collection” indicates an attempt to probe a system where inventory collection has not successfully occurred. This includes systems being inventoried for the first time and systems for which previous attempts failed because there was no response to SNMP requests. The term “Subsequent inventory collection” indicates an attempt to reprobe a system that was previously inventoried successfully.

**Note**

If a link or device is slow, DFM may only partially rediscover the device, and will not move the device to the Undiscovered class. To avoid this problem, adjust the device polling interval and timeout.

Table 7-2 Inventory Collection Scenarios and Their Outcome

Inventory Collection Phases	Inventory Collection Scenarios	Results
Initial inventory collection	No response from SNMP agent.	Classify device as Undiscovered and send DiscoveryError notification.
	Unknown OID from Cisco.	Classify device as Uncertified and probe device with standard MIB-II probes.
	Unknown OID from unsupported vendor.	Classify device as Unsupported.
	Receive initial SNMP response but probe does not successfully complete.	Classify device according to its sysObjectID and send DiscoveryError notification.
	Receive initial SNMP response and probe completes successfully.	Classify device according to its sysObjectID and clear DiscoveryError notifications from previous attempts (if any).
	No response from initial SNMP probe. Value of SupportsSNMP attribute is FALSE.	Classify device as Host and clear DiscoveryError notification.
Subsequent inventory collection	No response from SNMP agent.	No action. Probe defers to notifications from the analysis.
	Unknown OID from Cisco.	Reclassify device as Uncertified.
	Unknown OID from unsupported vendor.	Reclassify device as Unsupported.
	Receive initial SNMP response but probe does not successfully complete.	Send DiscoveryError notification.

Discovery Error and Devices Not Supporting SNMP

DFM's inventory collection process assumes that the devices to be managed support SNMP. Therefore, a `DiscoveryError` is notified when the inventory collection probe does not receive a response from a device's SNMP agent during initial inventory collection.

Certain systems, such as PC workstations, do not usually support SNMP. You can prevent DFM from generating `DiscoveryError` notifications for such devices by changing the value of the device's `SupportsSNMP` attribute.

To change the value of a device's `SupportsSNMP` attribute:

-
- Step 1** Expand the `Undiscovered` class in the left panel of the Inventory Browser.
 - Step 2** Select the device that you want to change the status of.
 - Step 3** In the right panel of the Inventory Browser, select the `Attributes` tab and find the `SupportsSNMP` attribute.
 - Step 4** Double-click on the `Value` field of the `SupportsSNMP` attribute and select **FALSE** from the drop-down menu.
 - Step 5** Click **Apply**.
 - Step 6** Select **Rediscover** from the Inventory menu.
-

When DFM reprobes the device, it checks the status of the device's `SupportsSNMP` attribute. Because this attribute is set to `FALSE`, DFM classifies the device as a host and does not manage it.

Duplicate IP Address Error

If the same IP address is configured on multiple systems and the systems are managed by DFM, DFM discovers the systems and:

1. Classifies the IP address as duplicateIP.
2. Disables all other IP-related notifications for the IP address.

From the Monitoring Console or Administration Console, you can determine which devices have the duplicate IP addresses by:

- Using the Alarm Log view:
 - Double-click the Duplicate notification in the Alarm Log. The Notification Properties window opens.
 - Choose the Details tab.
- Using the Inventory Browser view:

**Note**

This is the best method to use if more than two devices have duplicate IP addresses.

- Browse DuplicateIP.
- If DuplicateIP is not visible, right-click in the browser view and choose **Show All**.
- Expand and examine the view to locate all devices the IP is DuplicatedBy.

To correct a duplicate IP address error:

-
- Step 1** Reconfigure your devices to use unique IP addresses with no duplicates.
- Step 2** From the Administration Console, delete the DuplicateIP object from the Inventory Browser view by selecting the object, right-clicking it, and choosing **Delete**.
- Step 3** Rediscover all devices involved in the error.
-

**Note**

If you do not correct the problem, you can still clear the Notification by unmanaging the duplicate IP addresses. Refer to the [“How to Manage or Unmanage Elements”](#) section on page 6-16.

**Caution**

If an IP address has been discovered on one device and is subsequently discovered as a second device's only SNMP agent address, DFM will not discover the second device, nor will DFM report a discovery or duplicate IP error for the second device.

■ Duplicate IP Address Error