CHAPTER 1

# Getting Started

This chapter covers:

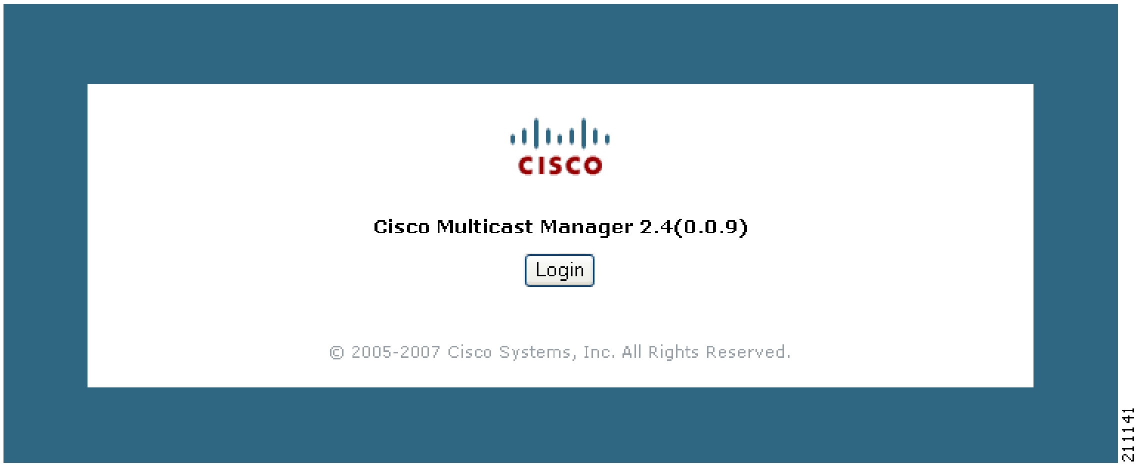
- Logging Into Cisco Multicast Manager, page 1-1
- Overview, page 1-2
- Creating a Domain, page 1-3
- Discovering Your Network, page 1-6

## Logging Into Cisco Multicast Manager

**Note** For details on stopping and starting Cisco Multicast Manager on Solaris and Linux, see the *Installation Guide for the Cisco Multicast Manager 2.4*.

To access CMM, enter the IP address or the name of the server where the software is installed. For example: http://172.16.0.1:8080. The default port of 8080 can be changed as described in the installation instructions.

***Figure 1-1 Cisco Multicast Manager Login Page***



Cisco Multicast Manager 2.4(0.0.9)

© 2005-2007 Cisco Systems, Inc. All Rights Reserved.

To enter CMM, click **Login**. You are prompted for a username and a password. The default CMM username is *admin*, and the default CMM password is *rmsmmt*.

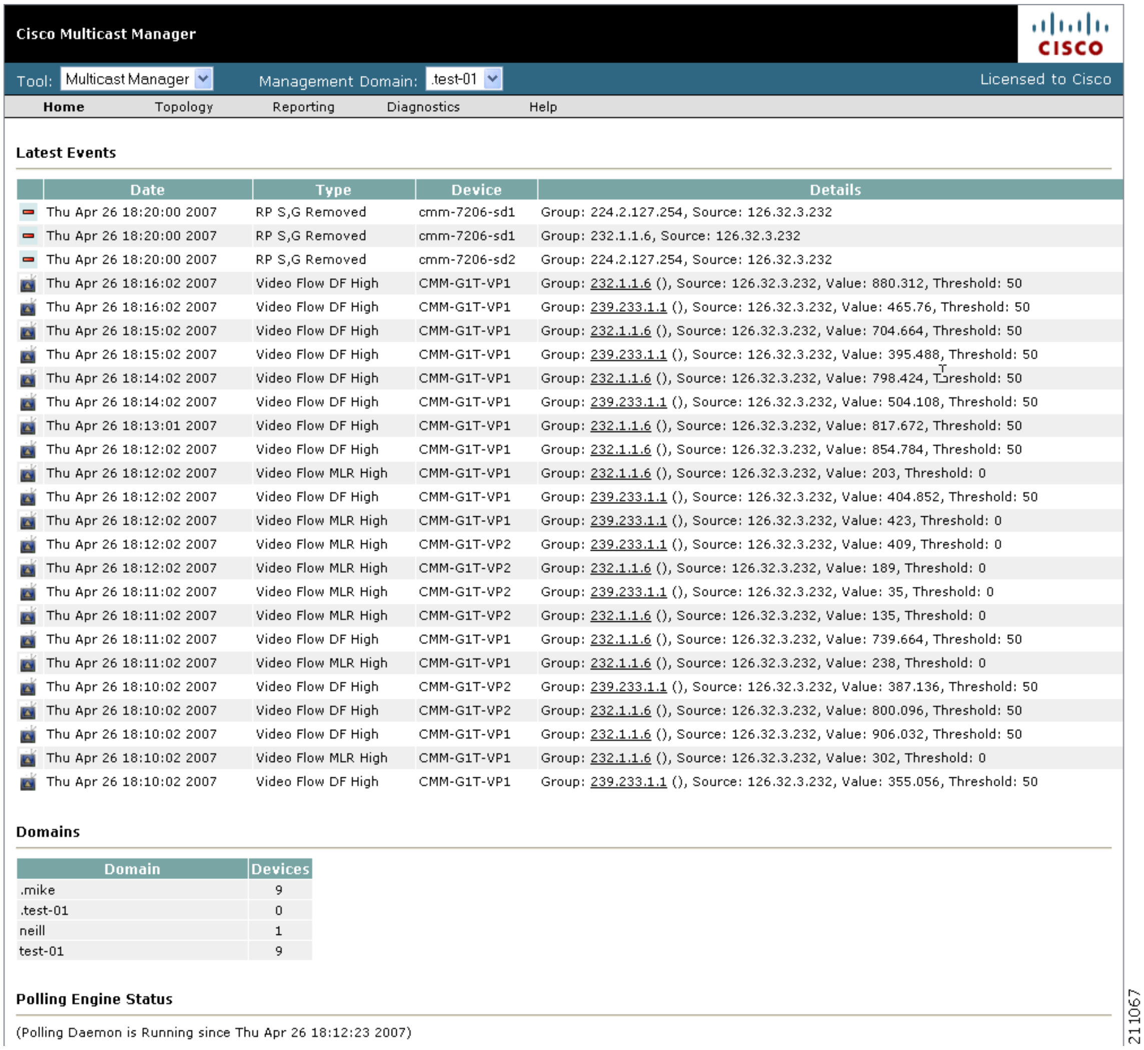
# Overview

Cisco Multicast Manager has two main tools: **Administration** and **Multicast Manager**. You can select either tool from the menu at the upper left of Cisco Multicast Manager Web interface. You can perform the following tasks with each tool:

| Tool | Tasks | Information |
|---|---|---|
| **Administration** | Manage domains | Creating a Domain, page 1-3 |
| | Use administrative utilities | Using Administrative Utilities, page 2-1 |
| | Configure security | Configuring System Security, page 2-4 |
| | Manage users | Managing Users and Passwords, page 2-5 |
| | Perform discovery | Discovering Your Network, page 1-6 |
| | Configure devices | Configuring Devices and Probes, page 2-7 |
| | Configure global polling | Configuring Global Polling, page 2-16 |
| | Configure multicast polling | Configuring Specific Multicast Manager Polling, page 2-26 |
| | Manage addresses | Managing Device Addresses, page 2-21 |
| **Multicast Manager** | View events through the **Home** page | • Viewing the Multicast Manager Home Page, page 3-1<br>• Latest Events, page 3-7 |
| | View **Topology** | Viewing Topology, page 3-2 |
| | Manage **Reporting** | Managing Reports, page 3-6 |
| | Manage **Diagnostics** | Managing Diagnostics, page 4-1 |
| | View **Help** | Viewing User Guide Help, page 4-28 |

When you first log into Cisco Multicast Manager, the Multicast Manager home page appears.

*Figure 1-2 Multicast Manager Home Page*



Latest Events

| | Date | Type | Device | Details |
|---|---|---|---|---|
| ▬ | Thu Apr 26 18:20:00 2007 | RP S,G Removed | cmm-7206-sd1 | Group: 224.2.127.254, Source: 126.32.3.232 |
| ▬ | Thu Apr 26 18:20:00 2007 | RP S,G Removed | cmm-7206-sd1 | Group: 232.1.1.6, Source: 126.32.3.232 |
| ▬ | Thu Apr 26 18:20:00 2007 | RP S,G Removed | cmm-7206-sd2 | Group: 224.2.127.254, Source: 126.32.3.232 |
| ▣ | Thu Apr 26 18:16:02 2007 | Video Flow DF High | CMM-G1T-VP1 | Group: 232.1.1.6 (), Source: 126.32.3.232, Value: 880.312, Threshold: 50 |
| ▣ | Thu Apr 26 18:16:02 2007 | Video Flow DF High | CMM-G1T-VP1 | Group: 239.233.1.1 (), Source: 126.32.3.232, Value: 465.76, Threshold: 50 |
| ▣ | Thu Apr 26 18:15:02 2007 | Video Flow DF High | CMM-G1T-VP1 | Group: 232.1.1.6 (), Source: 126.32.3.232, Value: 704.664, Threshold: 50 |
| ▣ | Thu Apr 26 18:15:02 2007 | Video Flow DF High | CMM-G1T-VP1 | Group: 239.233.1.1 (), Source: 126.32.3.232, Value: 395.488, Threshold: 50 |
| ▣ | Thu Apr 26 18:14:02 2007 | Video Flow DF High | CMM-G1T-VP1 | Group: 232.1.1.6 (), Source: 126.32.3.232, Value: 798.424, Threshold: 50 |
| ▣ | Thu Apr 26 18:14:02 2007 | Video Flow DF High | CMM-G1T-VP1 | Group: 239.233.1.1 (), Source: 126.32.3.232, Value: 504.108, Threshold: 50 |
| ▣ | Thu Apr 26 18:13:01 2007 | Video Flow DF High | CMM-G1T-VP1 | Group: 232.1.1.6 (), Source: 126.32.3.232, Value: 817.672, Threshold: 50 |
| ▣ | Thu Apr 26 18:12:02 2007 | Video Flow DF High | CMM-G1T-VP1 | Group: 232.1.1.6 (), Source: 126.32.3.232, Value: 854.784, Threshold: 50 |
| ▣ | Thu Apr 26 18:12:02 2007 | Video Flow MLR High | CMM-G1T-VP1 | Group: 232.1.1.6 (), Source: 126.32.3.232, Value: 203, Threshold: 0 |
| ▣ | Thu Apr 26 18:12:02 2007 | Video Flow DF High | CMM-G1T-VP1 | Group: 239.233.1.1 (), Source: 126.32.3.232, Value: 404.852, Threshold: 50 |
| ▣ | Thu Apr 26 18:12:02 2007 | Video Flow MLR High | CMM-G1T-VP1 | Group: 239.233.1.1 (), Source: 126.32.3.232, Value: 423, Threshold: 0 |
| ▣ | Thu Apr 26 18:12:02 2007 | Video Flow MLR High | CMM-G1T-VP2 | Group: 239.233.1.1 (), Source: 126.32.3.232, Value: 409, Threshold: 0 |
| ▣ | Thu Apr 26 18:12:02 2007 | Video Flow MLR High | CMM-G1T-VP2 | Group: 232.1.1.6 (), Source: 126.32.3.232, Value: 189, Threshold: 0 |
| ▣ | Thu Apr 26 18:11:02 2007 | Video Flow MLR High | CMM-G1T-VP2 | Group: 239.233.1.1 (), Source: 126.32.3.232, Value: 35, Threshold: 0 |
| ▣ | Thu Apr 26 18:11:02 2007 | Video Flow MLR High | CMM-G1T-VP2 | Group: 232.1.1.6 (), Source: 126.32.3.232, Value: 135, Threshold: 0 |
| ▣ | Thu Apr 26 18:11:02 2007 | Video Flow DF High | CMM-G1T-VP1 | Group: 232.1.1.6 (), Source: 126.32.3.232, Value: 739.664, Threshold: 50 |
| ▣ | Thu Apr 26 18:11:02 2007 | Video Flow MLR High | CMM-G1T-VP1 | Group: 232.1.1.6 (), Source: 126.32.3.232, Value: 238, Threshold: 0 |
| ▣ | Thu Apr 26 18:10:02 2007 | Video Flow DF High | CMM-G1T-VP2 | Group: 239.233.1.1 (), Source: 126.32.3.232, Value: 387.136, Threshold: 50 |
| ▣ | Thu Apr 26 18:10:02 2007 | Video Flow DF High | CMM-G1T-VP2 | Group: 232.1.1.6 (), Source: 126.32.3.232, Value: 800.096, Threshold: 50 |
| ▣ | Thu Apr 26 18:10:02 2007 | Video Flow DF High | CMM-G1T-VP1 | Group: 232.1.1.6 (), Source: 126.32.3.232, Value: 906.032, Threshold: 50 |
| ▣ | Thu Apr 26 18:10:02 2007 | Video Flow MLR High | CMM-G1T-VP1 | Group: 232.1.1.6 (), Source: 126.32.3.232, Value: 302, Threshold: 0 |
| ▣ | Thu Apr 26 18:10:02 2007 | Video Flow DF High | CMM-G1T-VP1 | Group: 239.233.1.1 (), Source: 126.32.3.232, Value: 355.056, Threshold: 50 |

Domains

| Domain | Devices |
|---|---|
| .mike | 9 |
| .test-01 | 0 |
| neill | 1 |
| test-01 | 9 |

Polling Engine Status

(Polling Daemon is Running since Thu Apr 26 18:12:23 2007)

For detailed information on this window, see the "Viewing the Multicast Manager Home Page" section on page 3-1.

# Creating a Domain

Before you can begin managing your networks, you must create a domain. A domain is a collection of multicast routers. Multiple domains may exist, and routers can belong to multiple domains. Using Domain Management, you can create and edit domains.

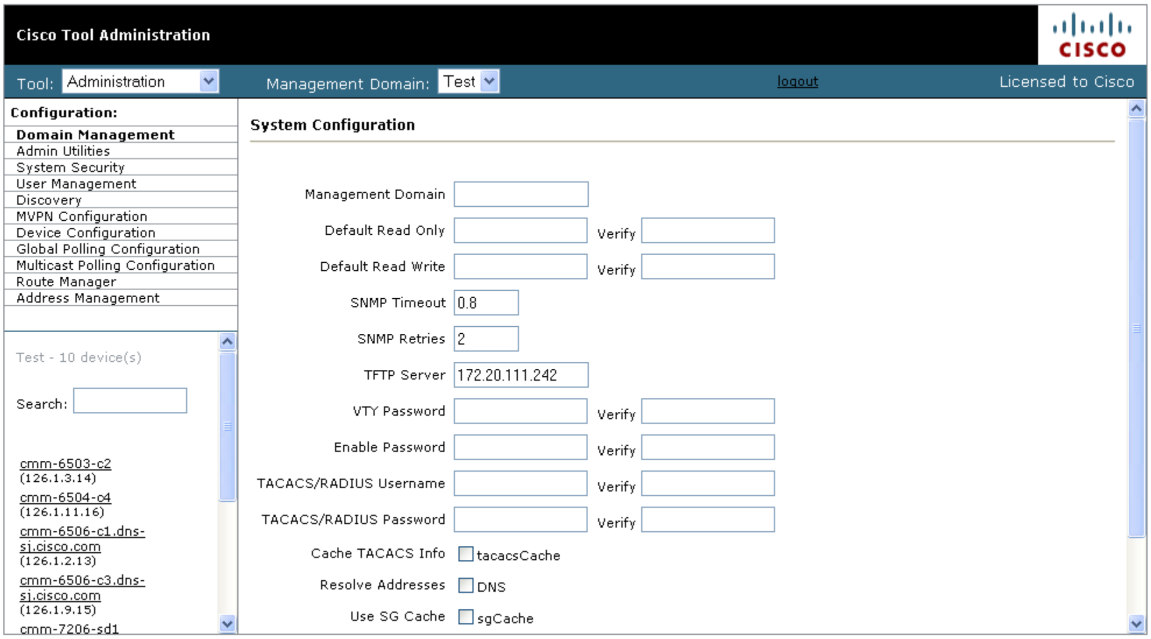
To create a domain:

**Step 1** From the Multicast Manager home page, select the **Administration** tool.

**Step 2** Select **Domain Management**.

**Step 3** Select **add a new domain**. The System Configuration page appears.

***Figure 1-3 System Configuration Page***



System Configuration

Management Domain

Default Read Only  Verify

Default Read Write  Verify

SNMP Timeout 0.8

SNMP Retries 2

TFTP Server 172.20.111.242

VTY Password  Verify

Enable Password  Verify

TACACS/RADIUS Username  Verify

TACACS/RADIUS Password  Verify

Cache TACACS Info ☐ tacacsCache

Resolve Addresses ☐ DNS

Use SG Cache ☐ sgCache

**Step 4** Complete the fields in the System Configuration page and click **Save** to continue and create the new domain. Click **Cancel** to exit without creating a domain.

The System Configuration page contains the following fields:

| Field | Description |
|---|---|
| Management Domain | A management domain is defined as a contiguous group of PIM neighbors sharing the same SNMP community string. |
| Default Read Only | SNMP read-only community string. |
| Default Read Write | SNMP read-write community string. This is required for retrieving and validating device configurations. |
| SNMP Timeout | Retry period if node does not respond. Default value is 0.8. |
| SNMP Retries | Number of retries to contact a node before issuing a timeout. Default value is 2. |
| TFTP Server | TFTP server IP address. Default is the IP address of Cisco Multicast Manager server. |
| VTY Password | The VTY password is required if you want to issue show commands from the application. Certain features, such as querying Layer 2 switches, also require this. If TACACS is being used, then a username and password can be supplied instead of the VTY password. |
| Enable Password | (*Not currently used.*) |
| TACACS/RADIUS Username | If you are using TACACS/RADIUS then you can enter a username here. See VTY Password above.<br>**Note** If you enter a TACACS/RADIUS username and password here, the application will use these values regardless of who is currently logged in. Users can also enter their own username and password when issuing show commands. |
| TACACS/RADIUS Password | If you are using TACACS/RADIUS then you can enter a password here. See VTY Password above.<br>**Note** If you enter a TACACS/RADIUS username and password here, the application will use these values regardless of who is currently logged in. Users can also enter their own username and password when issuing show commands. |
| Cache TACACS Info | If this box is checked, CMM will cache the TACACS username and password until the browser is closed. This eliminates having to enter the username and password each time you issue a router command from the application. |

| Field | Description |
|---|---|
| Resolve Addresses | Performs DNS lookups on all sources found. The DNS name appears alongside the IP address on the “Show All Groups” screen. If the server is not configured for DNS, then DO NOT check the box. If the box is checked, you may receive a slower response, due to the fact that the application is trying to resolve names. This option is not recommended if your network contains a large number of S,Gs. The Resolve Addresses option also causes discovery to do a reverse DNS lookup on a device name. The IP address returned by DNS is then used for management purposes. Otherwise, the IP address by which the device is found is used for management purposes. |
| Use SG Cache | Some networks contain thousands of sources and groups (S,G)s. During discovery, CMM caches all the S,Gs found in the RPs. If this box is checked, CMM reads the SG cache when showing lists of sources and groups, rather then retrieving them again from the RPs in the network. The cache is automatically refreshed if RPs are being polled as described later in this document (see the “RP Polling” section on page 2-26). The cache can also be refreshed manually by clicking the **Refresh Cache** button in the Multicast Diagnostics window (see the “Show All Groups” section on page 4-2). This button appears only if you have the **Use SG Cache** option selected. It is highly recommended to use the SG cache option. If there are no RPs in the domain being discovered, then the SG cache is created by querying all the devices that have been discovered, as would be the case in a PIM Dense-Mode network. In this case, the SG cache is updated only when you click the **Refresh Cache** button. |

# Discovering Your Network

**Note** If you are upgrading from CMM 2.3, you must run discovery to access new features.

After you have created a domain, the second step in using Cisco Multicast Manager is to discover your network using one of these choices, found within the **Discovery** menu:

- Adding Layer 2 Switches to Discovery, page 1-7

- Adding Video Probes, page 1-8
- Performing Multicast Discovery, page 1-12
- Adding or Rediscovering a Single Device, page 1-13

The discovery process is multicast-specific and finds only devices that are PIM-enabled. CMM builds a database of all found devices. Discovery adds support for multiple community strings per domain, along with device-specific SNMP timeout and retries.

**Note** If any new routers or interfaces are added to the network, run discovery again so that the database is consistent with the network topology.

A single router may also be added or rediscovered on the network. A router being added must have a connection to a device that already exists in the database. A router that is being rediscovered is initially removed from the database, along with any neighbors that exist in the database. The router and its neighbors are then added back into the database. This option would be used if a change on a device has caused a change in the SNMP ifIndexes.

**Note** When possible, use the SNMP **ifindex persist** command on all devices.

# Adding Layer 2 Switches to Discovery

Layer 2 switches are not included in discovery and must be added manually. You can add switches individually, or you can import a list of switches in a CSV file.

To add switches individually, enter the switch name or IP address and the community string, then click **Add**.

To import a list of switches:

**Step 1** Create a text file by typing:

```
#import file format switch IP address or switch name
# this line will be skipped
switchA
192.168.1.1, public
switchC
10.10.10.1, public
```

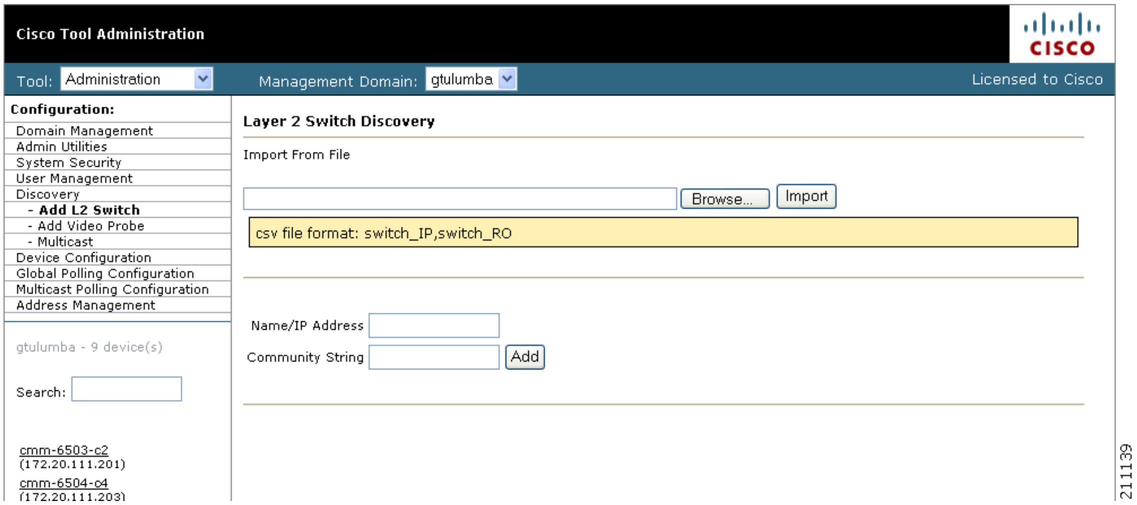
**Step 2** Save the file.

**Step 3** Within the Administration tool, select **Discovery**.

**Step 4** Select **Add L2 Switch**.

The Multicast Layer 2 Switch Configuration page appears.

***Figure 1-4 Multicast Layer 2 Switch Configuration***



csv file format: switch_IP,switch_RO

**Step 5** Click **Browse**. Open the file you created.

**Step 6** Click **Import**.

# Adding Video Probes

Configuring a video probe consists of these steps:

1. Gathering the IP addresses and names of the probes.

   Obtain the IP addresses and names of the probes that you will monitor.

2. Inputting a list of probes.

   You can add probes manually, using the Cisco Multicast Manager interface or by importing a CSV that includes a list of the probes that you want to monitor.

   – For information on adding probes manually, see Adding Video Probes Manually, page 1-9.

   – For information on importing probes listed in a text file, see Importing a List of Probes, page 1-11.

3. Setting up monitoring for the probes.

   For information on setting up monitoring for probes, see the following sections in Chapter 2, “Configuring with the CMM Administration Tool.”

   – Editing Basic Probe Parameters, page 2-14

   – Configuring Global Polling, page 2-16

   – Video Probe Polling, page 2-48

4. If needed, setting up a trap collector or email alerts.

- For information on setting up a trap receiver and email addresses see, Configuring Domain-Specific Trap Receivers and Email Addresses, page 2-20.

Cisco Multicast Manager can monitor the status and video quality of video streams delivered over the multicast network by using video probes that show activity on specified devices or routes.

You can specify a video probe to monitor in two ways:

- Manually, by entering the probes in the Video Probe Discovery page
- By importing a list of probes contained in a text file.

**Note** You must compile Cisco Multicast Manager MIBs into your NMS station. The MIBS are located in the following directories:

/opt/RMSMMT - solaris
/usr/local/netman - Linux

RMS-MMT-V1SMI.my
RMS-MMT.mi2
RMS-MMT.my

## Adding Video Probes Manually

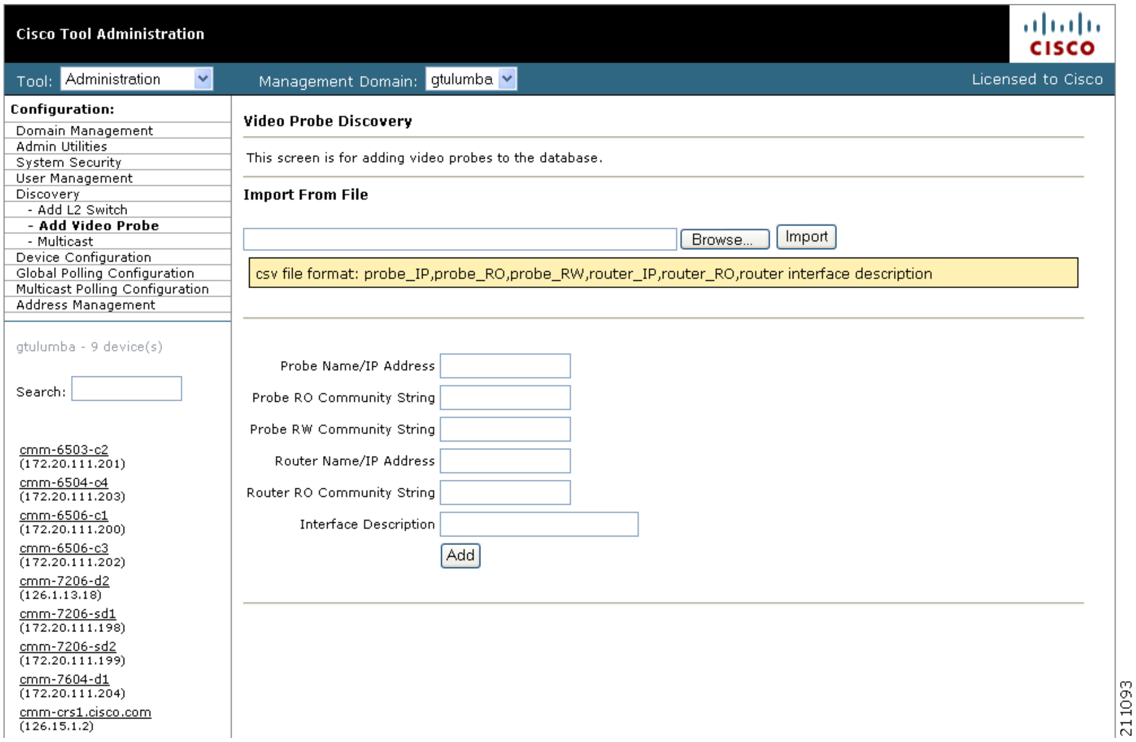
To add a video probe manually:

**Step 1** Within the administration tool, select **Discovery**.

**Step 2** Select **Add Video Probe**.

The Video Probe Discovery page appears, as shown in Figure 1-5.

*Figure 1-5 Video Probe Discovery Configuration Page*



Cisco Tool Administration

Tool: Administration    Management Domain: gtulumba    Licensed to Cisco

Configuration:
Domain Management
Admin Utilities
System Security
User Management
Discovery
- Add L2 Switch
- **Add Video Probe**
- Multicast
Device Configuration
Global Polling Configuration
Multicast Polling Configuration
Address Management

gtulumba - 9 device(s)

Search:

cmm-6503-c2 (172.20.111.201)
cmm-6504-c4 (172.20.111.203)
cmm-6506-c1 (172.20.111.200)
cmm-6506-c3 (172.20.111.202)
cmm-7206-d2 (126.1.13.18)
cmm-7206-sd1 (172.20.111.198)
cmm-7206-sd2 (172.20.111.199)
cmm-7604-d1 (172.20.111.204)
cmm-crs1.cisco.com (126.15.1.2)

**Video Probe Discovery**

This screen is for adding video probes to the database.

**Import From File**

Browse... Import

csv file format: probe_IP,probe_RO,probe_RW,router_IP,router_RO,router interface description

Probe Name/IP Address
Probe RO Community String
Probe RW Community String
Router Name/IP Address
Router RO Community String
Interface Description

Add

**Step 3** Complete the fields in the Video Probe Discovery page.

| Field | Description |
|---|---|
| Probe Name/IP Address | Enter the name or the IP address of the video probe. |
| Probe RO Community String | Enter the read-only (RO) SNMP community string for the probe. |
| Probe RW Community String | Enter the read-write (RW) SNMP community string for the probe. |
| Router Name/IP Address | Enter the hostname of the IP address of the router that the probe is monitoring. |
| Router RO Community String | Enter the RO community string for the router that the probe is monitoring. |
| Interface Description | Enter a description of the router interface. |

**Step 4** Click **Add**.

The Cisco Multicast Monitor system starts the probe discovery process, and attempts to contact the router. If the router is contacted successfully, the probe information is added to the Cisco Multicast Manger configuration. If the SNMP community string, router name, or IP address is incorrect, an error message appears.

## Importing a List of Probes

To import a list of video probes:

**Step 1** Create a comma-separated text file (CSV) in the format:

**ProbeIPaddress,Probe-SNMP-RO,Probe-SNMP-RW,Router-IP-Address,Router-SNMP-RO,router-interface-desc**

Each entry specifies the following information about a video probe.

| Entry | Description |
|---|---|
| ProbeIPaddress | The name or the IP address of the video probe. |
| Probe-SNMP-RO | The read-only (RO) SNMP community string for the probe. |
| Probe-SNMP-RW | Enter the read-write (RW) SNMP community string for the probe. |
| Router-IP-Address | The hostname of the IP address of the router that the probe is monitoring. |
| Router-SNMP-RO | The RO community string for the router that the probe is monitoring. |
| router-interface-desc | A description of the router interface. |

**Step 2** Save the text file to a directory on the computer where you are running Cisco Multicast Manager.

**Step 3** Click **Browse**.

**Step 4** Navigate to the directory where the text file is located and select the text file.

The directory path and file name appear in the Input From File text box.

**Step 5** Click **Import**.

The Cisco Multicast Monitor system starts the probe discovery process and attempts to discover the specified video probes. If the information in the CSV file is correct, the probes are added to the topology database. If the information in the CSV is incorrect, an error message appears.

**Note** If the probes are not being added, check that the server CMM is loaded on does have IP connectivity to the probes and the probes have SNMP enabled.

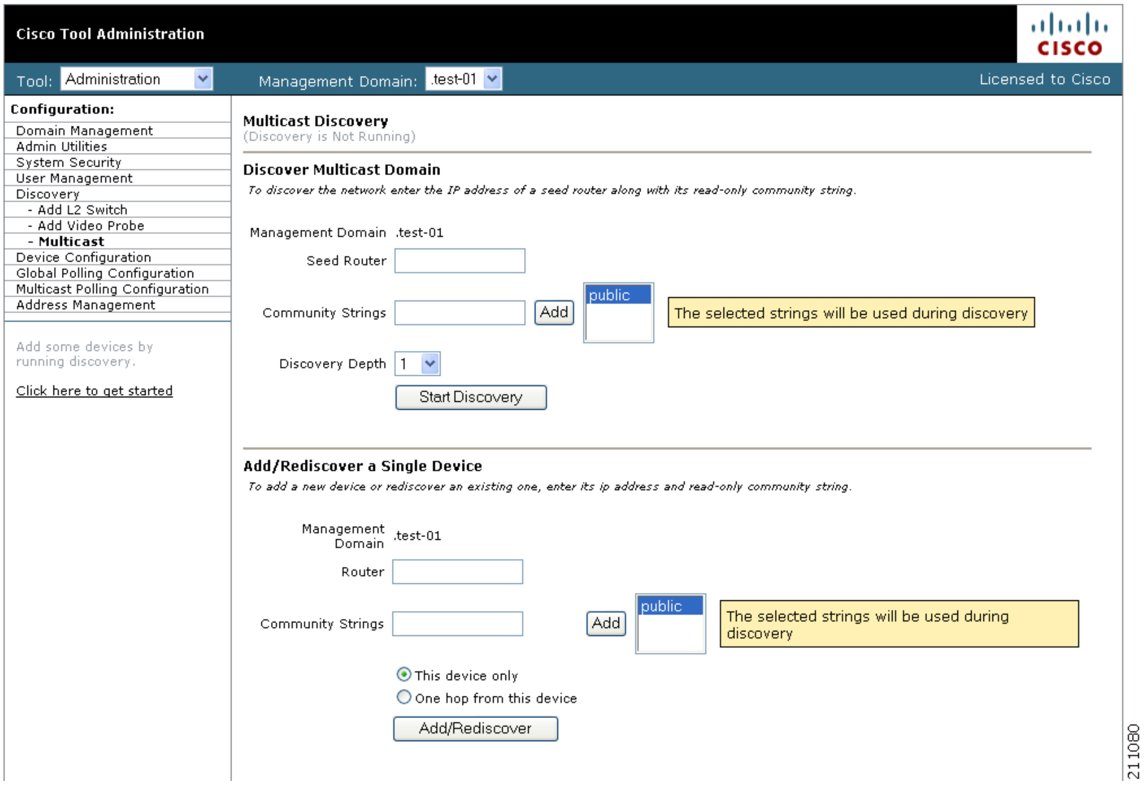
# Performing Multicast Discovery

To perform a new multicast discovery:

**Step 1** Within the Administration tool, select **Discovery**.

**Step 2** Select **Multicast**. The Multicast Discovery page appears, with a **Management Domain** selected.

***Figure 1-6 Multicast Discovery Page***



Cisco Tool Administration

Tool: Administration  Management Domain: .test-01  Licensed to Cisco

Configuration:
- Domain Management
- Admin Utilities
- System Security
- User Management
- Discovery
  - Add L2 Switch
  - Add Video Probe
  - **Multicast**
- Device Configuration
- Global Polling Configuration
- Multicast Polling Configuration
- Address Management

Add some devices by running discovery.

Click here to get started

**Multicast Discovery**
(Discovery is Not Running)

**Discover Multicast Domain**
*To discover the network enter the IP address of a seed router along with its read-only community string.*

Management Domain: .test-01
Seed Router:
Community Strings: [Add] public
The selected strings will be used during discovery
Discovery Depth: 1
[Start Discovery]

**Add/Rediscover a Single Device**
*To add a new device or rediscover an existing one, enter its ip address and read-only community string.*

Management Domain: .test-01
Router:
Community Strings: [Add] public
The selected strings will be used during discovery

● This device only
○ One hop from this device

[Add/Rediscover]

**Step 3** Complete the fields in the **Discover Multicast Domain** pane and click **Start Discovery** to continue.

The Discover Multicast Domain pane contains the following fields:

| Field | Description |
|---|---|
| Management Domain | (Read-only) Lists the selected management domain. |
| Seed Router | Enter the IP address of the seed router to start discovery. If you enabled DNS when configuring the domain, enter a name. |

| Field | Description |
|---|---|
| Community Strings | You can add additional community strings if required. |
| Discovery Depth | Number of PIM neighbors Cisco Multicast Manager will discover from the seed router (similar to a hop count). |

As routers are discovered, they appear in the browser window.

**Step 4** (Optional) To view discovery progress as it is running, click **Refresh Status**.

**Note** For details on adding or rediscovering a single device, see Adding or Rediscovering a Single Device, page 1-13.

CMM discovers all routers in the network that are multicast enabled and have interfaces participating in multicast routing. If the discovery fails to find any routers, or if there are routers in the network that you expected to discover but did not, check the following:

- Connectivity to the routers
- SNMP community strings on the routers
- Discovery depth setting—is it sufficient?
- SNMP ACLs on the routers

When discovery is complete, the browser window displays the time it took to discover the network and the number of devices discovered:

```
Discovery took 15 seconds
Discovered 5 routers
```

The time the discovery takes depends on the number of routers, number of interfaces, and router types.

If the discovery seems to stop at a particular router, or seems to pause, check that particular router's connectivity to its PIM neighbors. Also, check the PIM neighbor to see if it supports the PIM and IPMROUTE MIBs. Again, because the discovery is multicast-specific, unless these MIBs are supported, the device will not be included in the database. Issuing the **sh snmp mib** command on a router gives this information.

When discovery finishes, you can view the discovered routers in the lower left pane.

## Adding or Rediscovering a Single Device

To add or rediscover a single device:

**Step 1** Within the Administration tool, select **Discovery**.

**Step 2** Select **Multicast**. The Multicast Discovery page appears (see Figure 1-6). A **Management Domain** is selected.

**Step 3** Complete the fields in the **Add/Rediscover a Single Device** pane and click **Add/Rediscover** to continue.

The Add/Rediscover a Single Device pane contains these fields:

| Field | Description |
|---|---|
| Management Domain | (Read-only) Lists the selected management domain. |
| Router | Enter the IP address of the device you want to discover or add. |
| Community Strings | You can add additional community strings if required. |
| This device only | Rediscovers this device and updates the current database with the new information. |
| One hop from this device | Discovers this router and every router within one hop, and updates the current database with the new information. |

As devices are discovered, they appear in the browser window.