CISCO SYSTEMS

User Guide for CiscoView Device Manager for the Cisco Content Switching Module

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-6013-01

User Guide for CiscoView Device Manager for the Cisco Content Switching Module

CONTENTS

CHAPTER 4

CHAPTER 5

CHAPTER 6

Preface

This guide describes CiscoView Device Manager for the Cisco Content Switching Module (CVDM-CSM) and describes common tasks you can accomplish with CVDM-CSM.

Audience

This document is for the experienced Network Operations, Security Operations, or Super Admin user managing Cisco Catalyst 6500 Series of switches.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*`italic screen`* font

Item	Convention
Menu items and button names	boldface font
Selecting a menu item	Option>Network Preferences

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Product Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the product documentation that is available.

Table 1 Product Documentation

Document Title	Available Formats
Release Notes for CiscoView Device Manager for the Cisco Content Switching Module	On Cisco.com at this URL: http://www.cisco.com/go/cvdm
User Guide for CiscoView Device Manager for the Cisco Content Switching Module	On Cisco.com at this URL: http://www.cisco.com/go/cvdm
Context Sensitive Online Help	• Click **Help** from the top right corner of the CVDM-CSM desktop. • Click the Help button in any dialog box.

Related Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 2 describes the additional documentation that is available.

Table 2 Related Documentation

Document Title	Available Formats
Release Notes for CiscoView Device Manager for the Cisco Catalyst 6500 Series Switch	On Cisco.com at this URL: http://www.cisco.com/go/cvdm
User Guide for CiscoView Device Manager for the Cisco Catalyst 6500 Series Switch	On Cisco.com at this URL: http://www.cisco.com/go/cvdm

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on

Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Getting Started with CVDM-CSM

The CiscoView Device Manager for the Cisco Content Switching Module (CSM) enables users easily to configure content load-balancing services on their CSMs. It is a task-based tool that allows users to control the versatility of their Cisco CSM by offering configuration based on recommended practices in tasks, such as setting up virtual servers, creating server farms, and applying advanced policies. CiscoView Device Manager is a free embedded manager that resides in the Cisco Catalyst 6500 Series supervisor engine Flash memory.

The CiscoView Device Manager for the Cisco CSM manages several CSM features and helps users accomplish these tasks with ease.

For enterprises and service providers to offer accelerated content delivery services in their data centers, an easy-to-use, web based, device-management GUI is required for CVDM-CSM. The CVDM-CSM Device Manager is an embedded device manager targeted at single chassis setup, feature and service configuration, and monitoring of the Catalyst 6500/7600 series of products.

CiscoView Device Manager for the CSM supports server load balancing configuration on the CSM, including:

1. Configuring virtual servers.
2. Configuring server farms and attaching real servers to them.
3. Configuring client and server VLANs.
4. Configuring Layer 4 through Layer 7 policies, including maps and sticky groups.
5. Monitoring the health of servers

This section contains the following topics:

Key Features in CVDM-CSM

The following table describes the key features of CVDM-CSM.

Feature	Description
Dual Mode Setup Wizard	Allows users to customize deployment in two modes, using either a basic or an advanced wizard.
VLAN Setup	Client and Server side VLAN setup.
Virtual Server Setup	Advertise active (required for route health injection), Restricts clients access to virtual servers, Performance/load configuration, Enabling/disabling of connection persistence, Sticky configuration, Default/backup server farm policy setup, URL-hash prefix.
Server Farm configuration	Possible to set prediction algorithm, In-band health monitoring, NAT, Associating probes, Fail action—action taken on real server failure (purge/reassign), Configuring a set of real servers, Taking real servers in/out of service.
Real Server configuration	Server farm name and real IP address, Load parameters (maximum/minimum connections and threshold load), Health monitoring parameters (probe), Port translation, Weight.
Policy configuration	Configuring and associating Cookie map, Header map, URL map, Client group (access control lists), Sticky group, and Associate server farm and backup server farm.

Feature	Description
Map configuration	Map types such as Cookie map, Domain Name System map, Header map, URL map.
Sticky Group configuration	Sticky group types such as Cookie, CVDM-CSM, Header, Netmask.
Health Monitoring Configuration Probes	Probe types such as FTP, HTTP, Internet Control Message Protocol, Simple Mail Transfer Protocol, TCP, Telnet.
Fault Tolerant Group	Allows users to set Group identification, Fault tolerant VLAN, Failover time, Heartbeat time, Preempt, Priority.
XML Configuration	Allows users to set Client group, Credentials, VLAN, Port, XML service status.

Navigating in CVDM-CSM

Before you begin using CVDM-CSM, you must understand the basic operation of the user interface, including the login procedure and user interface elements. See the following sections for more information:

- Starting CVDM-CSM, page 1-4
- Understanding the CVDM-CSM Desktop, page 1-5

Starting CVDM-CSM

Step 1 In your browser, enter the IP address or DNS hostname of the device. The Enter Network Password dialog box appears.

Step 2 Enter your device username and password.

Step 3 Click **OK**. The CVDM-CSM Device Manager Home Page appears.

Step 4 Enter your device username and password. The SSH Credentials dialog box appears.

Step 5 Enter your SSH username and password. The Enter Enable Password dialog box appears.

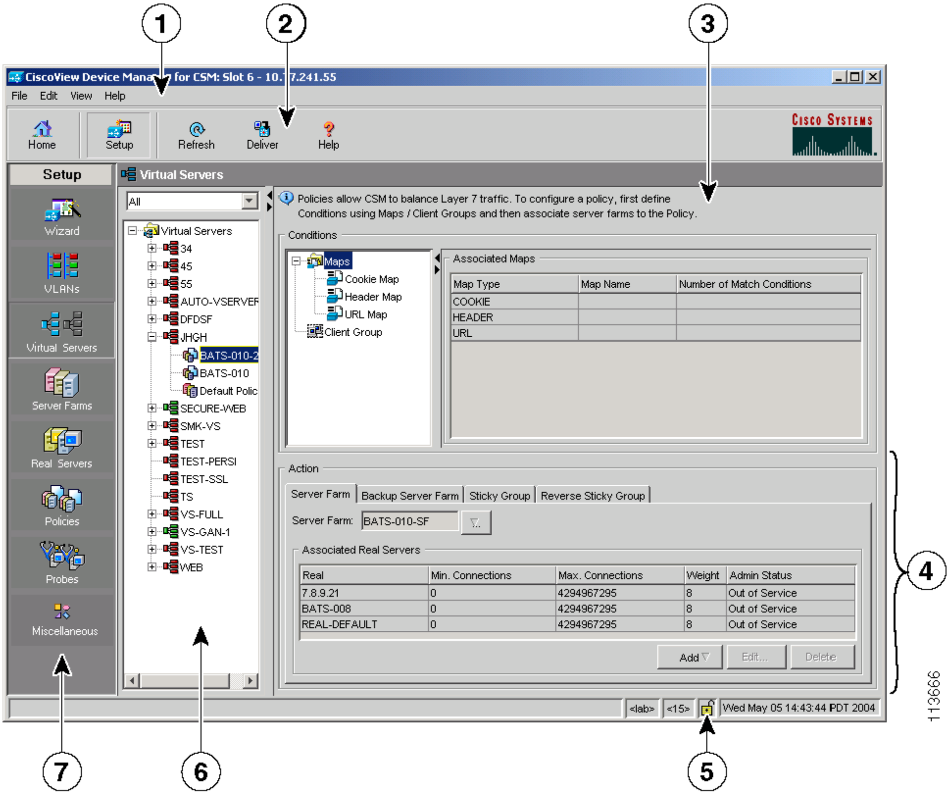
Step 6 Enter Enable Password.

Step 7 Click **OK**. The application starts.

Understanding the CVDM-CSM Desktop

This section describes the main GUI elements of the CVDM-CSM application.

Figure 1-1 CVDM-CSM GUI Elements



Policies allow CSM to balance Layer 7 traffic. To configure a policy, first define Conditions using Maps / Client Groups and then associate server farms to the Policy.

Map Type	Map Name	Number of Match Conditions
COOKIE		
HEADER		
URL		

Server Farm: BATS-010-SF

Real	Min. Connections	Max. Connections	Weight	Admin Status
7.8.9.21	0	4294967295	8	Out of Service
BATS-008	0	4294967295	8	Out of Service
REAL-DEFAULT	0	4294967295	8	Out of Service

Figure 1-1 Reference	Location	Description
1	Menu bar	Provides File, Edit, View, and Help buttons. • File – File > Save to Startup—Saves the configuration running on the device as the startup configuration. – Deliver to Device…—Send the configuration to the device. – File > Exit—Logs you out of CVDM-CSM and closes the window. A warning appears if any configuration have not been applied. Based on your preference, the configurations are either applied or discarded before the application closes. • Edit > Preferences—Edit your global user preferences. • View – View > Home—Displays the home page. – View > Setup—Displays the features page. – View > Running Configuration—Displays the configuration running on the **Supervisor** and the **CSM**. – View > Refresh—Collects the most recent device information and updates CVDM-CSM with it. • Tools > Ping —Checks the connection with the server and opens a dialog box showing the status. • Help – Help > Help Topics—Displays online help. – Help > About—Displays CVDM-CSM version information.

Figure 1-1 Reference	Location	Description
2	Task bar	Provides access to CVDM functionality. • Home—Displays the home page. • Setup—Displays the features page. • Refresh—Collects the most recent device information and updates CVDM-CSM with it. • Deliver—Sends CVDM-CSM data to the device. • Help—Displays context-sensitive help.
3	Page	CVDM-CSM working area in which you perform tasks.
4	Pane	One part of a divided page or dialog box.
5	Status bar	Provides the following information: • Message describing the current status of the application. • Icon showing a table of users logged in to the device. • Application user and privilege level. • Icon showing the list of pending CLIs to be delivered to the device. • Icon showing the security level of the connection. • Time stamp showing the application startup time.
6	Selector	Hierarchy of the groups and objects available in the Switch or Services page that allows you to access specific functions for a Switch or Service object. See the "Selector" section on page 1-8 for more information.
7	Left-most pane	Contains buttons, under the Switch or Services page, that allow you to access switch or services functions.

Selector

Figure 1-2 shows the selector; Table 1-1 describes the selector elements.

Figure 1-2 Selector

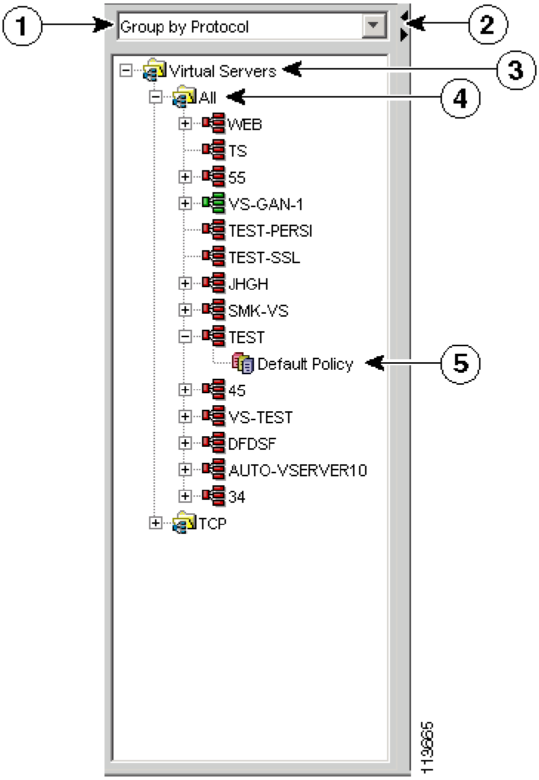


Table 1-1 Selector Elements

Figure 1-2 Reference	Location	Description
1	Group folder	Displays a group of objects. Click the plus (+) symbol to see the contents of this folder.
2	Selector handle	Click the handle to open and close the selector, or click the handle and drag it to resize it.
3	Subgroup folder	Displays a subgroup of objects. Click the plus (+) symbol to see the contents of this folder.
4	Object	Displays the individual entity contained in the group or subgroup. Click an object to open the page for that object.

Note Figure 1-2 shows what the selector looks like when there are folders, subfolders, and objects displayed. Some selectors do not contain all of these elements.

Understanding the Action Buttons

This section describes the action buttons that appear in CVDM-CSM dialog boxes and wizards.

- For a description of the wizard action buttons, see Table 1-2 on page 1-9.
- For a description of the dialog box action buttons, see Table 1-3 on page 1-10.

Table 1-2 Wizard Action Buttons

Button	Action
Back	Takes you to the previous page.
Next	Takes you to the next page.
Finish	Takes you to the wizard summary page.

Table 1-2 Wizard Action Buttons

Button	Action
Cancel	Exits the wizard without making any changes.
Help	Displays context-sensitive online help.

Table 1-3 Dialog Box Action Buttons

Button	Action
OK	Saves your changes.
Cancel	Exits the dialog box without making any changes.
Help	Displays context-sensitive online help.

Editing Preferences

Step 1 Select **Edit > Preferences.** The Preferences dialog box appears.

Step 2 Modify the appropriate values:

GUI Element	Action
Show CLI Preview for Wizards check box	Select this checkbox if you want CVDM to display the CLI commands to be delivered to the device after you have completed a wizard. When this checkbox is selected, when you click **Finish** in a wizard, the Deliver Configuration to the Switch/Module(s) dialog box opens and displays the CLI commands. For more information, see the "“Delivering CLI Commands to the Switch/Module” section on page 1-19”.
Show CLI Preview on Delivery checkbox	Click this checkbox if you want CVDM to display the CLI commands to be delivered to the device. When this checkbox is selected, if you click **Deliver**, then the Deliver Configuration to Switch/Module(s) dialog box opens and displays the CLI commands. For more information, see the “Delivering CLI Commands to the Switch/Module” section on page 1-19.
Save to Startup checkbox	Click this checkbox to save your CVDM settings as the device startup configuration.
Confirm before Exiting checkbox	Click this checkbox if you want CVDM to ask you to confirm that you want to exit the application. When this checkbox is selected, CVDM displays a dialog box asking you if you want to exit CVDM. From this dialog box, you can select the Always display this dialog box before exiting checkbox if you always want CVDM to confirm that you want to exit CVDM.

Viewing the Running Configuration Information for a Device

Step 1 Select **View > Running Config**, then select one of the following:

- **Supervisor...**
- **CSM: Slot** *X*...

Note Only options for installed service modules are available to be selected.

Step 2 The Show Running Configuration dialog box appears. Information about the running configuration for the selected component is displayed.

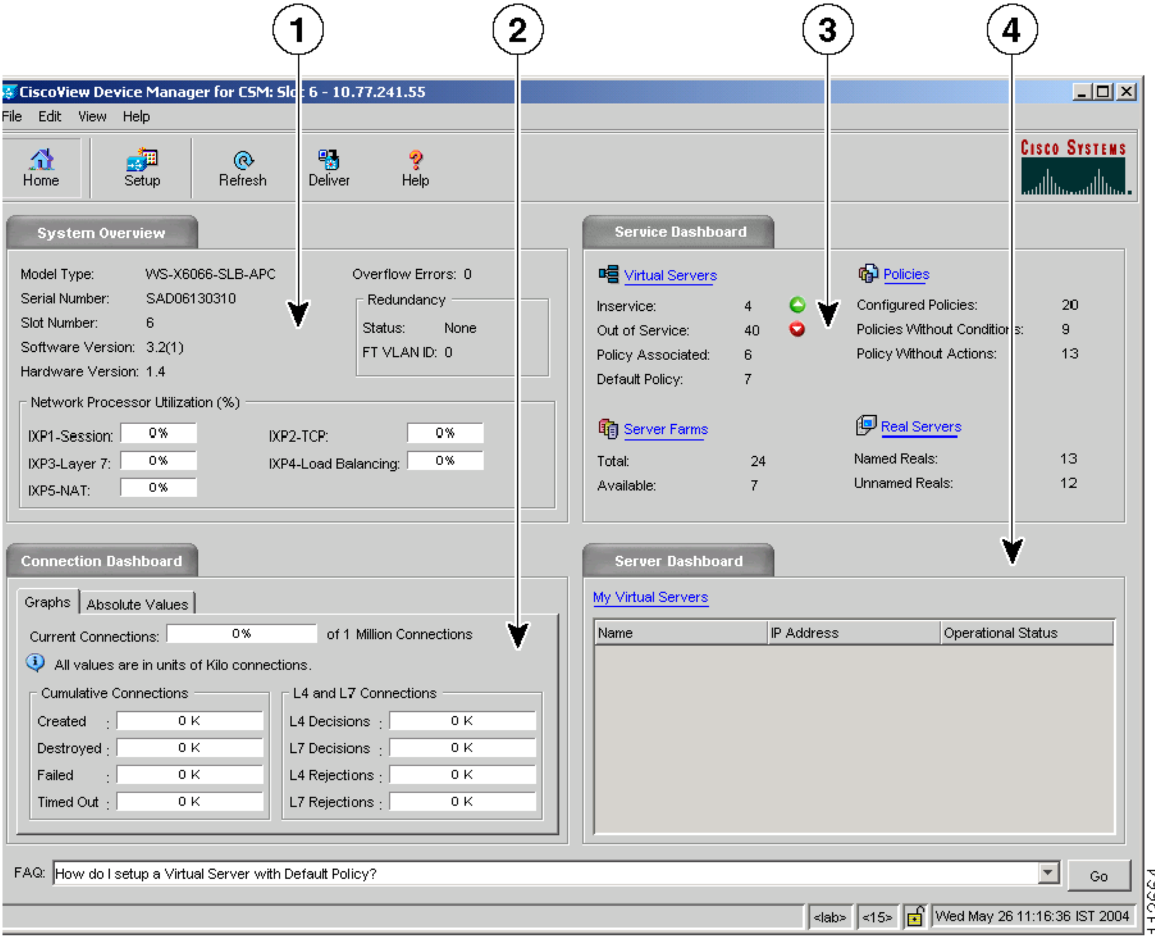
You can click the **Save to File** button to save this information as a text file.

CVDM-CSM Home Page

The Home page is the first screen that comes up when CVDM-CSM is started. The home page provides an overview of CVDM-CSM.

The home page displays the following information:

Figure 1-3 Homepage CVDM-CSM



System Overview

Model Type: WS-X6066-SLB-APC
Serial Number: SAD06130310
Slot Number: 6
Software Version: 3.2(1)
Hardware Version: 1.4

Overflow Errors: 0

Redundancy
Status: None
FT VLAN ID: 0

Network Processor Utilization (%)

IXP1-Session:	0%	IXP2-TCP:	0%
IXP3-Layer 7:	0%	IXP4-Load Balancing:	0%
IXP5-NAT:	0%		

Service Dashboard

Virtual Servers
Inservice: 4
Out of Service: 40
Policy Associated: 6
Default Policy: 7

Policies
Configured Policies: 20
Policies Without Conditions: 9
Policy Without Actions: 13

Server Farms
Total: 24
Available: 7

Real Servers
Named Reals: 13
Unnamed Reals: 12

Connection Dashboard

Graphs | Absolute Values

Current Connections: 0% of 1 Million Connections

All values are in units of Kilo connections.

Cumulative Connections		L4 and L7 Connections	
Created :	0 K	L4 Decisions :	0 K
Destroyed :	0 K	L7 Decisions :	0 K
Failed :	0 K	L4 Rejections :	0 K
Timed Out :	0 K	L7 Rejections :	0 K

Server Dashboard

My Virtual Servers

Name	IP Address	Operational Status

FAQ: How do I setup a Virtual Server with Default Policy? Go

<lab> <15> Wed May 26 11:16:36 IST 2004

Table 1-4 Home Page Description

Reference	Field	Description
1	**System Overview**	
	Model Type	Model Type of the CSM.
	Overflow errors	Number of overflow errors for the system.
	Serial Number	Serial number of the card.
	Slot Number	Slot number of the CSM for which the application is open.
	Software Version	Software version of the CSM module.
	Hardware Version	Hardware version of the CSM module.
	Redundancy	
	Status	Displays if the module is active or Standby.
	FT VLAN ID	Displays the VLAN over which heartbeat messages are sent. Both CSMs must have the same VLAN ID.
	Network Processor Utilization	Displays the utilization of the network processor in percentage for IXP1-Session, IXP2-TCP, IXP3-Layer7, IXP4-Load-Balancing, and IXP5-NAT.

Table 1-4 Home Page Description

Reference	Field	Description
2	**Connection Dashboard**	
	Graphs	Select this button to view the Connection Dash Board details as graphs. The graphs are indicated in units of Kilo connections.
	Actual Values	Select this button to view all fields as actual connections values.
	Cumulative Connections	
	Created Connections	Number of connections at the specified moment. The units are Kilo Connections.
	Destroyed Connections	Number of connections destroyed. The units are Kilo Connections.
	Failed Connection	Number of connections that failed. The units are Kilo Connections.
	Timed Out Connections	Number of connections that were timed out. The units are Kilo Connections.
	L4 and L7 Connections	
	L4 Decision	Number of layer 4 load balancing decisions taken. The units are Kilo Connections.
	L7 Decision	Number of layer 4 load balancing decisions taken. The units are Kilo Connections.

Table 1-4 Home Page Description

Reference	Field	Description
	L4 Rejections	Number of Layer 4 load-balancing rejections taken. The units are Kilo Connections.
	L7Rejections	Number of Layer 7 load-balancing rejections taken. The units are Kilo Connections.
3	**Service Dashboard**	
	Virtual Servers	
	Inservice	Number of virtual servers that are operational.
	Out of Service	Number of Virtual Servers that are not operational.
	Policy Associated	Number of Virtual Servers that have associated policies.
	Default Policy	Number of Virtual Servers that have only the default policy.
	Policies	
	Configured Policies	Number of policies that are configured in the CSM module.
	Policies without conditions	Number of policies that are without conditions.
	Policy without action	Number of policies that are without actions.
	Server Farms	
	Total	Number of server farms configured in the CSM Module.
	Available	Number of server farms with atleast one operational real server.
	Real Servers	Displays the admin status of the real servers.

Table 1-4 Home Page Description

Reference	Field	Description
	Named Reals	Number of Named Real Server configured on the CSM.
	Unnamed Reals	Number of Unnamed Real Server configured on the CSM.
4	**Server Dashboard**	
	My Virtual Server	Selected virtual servers that are used in emergencies as critical servers. For more details see "My Virtual Servers" section on page 1-17.
	Name	Name of the Virtual Server.
	IP Address	IP address of the Virtual Server.
	Operational Status	Virtual Servers that are out of service.

My Virtual Servers

My Virtual Servers page is a part of the Homepage under the **Server Dashboard**.

Step 1 Click **My Virtual Servers** link. The page appears and the following fields are displayed.

Field	Description
Virtual Server Name	A list of Virtual Server names.
Select	Select the check box against the respective virtual server to count them as My Virtual Servers.

Setup Page

The setup page allows you to access the features in CVDM-CSM. You can launch wizards from this page or you can start using the VLANs, Virtual Servers, Server Farms, Real Servers, and Policies features from this page.

On selecting the Setup, the following GUI elements are displayed in an outlook bar on the left side of the content window:

GUI Element	Description
Wizard	Click to launch wizards that will help you to configure and manage Client and VLAN server setup, Virtual Server, and associate default policies.
VLAN Setup	Allows you to set client-side and server-side VLAN setup.
Virtual Server Setup	Allows you to advertise active (required for route health injection), Restricts clients access to virtual servers, Performance/load configuration, Enabling/disabling of connection persistence, Sticky configuration, Default/backup server farm policy setup, and URL-hash prefix.
Server Farm Configuration	Allows you to set prediction algorithm, In-band health monitoring, NAT, Associate probes, Fail action—action taken on real server failure (purge/reassign), Configure a set of real servers, Taking real servers in/out of service.
Real Server Configuration	Allows you to create and manage Server farm name and real IP address, Load parameters (maximum/minimum connections and threshold load), Health monitoring parameters (probe), Port translation, and Weight.
Policy Configuration	Allows you to configure and associate Cookie map, Header map, URL map, Client group (access control lists), Sticky group, and Associate server farm and backup server farm.
Fault Tolerance	Allows you to set Group identification, Fault tolerant VLAN, Failover time, Heartbeat time, Preempt, and Priority.
XML Configuration	Allows you to set Client group, Credentials, VLAN, Port, and XML service status.

Delivering CLI Commands to the Switch/Module

You must deliver accumulated CLI commands to the device before any changes you make in CVDM-CSM will be applied.

Step 1 Click the **Deliver** button at the top of the page. The Deliver Configuration to Switch/Module(s) dialog box appears if you have configured CVDM to display the accumulated CLI commands when you click the Deliver button.

Note The Deliver Configuration to Switch/Module(s) dialog box also appears when you click the **Finish** button in a wizard if you have configured CVDM to display the accumulated CLI commands after you have completed a wizard.

Step 2 Modify the appropriate values:

GUI Element	Action/Description
Page	Displays the accumulated CLI commands to be delivered to the device.
Save to Startup checkbox	Click the checkbox to save the running configuration, generated by CVDM, as the device startup configuration.
Deliver button	Click to send the accumulated CLI commands to the device.
Save to File... button	Click to save the CLI commands as a text file.
Close button[1]	Close the dialog box without delivering any CLI commands.
Deliver Later button[2]	Click to deliver the wizard CLI commands to the device at a later time.

[1] This button is available only in the Deliver Configuration to Switch/Module(s) dialog box that is displayed after you click **Deliver** at the top of the window.

[2] This button is available only in the Deliver Configuration to Switch/Module(s) dialog box that is displayed after you click **Finish** in a wizard.

Note The Deliver Configuration to Switch/Module(s) dialog box displays *all* accumulated CLI commands that will be delivered to the device; therefore, any previous CLI commands that were not sent to the device are shown in this dialog box, as well as the CLI commands you have generated in this session.

Configuring CVDM-CSM

The CVDM-CSM Manager allows user to setup the CSM module features with the help of wizards, which simplifies the complex configuration.

This section includes the following topics:

- Understanding Wizards, page 2-1
- Basic Setup Wizard, page 2-2
- Advanced Setup Wizard, page 2-12
- How Do I?, page 2-14

Understanding Wizards

CVDM-CSM Manager allows you to choose between two types of setup wizards:

- Basic Setup Wizard
- Advanced Setup Wizard

To choose between the two Wizards:

Step 1 Click **Setup** from the task bar. The Setup page appears.

Step 2 Click **Wizards** in the left-most pane. The setup wizards information appears in the content area.

Step 3 You can select either of the following two wizards:

- Basic Setup Wizard

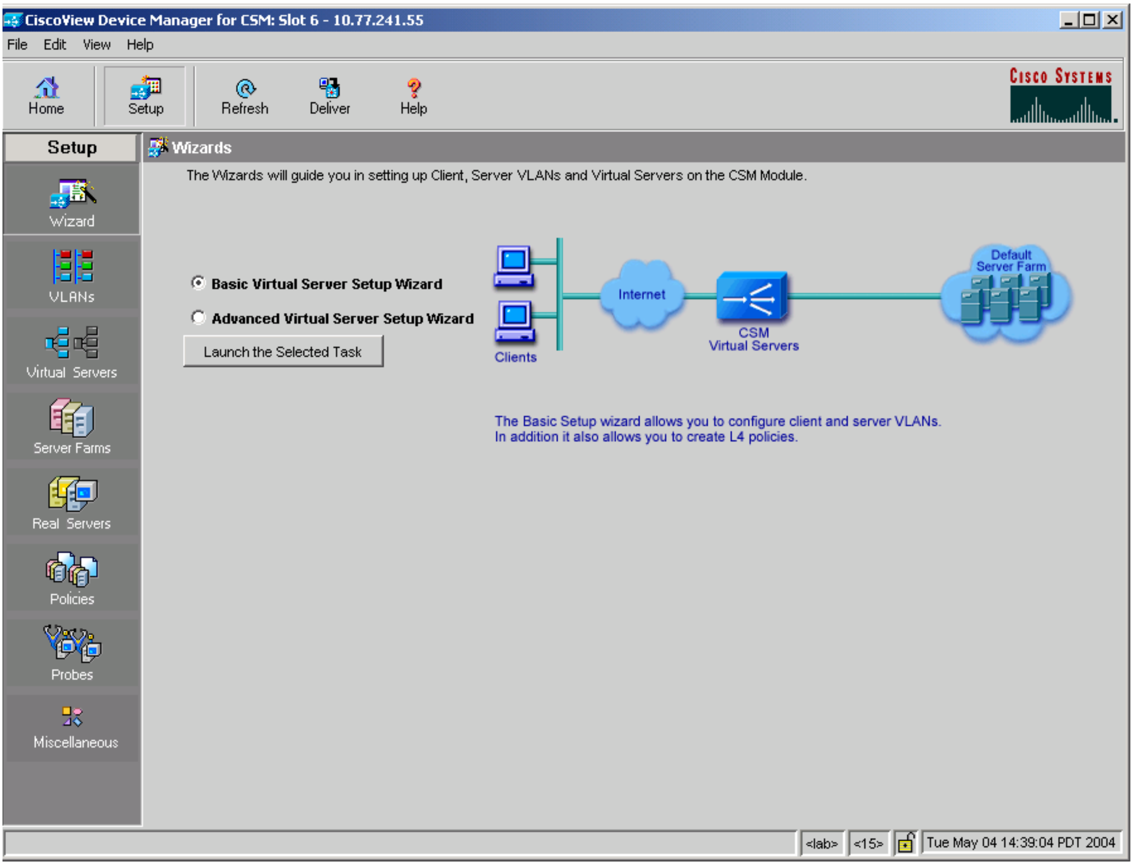
- Advanced Setup Wizard

Step 4 Click **Launch Selected Task** to launch the corresponding wizard.

Basic Setup Wizard

The Basic Setup Wizard allows you to configure client and server VLANs and also create Layer 4 policies.

Figure 2-1 Basic Setup Wizard Page



The Wizards will guide you in setting up Client, Server VLANs and Virtual Servers on the CSM Module.

● Basic Virtual Server Setup Wizard

○ Advanced Virtual Server Setup Wizard

Launch the Selected Task

The Basic Setup wizard allows you to configure client and server VLANs.
In addition it also allows you to create L4 policies.

Welcome Page

The Welcome page lists the three basic configuration steps:

- Configuring Client and Server Side VLAN
- Configuring Virtual Server
- Configuring Default Policy

Configuring Client and Server Side VLAN

Both wizards allows you to create Client side VLAN and Server side VLANs by specifying IP address, alias IP address, gateway and static route values.

To do this:

Step 1 Click **Setup** from the task bar, then click **Wizards** in the left-most pane.

Step 2 The Setup Wizards information appears in the content area.

Step 3 You can select any of the following two wizards:

- **Basic Setup Wizard**
- **Advanced Setup Wizard**.

Step 4 Click **Launch Selected Task** to launch the corresponding wizard dialog. The Welcome page appears.

Step 5 Select **Configure Client and Server Side VLAN**. The Configure Client and Server Side VLAN dialog box appears.

The following fields appear in the Configure Client and Server Side VLAN dialog box:

Field	Action/Description
Client VLAN	
VLAN ID	Specify the ID of the VLAN. You can create a new VLAN or choose from an available VLAN. Click ▽... and select of the following: • **Select VLAN** to select a VLAN from a list. • **Create VLAN** to create a VLAN by entering the VLAN ID.
IP Address	Enter the IP address of the VLAN. Only one management IP address is allowed per VLAN.
Alias	Enter the alias IP address. You can configure up to 255 aliases per VLAN. When more than one alias IP address is listed, they will appear serially separated by a comma. Click ▽... and select **Add Alias**. The Add Alias dialog box appears. Enter the alias IP address.
Gateways	From the list, select the gateway for the VLAN. You can configure up to seven gateways per VLAN, with a total of up to 255 gateways for the entire system. A gateway must be in the same network as specified in the IP address. When more than one gateway IP address is listed, they will appear serially separated by a comma. Click ▽... and select **Add Gateways**. The Add Gateways dialog box appears. Enter the Gateway IP address.
Static Routes	Specify the static route. When more than one static route is listed, they will appear serially separated by a comma. Click ▽... and select **Add Static Route** to add a static route from a list. For more information on adding static route, see "Adding Static Route" section on page 2-6.
Server VLAN	

Field	Action/Description
VLAN ID	Specify the ID of the VLAN. You can create a new VLAN or choose from an available VLAN. Click ▽... and select one of the following: • **Select VLAN** to select a VLAN from a list. • **Create VLAN** to create a VLAN by entering the VLAN ID.
IP Address	Enter the IP address for the CVDM-CSM.
Alias	Enter the alias IP address. When more than one alias IP address is listed, they will appear serially separated by a comma. Click ▽... and select **Add Alias**. The Add Alias dialog box appears. Enter the alias IP address.
Mask	From the list, select the IP mask to be applied. You can choose from Class A, Class B, Class A and Class D masks. If it is not specified, the default for network mask is 255.255.255.255.
Gateways	From the list, select the gateway for the VLAN. You can configure up to seven gateways per VLAN, with a total of up to 255 gateways for the entire system. A gateway must be in the same network as specified in the ip address. When more than one gateway IP address is listed, they will appear serially separated by a comma. Click ▽... and select **Add Gateways**. The Add Gateways dialog box appears. Enter the Gateway IP address.
Static Routes	Specify the static route. When more than one static route is listed, they will appear serially separated by a comma. Click ▽... and select **Add Static Route** to add a static route from a list. For more information on adding static route, see "Adding Static Route" section on page 2-6.

Adding Static Route

The following fields appear:

Field	Description
Destination IP	Enter the IP address of the destination.
Mask	From the list, select the mask to be applied. You can choose from Class A, Class B, Class A and Class D masks. If it is not specified, the default for network mask is 255.255.255.255.
Next Hop	Enter the IP address of the next hop.

Configuring Virtual Server

To configure a virtual server:

Step 1 Click **Setup** from the task bar, then click **Wizards** in the left-most pane. The Setup Wizards information appears in the content area.

Step 2 You can select any of the following two wizards:

- **Basic Setup Wizard**
- **Advanced Setup Wizard**.

Step 3 Click **Launch Selected Task** to launch the corresponding wizard dialog. The Welcome page appears.

Step 4 Click **Next**. The Configure Client and Server Side VLAN dialog box appears.

Step 5 Click **Next**. The Configure Virtual Server dialog box appears.

The following fields appear in the Configure Virtual Server dialog box:

Field	Description
Virtual Server	Click ▽... and select one of the following: • **Select Virtual Server** to select a Virtual Server from a list. • **Create Virtual Server** to create a Virtual Server by entering the name of the Virtual Server.
Virtual IP Address	
IP Address	Enter the IP address of the Virtual Sever.
Mask	Mask for the IP address to allow connections to an entire network. The default IP mask is 255.255.255.255.
Protocol	From the list, select the load-balancing protocol.
Allow Traffic from VLAN	From the list, select the VLAN from which traffic is enabled.
Port	From the list, select the port. This field is enabled only when you choose TCP or UDP as the protocol.
Service Type	From the list, select service type.

Configuring Default Policy

You can configure multiple real servers and associate them to the server farm, and delete the association of the existing real server.

Step 1 Click **Setup** from the taskbar, click **Wizards** in the left-most pane. The Setup Wizards information appears in the content area.

Step 2 You can select any of the following two wizards:

- **Basic Setup Wizard**
- **Advanced Setup Wizard**.

Step 3 Click **Launch Selected Task** to launch the corresponding wizard dialog. The Welcome page appears.

Step 4 Click **Next**. The Configure Client and Server Side VLAN dialog box appears.

Step 5 Click **Next**. The Configure Virtual Server dialog box appears.

Step 6 Click **Next**. The Configure Default Policy dialog box appears.

In case of the Advanced Setup Wizard you will have to Configure Layer 7 Policies to reach the Default policy dialog box.

The following fields appear in the Configure Default Policy dialog box:

Field	Description
Default Server Farm	Click ▽... and select one of the following: • **Select Server Farm** to select a Virtual Server from a list. • **Create Server Farm** to create a Server Farm by entering the name of the Server Farm.
Associated Real Servers	
Real	The Real Server associated to the server farms.
Minimum Connections	Minimum number of connections for the real server.
Maximum Connections	Maximum number of connections for the real server.

Field	Description
Weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Admin Status	Lets you know the admin status of the real server.

From the Configure Default Policy page, you can access functions to do the following:

- Click **Add** and do either of the following:
  - Choose **Select Named Real Server Farm** to choose a real server from a list. For more information on adding a named Real Server, see "Adding Named Real Server" section on page 5-17.
  - Choose **Create Unnamed Real Server Farm** to create a Server Farm. For more information on adding an unnamed Real Server, see "Adding Unnamed Real Server" section on page 5-20.
- Click **Edit** to edit the selected Real Server. For more information on editing a Real Server, see "Editing a Real Server" section on page 6-9.
- Click **Delete** to delete the selected Real Server.

Summary

You can see a list of all the generated CLI commands that are delivered to the device after you click the **Finish** button.

Step 1 Click **Setup** from the taskbar, click **Wizards** in the left-most pane. The Setup Wizards information appears in the content area.

Step 2 You can select any of the following two wizards:

- **Basic Setup Wizard**
- **Advanced Setup Wizard**

Step 3 Click **Launch Selected Task** to launch the corresponding wizard dialog. The Welcome page appears.

Step 4 Click **Next**. The Configure Client and Server Side VLAN dialog box appears.

Step 5 Click **Next**. The Configure Virtual Server dialog box appears.

In case of the Advanced Setup Wizard you will have to **Configure Layer 7 Policies** then click **Next**.

Step 6 Click **Next**. The Configure Default Policy dialog box appears.

Step 7 Click **Next**. The Summary dialog box appears.

Delivering a Configuration to the Switch or Module

You can preview CLI commands that will be delivered to the device after you click the **Finish** button.

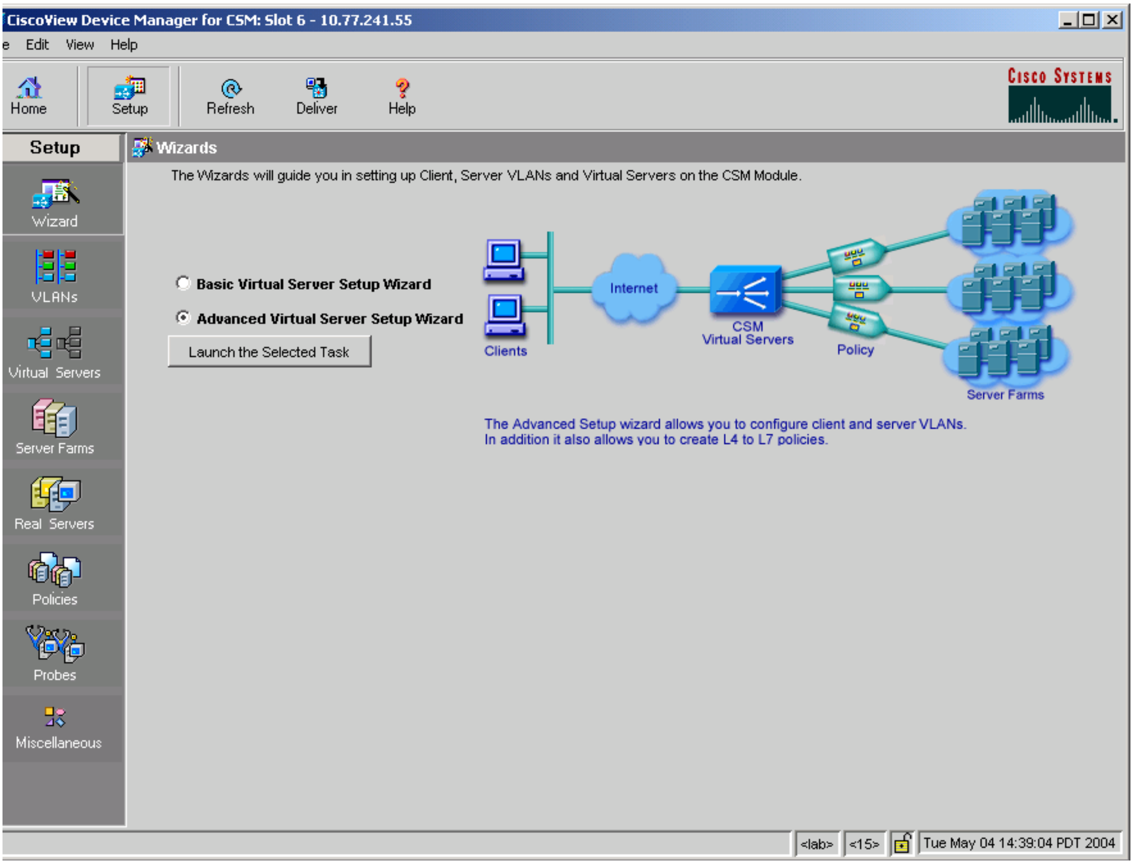
From the Deliver Configuration to Switch/Module(s) page, you can do the following:

- Deliver the CLI commands immediately to the device or module.
- Deliver the CLI commands at a later time to the device or module.
- Save the CLI commands immediately to the device or module.

Advanced Setup Wizard

The Advanced Setup Wizard allows you to configure client and server VLANs and also create layer 4 to layer 7 policies.

Figure 2-2 Advanced Wizards Page



CiscoView Device Manager for CSM: Slot 6 - 10.77.241.55

Wizards

The Wizards will guide you in setting up Client, Server VLANs and Virtual Servers on the CSM Module.

○ Basic Virtual Server Setup Wizard

● Advanced Virtual Server Setup Wizard

Launch the Selected Task

The Advanced Setup wizard allows you to configure client and server VLANs. In addition it also allows you to create L4 to L7 policies.

Welcome Page

The welcome page lists the four advanced configuration steps:

- Configuring Client and Server Side VLAN
- Configuring Virtual Server
- Configuring Layer 7 Policies
- Configuring Default Policy

Configuring Layer 7 Policies

You can create and associate layer 7 policies to the Virtual Server. You can view the already associated Policies, add new ones, delete existing policies, and also change the order of the policies.

You can configure the policy, and also configure and associate the following to the policy:

- One map of each type (URL, Header, Cookie and Return Code).
- One sticky group of any type (Cookie, SSL, NetMask or Header).
- One client group.

To do this:

Step 1 Click **Setup** from the taskbar, click **Wizards** in the left-most pane. The Setup Wizards information appears in the content area.

Step 2 Select **Advanced Setup Wizard**.

Step 3 Click **Launch Selected Task** to launch the corresponding wizard dialog box. The Welcome dialog appears. Click **Next**.

Step 4 The Configure Client and Server Side VLAN dialog box appears. Click **Next**.

Step 5 The Configure Virtual Server dialog box appears. Click **Next**.

Step 6 The Configure and Associate Layer 7 Policies dialog box appears. From this page, you can access functions to do the following:

- Click **Add** and select one of the following:
  - **Select Policy** to select from a list of configured policies.

  - **Create Policy** to add a new policy. For more information on creating policies, see "Adding Policies" section on page 7-4.

- Select a policy and click **Delete** to remove policies from the Virtual Server.
- Click the Up button to move the policies up in the list.
- Click the Down buton to move the policies down in the list.

Note Be sure to order the policies in the correct order. The traffic will be routed based on the order of policies.

How Do I?

This section describes how to perform a task. The following questions are answered:

- How Do I Set Up a Virtual Server with Default Policy?
- How Do I Set Up a Virtual Server with Layer 7 Policy?

How Do I Set Up a Virtual Server with Default Policy?

The Basic Setup Wizard allows you to configure and associate multiple Real Servers to the Server Farm and delete the association of the existing Real Server.

To setup a virtual server with the default policy:

Step 1 Click **Setup** from the taskbar, click **Wizards** in the left-most pane. The Setup Wizards information appears in the content area.

Step 2 Select **Basic Setup Wizard**, then click **Launch Selected Task**. The Welcome page appears.

Step 3 Click **Next**. The Configure Client and Server Side VLAN dialog box appears.

Step 4 Click **Next**. The Configure Virtual Server dialog box appears.

Step 5 Click **Next**. The Configure Default Policy dialog box appears.

Step 6 Configure the default server farm or specify one from the list.

Click ▽... and select one of the following:

- **Select Server Farm** to select a Virtual Server from a list.
- **Create Server Farm** to create a Server Farm by entering the name of the Server Farm.

Related Topics:

- Configuring Client and Server Side VLAN, page 2-3
- Configuring Virtual Server, page 2-6
- Configuring Default Policy, page 2-8
- How Do I Set Up a Virtual Server with Layer 7 Policy?, page 2-16

How Do I Set Up a Virtual Server with Layer 7 Policy?

The Advanced Setup Wizard allows you to configure client and server VLANs and create layer 4 to layer 7 policies.

To setup a virtual server with Layer 7 policy:

Step 1 Click **Setup** from the task bar, click **Wizards** in the left-most pane. The Setup Wizards information appears in the content area.

Step 2 Select **Advanced Setup Wizard**, then click **Launch Selected Task**. The Welcome page appears.

Step 3 Click **Next**. The Configure Client and Server Side VLAN dialog box appears.

Step 4 Click **Next**. The Configure Virtual Server dialog box appears.

Step 5 Click **Next**. The Configure and Associate Layer 7 Policies dialog box appears.

Configure the virtual server or specify one from the list, and associate the required maps, Sticky group and a Client group.

Related Topics:

- Configuring Client and Server Side VLAN, page 2-3
- Configuring Virtual Server, page 2-6
- Configuring Layer 7 Policies, page 2-13
- How Do I Set Up a Virtual Server with Default Policy?, page 2-15

CHAPTER 3

Managing VLANs

CVDM-CSM allows you to configures the client-side and server-side VLANs. Creating the VLAN ID and setting the client/server modes can be performed.

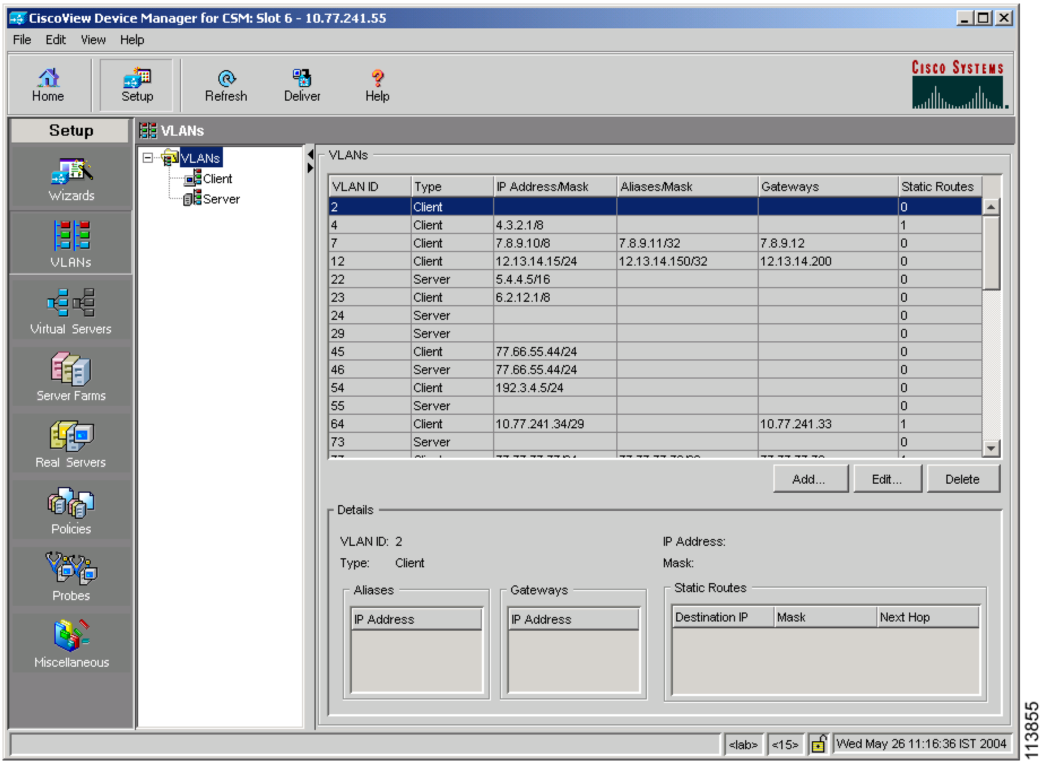
CVDM-CSM VLAN configuration allows you to configure seven gateways and 255 alias IP addresses per VLAN.

This section includes the following topics:

- Viewing a VLAN, page 3-2
  - Viewing VLAN Client, page 3-8
  - Viewing VLAN Server, page 3-9
- Adding a VLAN, page 3-5
- Editing a VLAN, page 3-6

Viewing a VLAN

Figure 3-1 VLAN Page



CiscoView Device Manager for CSM: Slot 6 - 10.77.241.55

VLAN ID	Type	IP Address/Mask	Aliases/Mask	Gateways	Static Routes
2	Client				0
4	Client	4.3.2.1/8			1
7	Client	7.8.9.10/8	7.8.9.11/32	7.8.9.12	0
12	Client	12.13.14.15/24	12.13.14.150/32	12.13.14.200	0
22	Server	5.4.4.5/16			0
23	Client	6.2.12.1/8			0
24	Server				0
29	Server				0
45	Client	77.66.55.44/24			0
46	Server	77.66.55.44/24			0
54	Client	192.3.4.5/24			0
55	Server				0
64	Client	10.77.241.34/29		10.77.241.33	1
73	Server				0

VLAN ID: 2

Type: Client

IP Address:

Mask:

IP Address

IP Address

Destination IP	Mask	Next Hop

Wed May 26 11:16:36 IST 2004

To view a VLAN:

Step 1 Click **Setup** from the task bar.

Step 2 Click **VLAN** in the left-most pane.

The following fields appear:

Field	Description
VLAN ID	ID for client/server VLANs.
VLAN TYPE	Type of VLAN for the client/server.
VLAN IP Address/Mask	IP address and mask of VLANs.
Alias IP Address/Mask	IP address and mask of the Aliases.
Gateway	Gateway for the VLAN.
Static Route	Static Route for the VLAN.

Step 3 When you select any row, the configuration details of the corresponding VLAN are displayed with the following fields:

Field	Description
VLAN ID	ID for client/server VLANs.
IP Address	IP Address of the VLANs.
Type	Type of the VLAN - client/server
Mask	Mask of the VLAN
Alias	The IP address of the alias.
Getaway	The IP address of the Gateway.
Static Routes	
Destination IP	The IP address of the destination.
Mask	The mask address of the VLAN.
Next Hop	The next hop address.

From this page, you can access functions to do the following:

- Click **Add** to add a VLAN. For more information, see "Adding a VLAN" section on page 3-5.
- Click **Edit** to edit a VLAN. For more information, see "Editing a VLAN" section on page 3-6.

- Select a row and click **Delete** to delete a VLAN.

Adding a VLAN

To add a VLAN:

Step 1 Click **Setup** at the top of the window, click **VLAN** from the left-most pane, and select **VLANs** from the object selector.

Step 2 Click the **Add** button, then select Single VLAN. The Add VLAN dialog box appears.

Step 3 Enter the appropriate values.

Field	Description
VLAN ID	ID for client/server VLANs. User can select a VLAN ID from the list.
VLAN Type	Type of VLAN - User can select either Client or Server VLAN Type from the list.
VLAN IP Address	IP Address of the VLAN.
VLAN Subnet Mask	Subnet Masks of the VLAN.
Aliases	This group will display a table with Alias IP address and mask details. You can add an alias or delete an existing alias by clicking on Add and Delete buttons respectively.
Gateways	This group will display a table with Gateway details. User can add a gateway or delete an existing gateway by clicking on Add and Delete buttons respectively.
Static Routes	
Destination IP	Enter the IP address of the destination.
Mask	Enter the mask address of the Destination IP.
Next Hop	Enter the Next Hop IP Address.

Editing a VLAN

To modify a single VLAN:

Step 1 Click **Setup** at the top of the window, click **VLANs** from the left-most pane, and select **VLANs** from the object selector.

Step 2 From the table, select the VLAN that you want to modify.

Step 3 Click the **Edit** button. The Edit VLAN dialog box appears.

Step 4 Modify the appropriate values.

Field	Description
VLAN ID	The VLAN ID values for the selected row. This field cannot be edited.
VLAN Type	The VLAN Type values for the selected row. This field cannot be edited.
VLAN IP Address	IP Address of VLANs
VLAN Subnet Mask	Subnet mask of VLANs
Aliases	This group will display a table with Alias IP address and mask details. User can add new alias or delete existing alias by clicking on Add and Delete buttons respectively.
Gateways	This group will display a table with Gateway details. User can add new gateway or delete existing gateway by clicking on Add and Delete buttons respectively.
Static Routes	
Destination IP	Enter the IP address of the destination.
Mask	Enter the mask address of the Destination IP.
Next Hop	Enter the Next Hop IP Address.

Viewing VLAN Client

To view a VLAN client:

Step 1 Click **Setup** from the task bar.

Step 2 Click **VLAN** in the left-most pane. Select **Client** in the object selector.

The following fields appear:

Field	Description
VLAN ID	ID for Client VLANs.
VLAN IP Address/Mask	IP address and mask of VLANs.
Alias IP Address/Mask	IP address and mask of Aliases.
Gateway	Gateway for the VLAN.
Static Route	Static Route for the VLAN.

Viewing VLAN Server

To view a VLAN Server

Step 1 Click **Setup** from the task bar.

Step 2 Click **VLAN** in the left-most pane. Select **Server** in the Object Selector.

The following fields appear:

Field	Description
VLAN ID	ID for Server VLANs.
VLAN IP Address/Mask	IP address and mask of VLANs.
Alias IP Address/Mask	IP address and mask of Aliases.
Gateway	Gateway for the VLAN.
Static Route	Static Route for the VLAN.

Managing Virtual Servers

Content Switching Module Device Manager (CVDM-CSM) displays details of existing virtual servers and enables users to perform detailed tasks that include creating or deleting virtual servers, associating them with server farms and policies, disallowing (or allowing) specific client IP addresses to connect to the virtual server, and turning the virtual services on or off.

Server farms that are represented as virtual servers can improve scalability and availability of services for your network. You can add new servers and remove failed or existing servers at any time without affecting the virtual server's availability.

Virtual servers represent groups of real servers and are associated with real server farms through policies. Configuring virtual servers requires setting the attributes of the virtual server, specifying the default server farm (default policy), and associating other server farms through a list of policies.

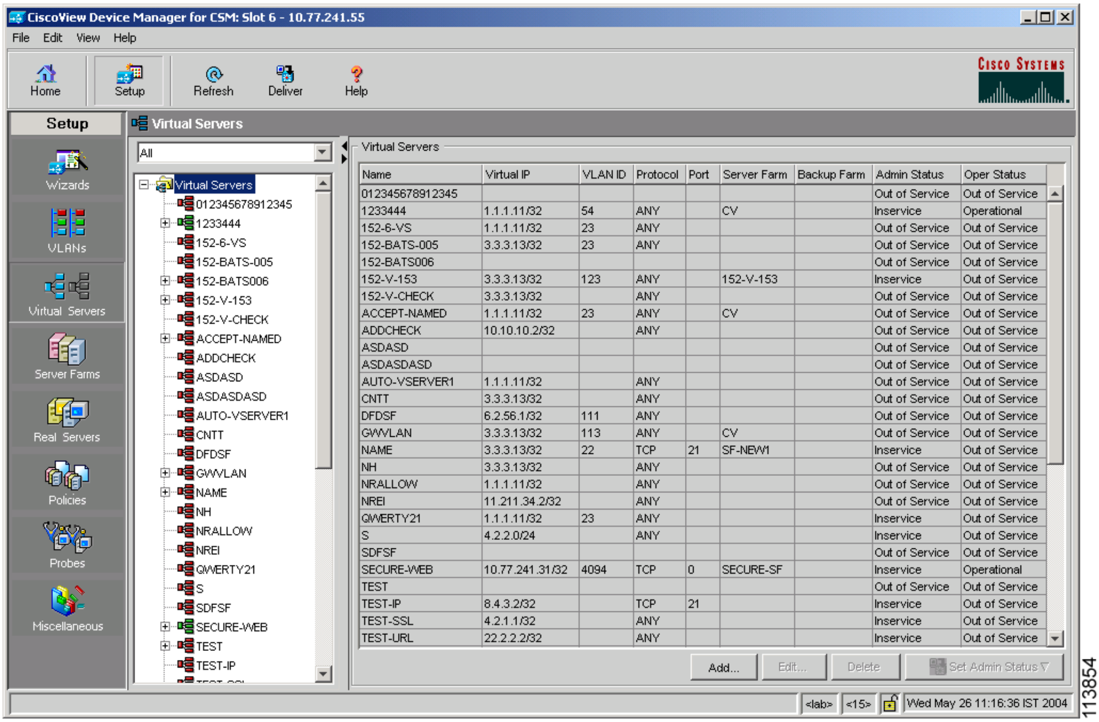
A server farm must be configured before associating it to the virtual server. Policies are processed in the order in which they are entered in the virtual server configuration.

This section includes the following topics:

- Viewing Virtual Servers, page 4-2
- Viewing an Individual Virtual Server, page 4-20
  - Viewing a Policy, page 4-28
  - Viewing a Default Policy, page 4-30
- Adding a Virtual Server, page 4-4
- Editing a Virtual Server, page 4-12

Viewing Virtual Servers

Figure 4-1 Virtual Servers Page



Virtual Servers

Name	Virtual IP	VLAN ID	Protocol	Port	Server Farm	Backup Farm	Admin Status	Oper Status
012345678912345							Out of Service	Out of Service
1233444	1.1.1.11/32	54	ANY		CV		Inservice	Operational
152-6-VS	1.1.1.11/32	23	ANY				Out of Service	Out of Service
152-BATS-005	3.3.3.13/32	23	ANY				Out of Service	Out of Service
152-BATS006							Out of Service	Out of Service
152-V-153	3.3.3.13/32	123	ANY		152-V-153		Inservice	Out of Service
152-V-CHECK	3.3.3.13/32		ANY				Out of Service	Out of Service
ACCEPT-NAMED	1.1.1.11/32	23	ANY		CV		Out of Service	Out of Service
ADDCHECK	10.10.10.2/32		ANY				Out of Service	Out of Service
ASDASD							Out of Service	Out of Service
ASDASDASD							Out of Service	Out of Service
AUTO-VSERVER1	1.1.1.11/32		ANY				Out of Service	Out of Service
CNTT	3.3.3.13/32		ANY				Out of Service	Out of Service
DFDSF	6.2.56.1/32	111	ANY				Out of Service	Out of Service
GWVLAN	3.3.3.13/32	113	ANY		CV		Out of Service	Out of Service
NAME	3.3.3.13/32	22	TCP	21	SF-NEW1		Inservice	Out of Service
NH	3.3.3.13/32		ANY				Out of Service	Out of Service
NRALLOW	1.1.1.11/32		ANY				Out of Service	Out of Service
NREI	11.211.34.2/32		ANY				Out of Service	Out of Service
QWERTY21	1.1.1.11/32	23	ANY				Inservice	Out of Service
S	4.2.2.0/24		ANY				Inservice	Out of Service
SDFSF							Out of Service	Out of Service
SECURE-WEB	10.77.241.31/32	4094	TCP	0	SECURE-SF		Inservice	Operational
TEST							Out of Service	Out of Service
TEST-IP	8.4.3.2/32		TCP	21			Inservice	Out of Service
TEST-SSL	4.2.1.1/32		ANY				Inservice	Out of Service
TEST-URL	22.2.2.2/32		ANY				Inservice	Out of Service

You can view all Virtual Servers that exist on the device.

To view the Virtual Servers:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Virtual Servers** under the **Services Dashboard**.

Or:

Step 1 Click **Setup** from the task bar, then click **Virtual Servers** in the left-most pane.

Step 2 Select **Virtual Servers** root node of the virtual server tree.

The following fields appear:

Field	Description
Name	Name of the virtual server.
Virtual IP Address	IP address of the virtual server.
VLAN ID	ID of the VLAN.
Protocol	Load-balancing protocol.
Port	TCP/UDP port number or name.
Server Farm	Name of the server farm associated to the real server.
Backup Farm	Name of the backup server farm associated to the real server.
Admin Status	Lets you know the admin status of the Virtual Server.
Operational Status	Lets you know the operational status of the Virtual Server.

You can group the Virtual Servers based on various common parameters.

To group the Virtual Servers, click ▽... at the top of the object selector.

You can select one of the following options:

- All
- Group by Protocol
- Group by Admin Status
- Group by Policies

From the Virtual Servers page, you can access functions to do the following:

- Click **Add** to add a Virtual Server. For more information, see "Adding a Virtual Server" section on page 4-4.
- Click **Edit** to edit a Virtual Server. For more information, see "Editing a Virtual Server" section on page 4-12.

- Select a row and click **Delete** to delete Virtual Servers.
- Click **Set Admin Status** to set the status of the Virtual Server instantly.

Adding a Virtual Server

You can add a Virtual Server by giving the required configuration details.

To add a new Virtual Server:

Step 1 Click **Home** at the top of the page

Step 2 Click **Virtual Servers** under the **Services Dashboard**.

Step 3 Click **Add**. The Add Virtual Server dialog box appears.

Or:

Step 1 Click **Setup** from the task bar, then click **Virtual Servers** in the left-most pane.

Step 2 Select **Virtual Servers** from the object selector.

Step 3 Click **Add**. The Add Virtual Server dialog box appears with the following tabs:

- General
- Policies
- Default Policy
- Client Restriction
- Sticky Connections
- Other

General

Click **General** to configure the basic configuration details.

The following details are displayed:

Field	Action/Description
Name	Enter the name of the Virtual Servers.
Status	From the list, select the status of the Virtual Server.
VLAN ID	Specify a VLAN for incoming traffic from the list.
Virtual IP Address	
IP Address	Enter the IP Address of the virtual server.
Protocol	From the list, select the type of IP protocol used. You can choose between Any, TCP or UDP or enter a number between 1 and 255.
Port	From the list, select the port number. This field is enabled only when you choose TCP or UDP.
Service Type	From the list, select the service type.
Advertise	
Advertise Virtual IP Advertise only if reals are active	Choose between the two.

Policies

Click **Policies** to add or delete Policies. You have the following options:

- Click **Add** and select one of the following to associate policies from the Virtual Server.
  - **Select Policy** to select a policy from a list.
  - **Create Policy** to create a policy. For more information see "Adding Policies" section on page 7-4.
- Select a policy and click **Delete** to remove policies from the Virtual Server.
- Click the Up button to move the policies up in the list.
- Click the Down button to move the policies down in the list.

Note Be sure to order the policies in the correct order. The traffic will be routed based on the order of policies.

Default Policy

Click **Default Policy** to add the default and backup Server Farms.

The following details are displayed:

Default Server Farm	Click ▽... and select one of the following: • **Select Server Farm** to select from a list of server farms. • **Create Server Farm** to create a server farm. For more information on creating server farms, see "Adding Server Farms" section on page 5-4. • **Clear Server Farm** to clear a server farm.
Backup Server Farm	
Server Farm	Click ▽... and select one of the following: • **Select Server Farm** to select from a list of server farms. • **Create Server Farm** to create a server farm. For more information on creating server farms, see "Adding Server Farms" section on page 5-4. • **Clear Server Farm** to clear a server farm.
Sticky	Select to enable the sticky property. You can set the sticky option for the server farms by allowing multiple connections from the same client to stick (or attach) to the same real server.

Client Restriction

Click **Client Restriction** to add details of the restricted clients. You have the following options:

- Click **Add** to create client restrictions for multiple clients.
- Click **Edit** to edit the client restrictions for multiple clients.
- Select a row in the table and click **Delete** to delete the selected client restriction.

When you click Add or Edit, the following details are displayed:

Field	Description
IP Address	IP Address of the client.
Mask	Specify the type of IP mask. It can be from Class A, Class B, Class C or Class D masks. If it is not specified, the default for network mask is 255.255.255.255.
Exclude	Select the client to exclude traffic from it.

Sticky Connections

Click **Sticky Connections** to add details of the sticky connections.

The following details are displayed:

Field	Description
Sticky Timer	Specifies the period of time (in minutes) that the sticky information is kept.
Mask	From the list, select, Class A, Class B, Class A and Class D masks. If it is not specified, the default for network mask is 255.255.255.255.
Sticky Group	Click ▽... and select one of the following: • **Select Sticky Group** to select from a list of Sticky Groups. • **Create Sticky Group** to create a Sticky Group. For more information on creating server farms, see "Adding a Sticky Group" section on page 9-5. • **Clear Sticky Group** to clear a Sticky Group.

Field	Description
Reverse Sticky Group	Click ▽... and select one of the following: • **Select Sticky Group** to select from a list of Sticky Groups. • **Create Sticky Group** to create a Sticky Group. For more information on creating server farms, see "Adding a Sticky Group" section on page 9-5. • **Clear Sticky Group** to clear a Sticky Group.
SSL Sticky	
Offset	Enter the offset for the SSL ID.
Length	Enter the length of the SSL ID.

Other

Click **Other** to add details of performance, load, and traffic- related parameters.

The following details are displayed:

Field	Description
Performance/Load Parameters	
Idle Timer	Enter idle connection timer duration in seconds.
Pending Timeout	Enter the time (in seconds) to wait before a connection is considered unreachable.
Parse Length	Enter the maximum number of bytes to parse for URLs and cookies.
Maximum Connections	Enter the maximum number of connections to the real server.

Field	Description
URL Hash	Select this check box to enable the begin and end pattern fields.
Begin Pattern	Specify the beginning pattern of the URL to parse.
End Pattern	Specify the ending pattern of the URL to parse.
Connection/Traffic Parameters	
Enable HTTP Persistence	Select this to enable or disable HTTP persistence for connections in the virtual server.
Enable Unidirectional Traffic	Select this to enable unidirectional traffic.

Editing a Virtual Server

You can monitor Virtual Servers connection details and the list of Policies for the selected Virtual Servers.

To monitor Virtual Servers:

Step 1 Click **Home** at the top of the page

Step 2 Click **Virtual Servers** under the **Services Dashboard**.

Step 3 Select a row from the table. Click **Edit**. The Edit Virtual Server dialog box appears.

Or:

Step 1 Click **Setup** from the taskbar, then click **Virtual Servers** in the left-most pane.

Step 2 Select **Virtual Servers** from the object selector.

Step 3 Select a row from the table. Click **Edit**. The Edit Virtual Server dialog box appears with the following tabs:

- General
- Policies
- Default Policy
- Client Restriction
- Sticky Connections
- Other

General

Click **General** to edit the basic configuration detail

The following details are displayed:

Field	Description
Name	Name of the Virtual Servers.
Status	From the list, select the status of the Virtual Server.
VLAN ID	From the list, select VLAN for incoming traffic from the list.
Virtual IP Address	Enter the IP Address of the Virtual Servers.
Protocol	From the list, select the type of IP Protocol used. You can choose from Any, TCP, or UPD, or you can enter a number between 1 and 255.
Port	From the list, select the list of valid port numbers. This field is enabled only when you choose TCP or UDP.
Service Type	From the list, select the service type.
Advertise	
Advertise Virtual IP	Select this to advertise a virtual IP.
Advertise only if reals are active	Select this to advertise only if real servers are active.

Policies

Click **Policies** to edit Policies. You have the following options:

- Click **Add** to associate policies from the Virtual Server. For more information see "Adding Policies" section on page 7-4.
- Click **Delete** to remove policies from the Virtual Server.
- Click the Up button to move the policies up in the list.
- Click the Down button to move the policies down in the list

Note Be sure to order the policies in the correct order. The traffic will be routed based on the order of policies.

Default Policy

Click **Server Farms** to edit a Server Farm.

The following details are displayed:

Default Server Farm	Click ▽... nd select one of the following: • **Select Server Farm** to select from a list of server farms. • **Create Server Farm** to create a server farm. For more information on creating server farms, see "Adding Server Farms" section on page 5-4. • **Clear Server Farm** to clear a server farm.
Backup Server Farm	
Server Farm	Click ▽... and select one of the following: • **Select Server Farm** to select from a list of server farms. • **Create Server Farm** to create a server farm. For more information on creating server farms, see "Adding Server Farms" section on page 5-4. • **Clear Server Farm** to clear a server farm.
Sticky	Select to enable the sticky property. You can set the sticky option for the server farms by allowing multiple connections from the same client to stick (or attach) to the same real server.

Client Restriction

Click **Client Restriction** to edit the details of the restricted clients.You have the following options:

- Click **Add** to create client restrictions for multiple clients.
- Click **Edit** to edit the client restrictions for multiple clients.
- Select a row in the table and click **Delete** to delete the selected client restriction.

When you click Add or Edit, the following details are displayed:

Field	Description
IP Address	IP Address of the client.
Mask	Specify the type of IP mask. It can be from Class A, Class B, Class C or Class D masks. If it is not specified, the default for network mask is 255.255.255.255.
Exclude	Select the client to exclude traffic from it.

Sticky Connections

Click **Sticky Connections** to edit details of the sticky connections.

The following details are displayed:

Field	Description
Sticky Timer	Enter the sticky time.
Mask	From the list, select Class A, Class B, Class A and Class D masks. If it is not specified, the default for network mask is 255.255.255.255.
Sticky Group	Click ▽... and select one of the following: • **Select Sticky Group** to select from a list of Sticky Groups. • **Create Sticky Group** to create a Sticky Group. For more information on creating server farms, see "Adding a Sticky Group" section on page 9-5. • **Clear Sticky Group** to clear a Sticky Group.
Reverse Sticky Group	Click ▽... and select one of the following: • **Select Sticky Group** to select from a list of Sticky Groups. • **Create Sticky Group** to create a Sticky Group. For more information on creating server farms, see "Adding a Sticky Group" section on page 9-5. • **Clear Sticky Group** to clear a Sticky Group.
SSL Sticky	

Field	Description
Offset	Enter the offset for the SSL ID.
Length	Enter the length of the SSL ID.

Other

Click **Other** to edit details of performance, load, and traffic-related parameters.

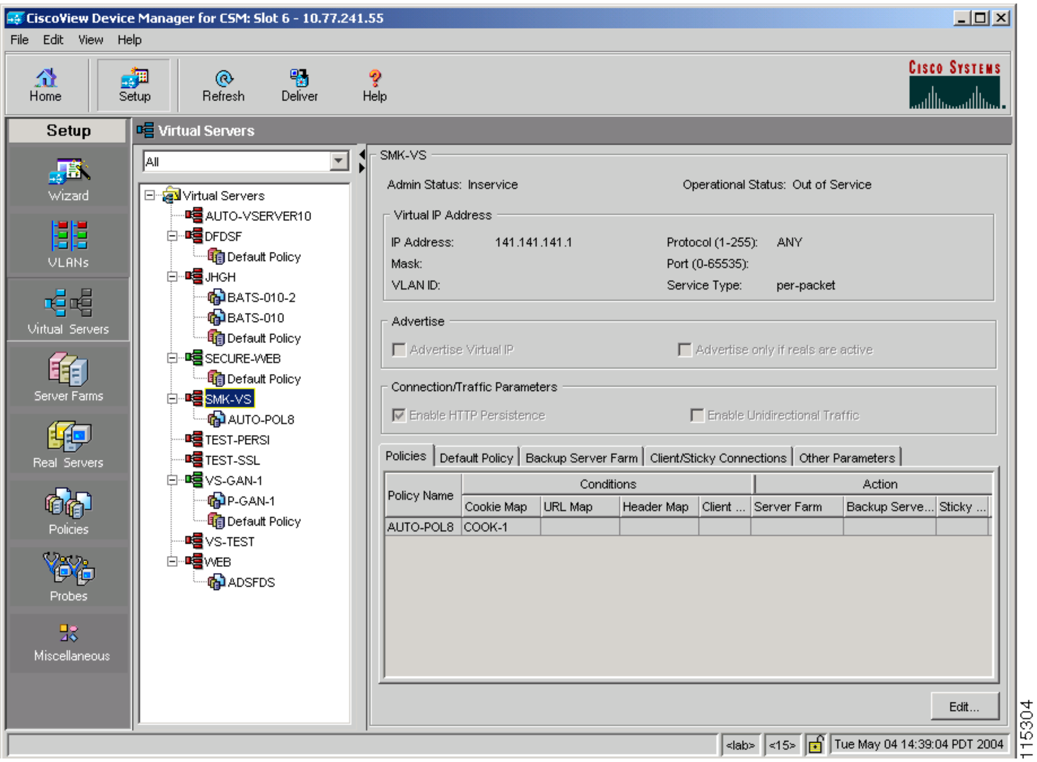
The following details are displayed:

Field	Description
Performance/Load Parameters	
Idle Timer	Enter idle connection timer duration (in seconds).
Pending Timeout	Enter the time (in seconds) to wait before a connection is considered unreachable.
Parse Length	Enter the maximum number of bytes to parse for URLs and cookies.
Maximum Connections	Enter the maximum number of connections to the real server.
URL Hash	Select this check box to enable the begin and end pattern fields.
Begin Pattern	Specify the beginning pattern of the URL to parse.
End Pattern	Specify the ending pattern of the URL to parse.
Connection/Traffic Parameters	
Enable HTTP Persistence	Select this to enable or disable HTTP persistence for connections in the virtual server.
Enable Unidirectional Traffic	Select this to enable unidirectional traffic.

Viewing an Individual Virtual Server

You can view the configuration details of each Virtual Server when you click any of them.

Figure 4-2 Virtual Server - Individual Virtual Server Page



CiscoView Device Manager for CSM: Slot 6 - 10.77.241.55

SMK-VS

Admin Status: Inservice Operational Status: Out of Service

Virtual IP Address

IP Address: 141.141.141.1 Protocol (1-255): ANY
Mask: Port (0-65535):
VLAN ID: Service Type: per-packet

Advertise

□ Advertise Virtual IP □ Advertise only if reals are active

Connection/Traffic Parameters

☑ Enable HTTP Persistence □ Enable Unidirectional Traffic

Policies | Default Policy | Backup Server Farm | Client/Sticky Connections | Other Parameters

Policy Name	Conditions				Action		
	Cookie Map	URL Map	Header Map	Client ...	Server Farm	Backup Serve...	Sticky ...
AUTO-POL8	COOK-1						

<lab> <15> Tue May 04 14:39:04 PDT 2004

To monitor the individual Virtual Servers:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Virtual Servers** under the **Services Dashboard**. Click the virtual server for which you want to view configuration details.

Or:

Step 1 Click **Setup** from the task bar, then click **Virtual Servers** in the left-most pane.

Step 2 Select **Virtual Servers** from the object selector.

Step 3 Click the virtual server for which you want to view configuration details.

The following fields appear:

Field	Description
Admin Status	Lets you know if the real server is In Service or Out of Service.
Operational Status	Lets you know the operational status of the Virtual Server.
Virtual IP Address	IP Address of the Virtual Server.
Protocol	Type of IP Protocol used. You can choose between Any, TCP or UDP or enter a number between 1 and 255.
Mask	Type of IP mask. It can be a Class A, Class B, Class C or Class D mask. If it is not specified, the default for network mask is 255.255.255.255.
Port	Port alloted for the traffic. This field is enabled only when you choose TCP or UDP.
VLAN ID	Specifies the VLAN for incoming traffic.
Service Type	Specifies the service type.
Advertise	
Advertise Virtual IP	Select this to advertise a virtual IP.
Advertise only if reals are active	Select this to advertise only if real servers are active.

Field	Description
Enable HTTP Persistence	Select this to enable or disable HTTP persistence for connections in the virtual server.
Enable Unidirectional Traffic	Select this to enable unidirectional traffic.

The following tabs appear:

- Policies
- Default Policy
- Backup Server Farm
- Client and Sticky Connections
- Other Parameters

Policies

Click **Policies** to view the details of various policies.

The following fields appear:

s

Field	Description
Policy Name	Policy associated with a virtual server.
Conditions	
Cookie Map	Name of the cookie map associated with a policy. Only one Cookie map can be associated with a policy.
URL Map	Name of the URL map associated with a policy. Only one URL map can be associated with a policy.
Header Map	Name of the Header map associated with a policy. Only one Header map can be associated with a policy.
Client Group	Client group can either be standard access lists names or an ID between 1 to 99. Only one client-group can be associated with a given SLB policy.
Action	
Server Farm	Name of the server farm associated to the real server. You can choose one server farm and/or backup server farm to associate to the Policy.
Backup Server Farm	
Sticky Group	Number identifying the sticky group to which the virtual server belongs.
Reverse Sticky Group	Number identifying the reverse sticky group to which the virtual server belongs.

Default Policy

Click **Default Policy** to view the details of the default policy.

The following fields appear:

Server Farm	
Associated Real Servers	
Real	Real Server associated to the Server farms through policies.
Minimum Connections	Minimum number of connections to the real server.
Maximum Connections	Maximum number of connections to the real server.
Weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Admin Status	Lets you know the status of the real server.

Backup Server Farm

Click **Backup Server Farm** to view the details of the default policy.

The following fields appear:

Backup Server Farm	
Associated Real Servers	
Real	Real Server associated to the Server farms through policies.
Minimum Connections	Minimum number of connections to the real server.
Maximum Connections	Maximum number of connections to the real server.
Weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Admin Status	Lets you know the status of the real server.

Client and Sticky Connections

Click **Client / Sticky Connections** to view details of the restricted clients and the details related to sticky connections.

The following fields appear:

Field	Description
Client Restriction	
IP Address	IP Address of the client.
Mask	Specify the type of IP mask. It can be from Class A, Class B, Class C or Class D masks. If it is not specified, the default for network mask is 255.255.255.255.
Exclude	Select the client to exclude traffic from it.
Sticky Connections	
Sticky Timer	Specifies the period of time (in minutes) that the sticky information is kept.
Mask	Specifies if it is a Class A, Class B, Class A and Class D mask. If it is not specified, the default for network mask is 255.255.255.255.
Sticky Group	Sticky Group associated with the Virtual Server.
Reverse Sticky	Number identifying the reverse sticky group to which the virtual server belongs.
SSL Sticky	
Offset	The offset for the SSL ID.
Length	The length of the SSL ID.

Other Parameters

Click **Other Parameters** to view details of performance, load and traffic related parameters.

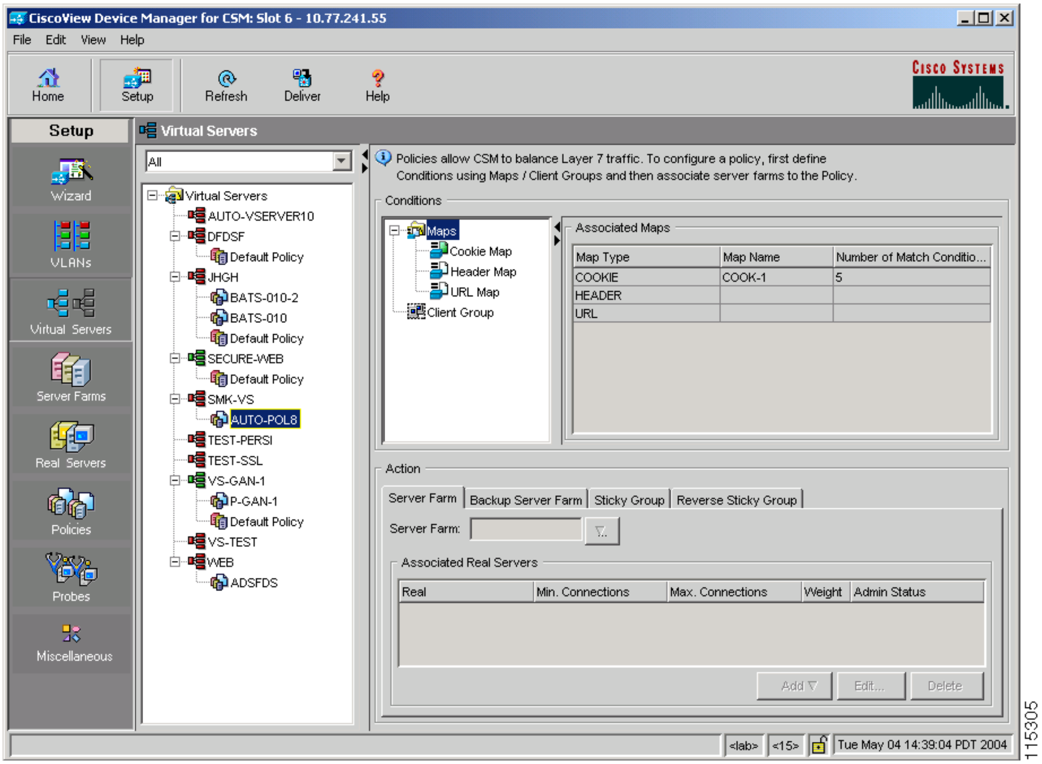
The following fields appear:

Field	Description
Performance/Load Parameters	
Idle Timer	Duration of the idle connection timer (in seconds).
Pending Timeout	Time (in seconds) to wait before a connection is considered unreachable.
Parse Length	Maximum number of bytes to parse for URLs and cookies.
Maximum Connections	Maximum number of connections to the real server.
URL Hash	
Begin Pattern	Specifies the beginning pattern of the URL to parse.
End Pattern	Specifies the ending pattern of the URL to parse.
Connection/Traffic Parameters	
Enable HTTP Persistence	Enable or disable HTTP persistence for connections in the virtual server.
Enable Unidirectional Traffic	Enable unidirectional traffic.

Viewing a Policy

You can view the details of the conditions and actions of the policy associated with each Virtual Server.

Figure 4-3 Virtual Server - Policy Page



Policies allow CSM to balance Layer 7 traffic. To configure a policy, first define Conditions using Maps / Client Groups and then associate server farms to the Policy.

Map Type	Map Name	Number of Match Conditio...
COOKIE	COOK-1	5
HEADER		
URL		

Server Farm:

Real	Min. Connections	Max. Connections	Weight	Admin Status

To the view the conditions and actions of each of the policies associated with individual Virtual Servers:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Virtual Servers** under the **Services Dashboard**. Select the required Virtual Server and click the policy associated with it.

Or:

Step 1 Click **Setup** from the task bar, then click **Virtual Servers** in the left-most pane.

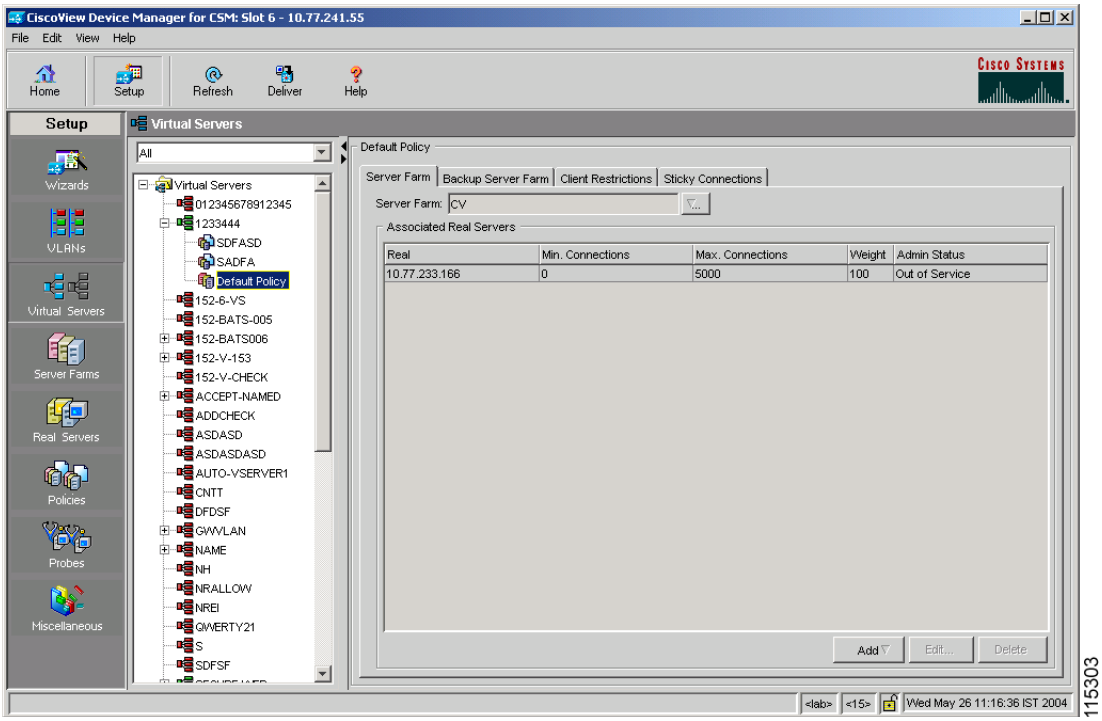
Step 2 Select **Virtual Servers** from the object selector. Select the required Virtual Server and click the policy associated with it.

For more information on policies associated with the individual Virtual Servers see "Viewing Policy Nodes" section on page 7-13.

Viewing a Default Policy

You can view the details of the default policy associated with each Virtual Server.

Figure 4-4 Virtual Server - Default Policy Page



Server Farm: CV

Real	Min. Connections	Max. Connections	Weight	Admin Status
10.77.233.166	0	5000	100	Out of Service

To view the details of the default policy associated with the individual Virtual Servers:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Virtual Servers** under the **Services Dashboard**.

Step 3 Select the required Virtual Server and click the default policy associated with it.

Or:

Step 1 Click **Setup** from the task bar, then click **Virtual Servers** in the left-most pane.

Step 2 Select **Virtual Servers** from the object selector. Select the required Virtual Server and click the default policy associated with it.

The following tabs appear:

- Server Farms
- Backup Server Farms
- Restricted Clients
- Sticky Connections

Server Farms

Click **Server Farms** to view details of all the Server Farms that are associated to a policy.

The following fields appear:

Field	Description
Server Farm	You can create or choose one Server Farm to associate to the Policy. Click ▽... and select one of the following: • **Select Server Farm** to select a Server Farm from the list. • **Create Server Farm** to create a Server Farm. For more information on creating Server Farms, see "Adding Server Farms" section on page 5-4.

From this dialog, you can access functions to do the following:

- Click **Add** and do one of the following:

- Select **Create Named Real Server** to create a named real server. For more information, see "Adding Named Real Server" section on page 5-17.
- Select **Create Unnamed Real Server** to create an unnamed real server. For more information, see "Adding Unnamed Real Server" section on page 5-20.

- Select a Real Server and click **Edit** to edit the configuration values.
- Select a Real Server and click **Delete** to delete the Real Server.

For more information on Server Farms, see "Viewing Server Farms" section on page 5-2.

Backup Server Farms

Click **Backup Server Farms** to view details of all the Backup Server Farms that are associated to this policy.

The following fields appear:

Field	Description
Backup Server Farm	You can create or choose one Backup Server Farm to associate to the Policy. Click ▽... and select one of the following: • **Select Server Farm** to select a Backup Server Farm from the list. • **Create Server Farm** to create a or Backup Server Farm. For more information on creating Server Farms, see "Adding Server Farms" section on page 5-4.

From this dialog, you can access functions to do the following:

- Click **Add** and do one of the following:

  - Select **Create Named Real Server** to create a named real server. For more information, see "Adding Named Real Server" section on page 5-17.
  - Select **Create Unnamed Real Server** to create an unnamed real server. For more information, see "Adding Unnamed Real Server" section on page 5-20.
- Select a Real Server and click **Edit** to edit the configuration values.
- Select a Real Server and click **Delete** to delete the Real Server.

For more information on Server Farms, see "Viewing Server Farms" section on page 5-2.

Restricted Clients

Click **Restricted Clients** to add details of the restricted clients.

The following details are displayed:

Field	Description
IP Address	IP Address of the client.
Mask	Specify the type of IP mask. It can be from Class A, Class B, Class C or Class D masks. If it is not specified, the default for network mask is 255.255.255.255.
Exclude	Select the client to exclude traffic from it.

Sticky Connections

Click **Sticky Connections** to add details of the sticky connections.

The following details are displayed:

Field	Description
Sticky Timer	Specifies the period of time (in minutes) that the sticky information is kept.
Mask	From the list, select From the list, select Class A, Class B, Class A and Class D masks. If it is not specified, the default for network mask is 255.255.255.255.
Sticky Group	Specify the Sticky Group associated with the Virtual Server.
Reverse Sticky Group	Enter the number identifying the reverse sticky group to which the virtual server belongs.
SSL Sticky	
Offset	Enter the offset for the SSL ID.
Length	Enter the length of the SSL ID.

Managing Server Farms

The managing Server Farms page has two sections Server Fams and NAT Pools, for more details see:

- Server Farms, page 5-1
- NAT Pools, page 5-28

Server Farms

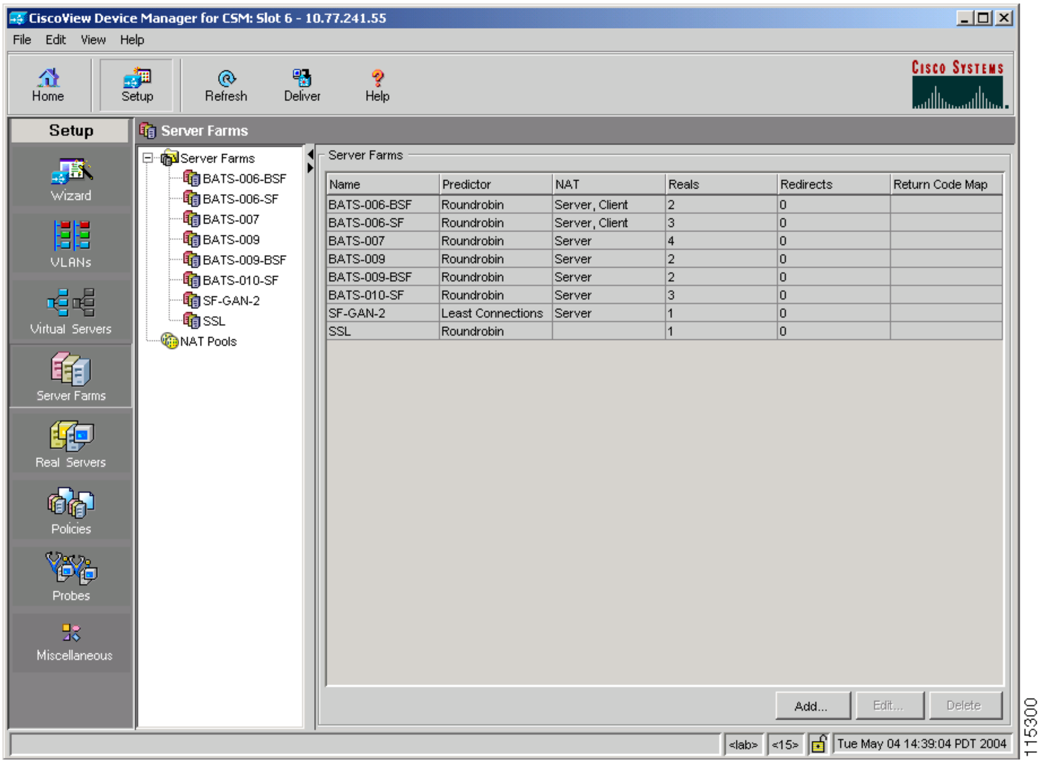
A server farm (or server pool) is a collection of servers that contain the same content. You can specify the server farm name when you configure the server farm and add real servers.

Related Topics:

- Viewing Server Farms, page 5-2
- Adding Server Farms, page 5-4
  - Adding Named Real Server, page 5-17
  - Adding Unnamed Real Server, page 5-20
  - Adding Redirect Virtual Server, page 5-24
- Editing Server Farms, page 5-9
  - Editing a Real Server, page 5-22
  - Editing Redirect Virtual Servers, page 5-26
- Viewing Server Farm Node, page 5-14

Viewing Server Farms

Figure 5-1 Server Farms Page



Name	Predictor	NAT	Reals	Redirects	Return Code Map
BATS-006-BSF	Roundrobin	Server, Client	2	0	
BATS-006-SF	Roundrobin	Server, Client	3	0	
BATS-007	Roundrobin	Server	4	0	
BATS-009	Roundrobin	Server	2	0	
BATS-009-BSF	Roundrobin	Server	2	0	
BATS-010-SF	Roundrobin	Server	3	0	
SF-GAN-2	Least Connections	Server	1	0	
SSL	Roundrobin		1	0	

To view Server Farms:

Step 1 Click **Home** at the top of the window.

Step 2 Click **Server Farms** under **Services Dashboard**.

Or:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Server Farms** in the left-most pane. The following details are shown in the content area.

Field	Description
Name	Name of the server farm about which information is being displayed. Information about each server farm is displayed on a separate line.
Predictor	Type of load-balancing algorithm used by the server farm.
NAT	Shows whether server and client NAT (Network Address Transalation) is enabled.
Reals	Number of real servers configured in the server farm.
Redirects	Shows the number of redirect virtual servers configured in the server farm.
Return Code Map	Return code map name associated with the server farm.

From this section, you can access functions to do the following:

- Click **Add** to add Server Farms. For more information, see "Adding Server Farms" section on page 5-4.
- Select a node and click **Edit** to edit a Server Farm. For more information, see "Editing Server Farms" section on page 5-9.
- Select a node and click **Delete** to delete the Server Farm.

Adding Server Farms

To add Server Farms:

Step 1 Click **Home** at the top of the window.

Step 2 Click **Server Farms** under **Services Dashboard**.

Step 3 Click the **Add** button provided at the end of the table to create a new Server Farm.

Or:

Step 1 Click **Setup** from the task bar and click **Server Farms** in the left-most pane.

Step 2 Click the **Add** button provided at the end of the table to create a new Server Farm. The Add Server Farm dialog box has the following tabs:

- General
- Real Server
- Health Checkup
- Redirect Virtual Server

General

In the **General** tab, the following details are displayed:

Field	Descriptions
Name	Enter the name of the Server Farm.
Load Balancing Algorithm	Specify the load-balancing algorithm for the server farm from the list. Based on the load balancing algorithm the traffic will be diverted to the respective real server. The fields **Mask Type** and **Mask** are applicable only for Hash Address algorithm type.
NAT	Select the check box to specify Client NAT or Server NAT. When client NAT is enabled you must specify the corresponding client NAT pool.

Real Server

In the **Real Servers** tab, the following details are displayed:

Fields	Description
Real	Number of real servers configured in the server farm.
Min. Connections	The minimum number of connections for the real server.
Max. Connections	The maximum number of connections for the real server.
Weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Admin Status	Lets you know if the real server is in service or out of service.

From this page, you can click **Add** to add new named or unnamed real server. For more information on adding named and unnamed real servers, see

- "Adding Named Real Server" section on page 5-17
- "Adding Unnamed Real Server" section on page 5-20

Health Checkup

In the **Health Checkup** tab, the following details are displayed:

Field	Description
Fail Action	Specify the fail action criteria. Choose among None, Purge, and Reassign.
HTTP Return Code	Specify the return code map.
Inband Health Checkup	Select the check box to activate the following fields. • Number of Retries-Enter the number of retries. • Retry Interval (in seconds)- Enter the retry interval span in seconds.
Associate Probes	You can associate or disassociate a probe to the server farm.

Redirect Virtual Server

In the **Redirect Virtual Server** tab, the following details are displayed:

Field	Description
Name	The name of the redirect virtual server.
SSL Port	SSL port number; the range is from 1 to 65535.
Status	Status of the redirect virtual server.

From this page, you can access functions to do the following:

- Add a new redirect virtual server. For more information, see "Adding Redirect Virtual Server" section on page 5-24.
- Select a row and click **Delete** to delete a Redirect Virtual Server.

Editing Server Farms

To edit selected Server Farm details:

Step 1 Click **Home** at the top of the window.

Step 2 Click **Server Farms** under **Services Dashboard**.

Step 3 Select the server farm node. The details are displayed in the right pane.

Step 4 Click **Edit** to launch the Edit Server Farms dialog box.

Or:

Step 1 Click **Setup** from the task bar, then select Server Farms from the left-most pane. The Server Farm details appear in the content pane.

Step 2 Select the Sever Farm Node. The details are displayed on the right pane.

Step 3 Click **Edit** to launch the Edit Server Farms dialog box. The Edit Server Farm dialog box has the following tabs:

- General
- Real Server
- Health Checkup
- Redirect Virtual Server

General

In the **General** tab the following details are displayed:

Fields	Descriptions
Name	The name of the Server Farm.
Load Balancing Algorithm	Specify the load-balancing algorithm for the server farm from the list. Based on the load balancing algorithm the traffic will be diverted to the respective real server. The fields **Mask Type** and **Mask** are applicable only for Hash Address algorithm type.
NAT	Select the check box to specify Client NAT or Server NAT. When client NAT is enabled you must specify the corresponding client NAT pool.

Real Server

In the **Real Servers** tab the following details are displayed:

Fields	Description
Real	Number of real servers configured in the server farm.
Min. Connections	The minimum number of connections for the real server.
Max. Connections	The maximum number of connections for the real server.
Weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Admin Status	Lets you know if the real server is in service or out of service.

From this section, you can click **Edit** to edit a real server. For more information on editing real servers see "Editing a Real Server" section on page 5-22.

Health Checkup

In the **Health Checkup** tab, the following details are displayed:

Field	Description
Fail Action	Specify the fail action criteria. Choose among None, Purge, and Reassign.
HTTP Return Code	Specify the return code map.
Inband Health Checkup	Select the check box to activate the following fields. • Number of Retries-Enter the number of retries. • Retry Interval (in seconds)- Enter the retry interval span in seconds.
Associate Probes	You can associate or disassociate a probe to the server farm.

Redirect Virtual Server

In the **Redirect Virtual Server** tab, the following details are displayed:

Field	Description
Name	The Name of the redirect virtual server.
SSL Port	SSL port number; the range is from 1 to 65535.
Status	Status of the redirect virtual server.

From this section click **Edit** to edit a redirect virtual server. For more information on editing Redirect Virtual Servers see "Editing Redirect Virtual Servers" section on page 5-26.

Viewing Server Farm Node

To view Server Farm Nodes:

Step 1 Click **Home** at the top of the window.

Step 2 Click **Server Farms** under **Services Dashboard**.

Step 3 Select the **Server Farm Node** from the object selector. The details are shown on the content area.

Or:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Server Farms** on the left-most pane.

Step 3 Select the **Server Farm Node** in the object selector. The details are shown on the content area. The following fields are displayed:

Field	Description
Predictor	
Load-balancing Algorithm	The load-balancing algorithm for the server farm. Based on the load balancing algorithm the traffic will be diverted to the respective real server. The fields **Mask Type** and **Mask** are applicable only for Hash Address algorithm type.
NAT	Displays Client NAT and Server NAT status. When client NAT is enabled the corresponding client NAT pool is displayed.
Real Server	
Real Server Name	The name of the Real Server.
Min. Connections	The minimum number of connections for thereal server.
Max. Connections	The maximum connections for the real server.
Weight	The weight of the real server.
Admin Status	The admin status of the real server farm with respect to this server farm.
Operational Status	The operational status of the real server farm with respect to this server farm.
Set Admin Status	Click this button to set the state of the Server instantly.
Health Checkup	
Fail Action	The course of action determind for the server farm in case of failure.
HTTP Return Code	The HTTP return code map for the server farm.
Inband Health Checkup	

Field	Description
Number of Retries	The number of retries for the real server.
Retry Interval	The time duration for which the retry occurs.
Associate Probes	The list of probes associated with the server farm.

From the Server Farm Node page, you can access functions to do the following:

- Select a real server and click **Set Admin Status** to set its state instantly.
- Click the **Redirect Virtual Server** button you can add or edit a redirect virtual server. For more information, see:
  - "Adding Redirect Virtual Server" section on page 5-24
  - "Editing Redirect Virtual Servers" section on page 5-26
- Select a redirect virtual server and click **Delete** to delete a redirect virtual server.
- Click **Edit** to edit server farms. For more information, see "Editing Server Farms" section on page 5-9.

Adding Named Real Server

To add a named Real server.

Step 1 Click **Home** at the top of the window.

Step 2 Click **Server Farms** under **Services Dashboard**.

Step 3 Click the **Add** button provided at the end of the table.

Step 4 In the Add Server Farm dialog box, select **Real Server**.

Step 5 Click the **Add** button provided at the end of the table, and specify **Select Named Real Server**.

Or:

Step 1 Click **Setup** from the task bar and click **Server Farm** in the left-most pane.

Step 2 Click the **Add** button provided at the end of the table.

Step 3 In the Add Server Farm dialog box select **Real Server**.

Step 4 Click the **Add** button provided at the end of the table and specify **Select Named Real Server**. The following fields are displayed:

Field	Description
Name	From the list, select the name of the named real server.
Port	Enter the port number.
Min. Connections	Enter the minimum number of connections for the real server.
Max. Connections	Enter the maximum number of connections for the real server.
Weight	Enter the weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Redirect Virtual Server	Click ▽... and do one of the following: • Select redirect virtual server from the table. • Create a redirect virtual server. • Clear an exisitng redirect virtual server.
Status	Specify the status of the real server.
Back Up Real Server	
Name	Click ▽... and do one of the following: • Select named real server from the table. • Select an unnamed real server. • Clear an exisitng backup real server.
Port	Displays the backup real server port number.
Probe	

Field	Description
Probe Name	Click ▽... and do one of the following: • Select probe from the table. • Create probe. • Clear an existing probe.
Tag	Enter the tag for the probe.

Adding Unnamed Real Server

To add an unnamed Real Server.

Step 1 Click **Home** at the top of the window.

Step 2 Click **Server Farms** under **Services Dashboard**.

Step 3 Click the **Add** button provided at the end of the table.

Step 4 In the Add Server Farm dialog box select **Real Server**.

Step 5 Click the **Add** button provided at the end of the table and specify **Add Unnamed Real Server**.

Or:

Step 1 Click **Setup** from the task bar and click **Server Farm** in the left-most pane.

Step 2 Click the **Add** button provided at the end of the table.

Step 3 In the Add Server Farm dialog box select **Real Server**.

Step 4 Click the **Add** button provided at the end of the table and specify **Add Unnamed Real Server**. The following fields are displayed:

Field	Description
IP Address	Enter the IP address of the destination.
Port	Decimal TCP/UDP port number (from 0 to 65535) or port name.
Minimum Connections	Enter the minimum number of connections to the real server.
Maximum Connections	Enter the maximum number of connections to the real server.
Weight	Enter the weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Redirect Virtual Server	Choose one real server from the list.
Status	Specify the status of the real server.
Backup Real Server	
Name	From the list, select the name of backup real server.
Port	Enter the decimal TCP/UDP port number (from 0 to 65535) or port name.
Probe	
Name	From the list, select the name of probe.
Tag	Enter the tag for the probe.

Editing a Real Server

To edit a Real server.

Step 1 Click **Home** at the top of the window.

Step 2 Click **Server Farms** under **Services Dashboard**.

Step 3 Click the **Add** button provided at the end of the table.

Step 4 In the **Add Server Farm** dialog box select **Real Server**.

Step 5 Click the **Edit** button provided at the end of the table.

Or:

Step 1 Click **Setup** from the task bar and click **Server Farm** in the left-most pane.

Step 2 Click the **Add** button provided at the end of the table.

Step 3 In the Add Server Farm dialog box select **Real Server**.

Step 4 Click the **Edit** button provided at the end of the table. The following fields are displayed:

Field	Description
Min. Connections	Minimum number of connections to the real server.
Max. Connections	Maximum number of connections to the real server.
Weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
Redirect Virtual Server	Choose a real server from the list.
Status	Lets you know if the Real Server is in service, out of service or in service standby.
Back Up Real Server	
Name	Choose a backup server farm from the list.
Port	Decimal TCP/UDP port number (from 0 to 65535) or port name.
Probe	
Name	Choose a probe name from the list.
Tag	Specify a tag for the probe.

From this page, you can click **Delete** to delete a Real Server.

Adding Redirect Virtual Server

To add a Redirect Virtual Server:

Step 1 Click **Home** at the top of the window.

Step 2 Click **Server Farms** under **Services Dashboard**.

Step 3 Click the **Add** button provided at the end of the table.

Step 4 In the Add Server Farm dialog box select **Redirect Virtual Server**.

Step 5 Click the **Add** button provided at the end of the table.

Or:

Step 1 Click **Setup** from the task bar and click **Server Farm** in the left-most pane.

Step 2 Click the **Add** button provided at the end of the table.

Step 3 In the Add Server Farm dialog box select **Redirect Virtual Server**.

Step 4 Click the **Add** button provided at the end of the table.

The following fields are displayed:

Field	Description
Name	Specify the name of the Redirect virtual server.
SSL Port	SSL port number. The range is from 1 to 65535.
Status	Specify the status of the Redirect Virtual Server.
Back Up	
Response	Specify the backup response.
HTTP Status Code	Select the HTTP status code.
Relocation	
Response	Specify the relocation response.
HTTP Status Code	Select the HTTP Status Code.

Editing Redirect Virtual Servers

To edit a Redirect Virtual Server:

Step 1 Click **Home** at the top of the window.

Step 2 Click **Server Farms** under **Services Dashboard**.

Step 3 Click the **Add** button provided at the end of the table.

Step 4 In the Add Server Farm dialog box select **Redirect Virtual Server**.

Step 5 Click the **Edit** button provided at the end of the table.

Or:

Step 1 Click **Setup** from the task bar and click **Server Farm** in the left-most pane.

Step 2 Click the **Add** button provided at the end of the table.

Step 3 In the Add Server Farm dialog box select **Redirect Virtual Server**.

Step 4 Click the **Edit** button provided at the end of the table.

The following fields are displayed:

Field	Description
Name	Specify the name of the Redirect virtual server.
SSL Port	SSL port number. The range is from 1 to 65535.
Status	Edit the status of the Redirect Virtual Server.
Back Up	
Response	Specify the back up response.
HTTP Status Code	Select the HTTP Status Code.
Relocation	
Response	Specify the relocation response.
HTTP Status Code	Select the HTTP Status Code.

NAT Pools

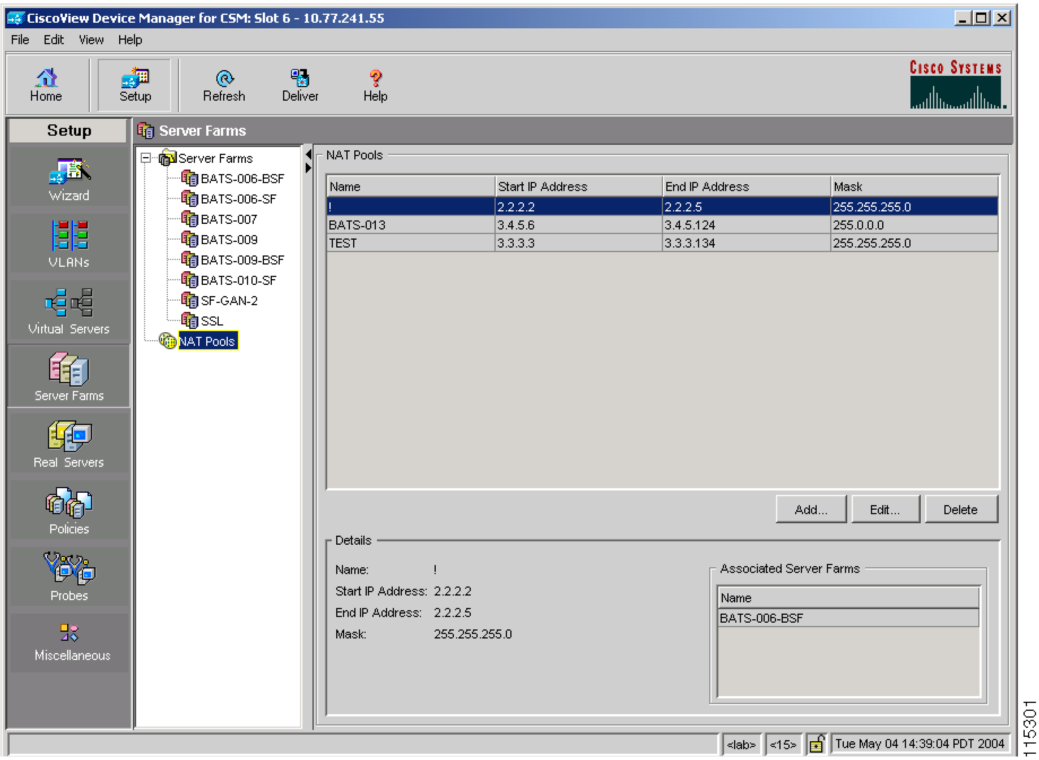
When you configure client Network Address Translation (NAT) pools, NAT converts the source IP address of the client requests into an IP address on the server-side VLAN. You can configure NAT pool with range of IP Addresses. To configure NAT pool with single IP Address, you can give Starting IP and Ending IP as the same.

Related Topics:

- Viewing NAT Pools, page 5-29
- Adding NAT Pools, page 5-31
- Editing NAT Pools, page 5-32

Viewing NAT Pools

Figure 5-2 NAT Pools



Name	Start IP Address	End IP Address	Mask
!	2.2.2.2	2.2.2.5	255.255.255.0
BATS-013	3.4.5.6	3.4.5.124	255.0.0.0
TEST	3.3.3.3	3.3.3.134	255.255.255.0

Name: !
Start IP Address: 2.2.2.2
End IP Address: 2.2.2.5
Mask: 255.255.255.0

Name
BATS-006-BSF

To view NAT Pools:

Step 1 Click **Home** at the top of the window.

Step 2 Click **Server Farms** under **Services Dashboard**.

Step 3 Click **NAT Pools**.

Or:

Step 1 Click **Setup** from the task bar and click **Server Farm** in the left-most pane.

Step 2 Click **NAT Pools**. The details are displayed on the content pane. The following fields are displayed:

Field	Description
Name	Name of the NAT Pool.
Start IP Address	The start IP Address of the NAT Pool.
End IP Address	The end IP Address of the NAT Pool.
Mask	The mask IP of the NAT Pool.
Details	
Name	Name of the NAT Pool.
Start IP Address	The start IP Address of the NAT Pool.
End IP Address	The end IP Address of the NAT Pool.
Mask	The mask IP of the NAT Pool.
Associated Server Farms	
Name	Displays the name of the Server Farm that has this NAT pool associated with it.

From this section, you can access functions to do the following:

- Click **Add** to add NAT Pools. For more information, see "Adding NAT Pools" section on page 5-31.
- Select a node and click **Edit** to edit NAT Pools. For more information, see "Editing NAT Pools" section on page 5-32.
- Select a node and click **Delete** to delete the NAT Pool.

Adding NAT Pools

To add NAT Pools:

Step 1 Click **Home** at the top of the window.

Step 2 Click **Server Farms** under **Services Dashboard**.

Step 3 Click **NAT Pools**.

Step 4 Click the **Add** button at the end of the content pane.

Step 5 The Add NAT Pool dialog box pops up.

Or:

Step 1 Click **Setup** from the task bar and click **Server Farm** in the left-most pane.

Step 2 Click **NAT Pools**.

Step 3 Click the **Add** button at the end of the content pane.

Step 4 The Add NAT Pool dialog box pops up and the following fields are displayed:

Field	Description
Name	The name of the NAT Pool.
Start IP Address	The start IP Address of the NAT Pool.
End IP Address	The end IP Address of the NAT Pool.
Mask	The mask IP of the NAT Pool.

Note To create a NAT pool with a single IP address provide the same IP address for the Start and End IP address field.

Editing NAT Pools

To edit NAT Pools:

Step 1 Click **Home** at the top of the window.

Step 2 Click **Server Farms** under **Services Dashboard**.

Step 3 Click **NAT Pools**.

Step 4 Click the **Edit** button at the end of the content pane.

Step 5 The Edit NAT Pool dialog box pops up.

Or:

Step 1 Click **Setup** from the task bar and click **Server Farm** in the left-most pane.

Step 2 Click **NAT Pools**.

Step 3 Click the **Edit** button at the end of the content pane.

Step 4 The Edit NAT Pool dialog box pops up and the following fields are displayed:

Field	Description
Name	The name of the NAT Pool. You cannot edit this field.
Start IP Address	The start IP Address of the NAT Pool.
End IP Address	The end IP Address of the NAT Pool.
Mask	The mask IP of the NAT Pool.

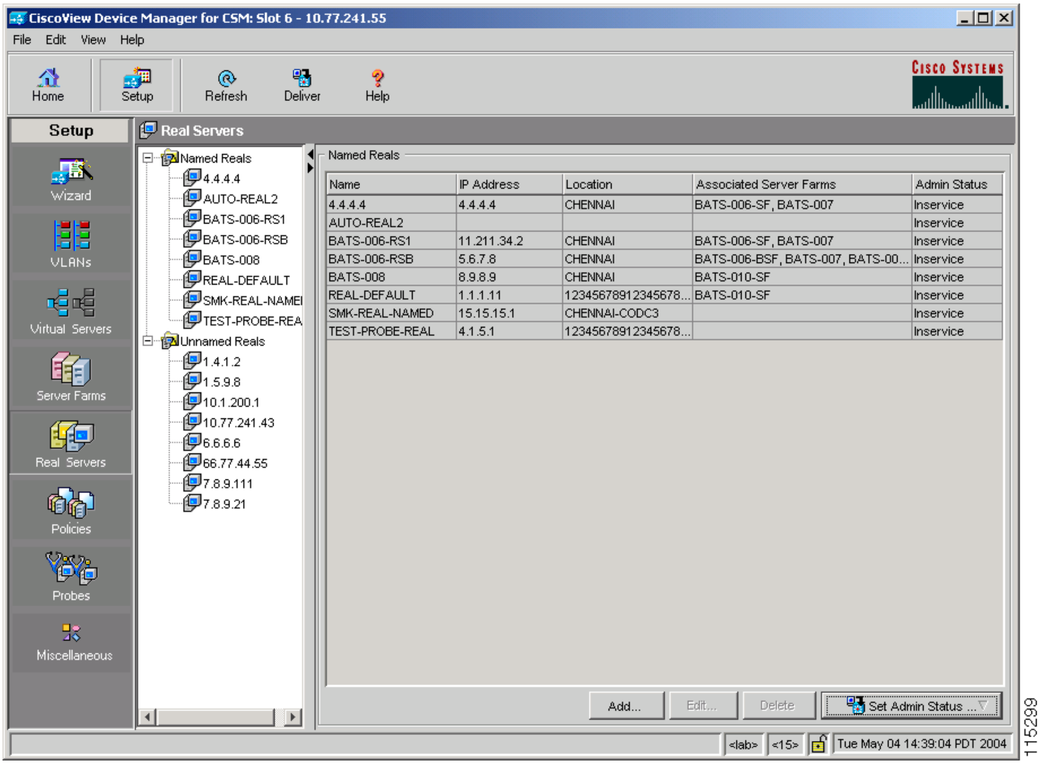
Managing Real Servers

Real servers are physical devices that are assigned to a server farm and provides services that are load balanced.

This section includes the following topics:

Viewing Named Real Servers

Figure 6-1 Named Real Servers Page



Name	IP Address	Location	Associated Server Farms	Admin Status
4.4.4.4	4.4.4.4	CHENNAI	BATS-006-SF, BATS-007	Inservice
AUTO-REAL2				Inservice
BATS-006-RS1	11.211.34.2	CHENNAI	BATS-006-SF, BATS-007	Inservice
BATS-006-RSB	5.6.7.8	CHENNAI	BATS-006-BSF, BATS-007, BATS-00...	Inservice
BATS-008	8.9.8.9	CHENNAI	BATS-010-SF	Inservice
REAL-DEFAULT	1.1.1.11	12345678912345678...	BATS-010-SF	Inservice
SMK-REAL-NAMED	15.15.15.1	CHENNAI-CODC3		Inservice
TEST-PROBE-REAL	4.1.5.1	12345678912345678...		Inservice

You can view information about all the existing Real Server details on the device.

To view Named Real Servers:

Step 1 Click **Home** at the top of the window.

Step 2 Click **Real Servers** under **Services Dashboard**.

Or:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Real Servers** from the left-most pane.

The following fields appear.

:

Field	Description
Name	The name of the Real Server.
IP Address	The IP Address of the Real Server.
Location	The location of the Real Server.
Associated Server Farms	The real server associated with the server farms.
Admin Status	Status of the real server.
Add	Lets you add a new Real Server.
Edit	Lets you edit a Real Server.
Delete	Lets you delete a Real Server.
Set Admin Status	Lets you set the admin status. When you select the options you will be prompted with a confirmation box. Click on **Yes** to set the appropriate admin status. Select **No** to keep the admin status unchanged.

From the Real Server page, you can access functions to do the following

- Add a new Real Server. For more information, see "Adding a Real Server" section on page 6-8.
- Edit a Real Server. For more information, see "Editing a Real Server" section on page 6-9.
- Click the **Delete** button to delete a named Real Server.

Viewing Named Real Servers Node

To view Named Real Servers Node.

Step 1 Click **Home** at the top of the window.

Step 2 Click **Real Servers** under **Services Dashboard**.

Step 3 Select a named Real Server.

Or:

Step 1 Click **Setup** from the task bar and click **Named Real Servers** in the left-most pane.

Step 2 Select a named Real Server.

The following files appear:

Field	Description
Real Server Name	The name of the Real Server.
Location	The location of the Real Server.
Real Server IP Address	IP address of the Real Server.
Admin Status	Status of the Real Server.
Server Farm	The name of the Server Farm to which the real server is associated.
Port	The port number of the real server.
Min. Connections	The minimum connections for the real server.
Max. Connections	The maximum connections for the real server.
Weight	The weight of the real server.
Admin Status	The admin status of the real server with respect to the server farm.
Operational Status	The operational status of the real server with respect to the server farm.
Set Admin Status	Lets you set the admin status. When you select the options you will be prompted with a confirmation box. Click on **Yes** to set the appropriate admin status. Select **No** to keep the admin status unchanged.
Details	The details pertaining to the named real server.

Viewing Unnamed Real Servers

To view Unnamed Real Servers.

Step 1 Click **Home** at the top of the window.

Step 2 Click **Real Servers** under **Services Dashboard**.

Step 3 Click **Unnamed Real Servers** in the left-most pane.

Or:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Unnamed Real Servers** in the left-most pane.

The following fields appear:

Field	Description
Real	The name or IP address of the Real Server.
Associated Server Farms	The Server Farm associated with the Real Server.

Note You can create unnamed real servers only inside a server farm.

Viewing an Unnamed Real Servers Node

Note You can congfigure Unnamed Real Servers only within a Server Farm.

To view Unnamed Real Servers Node.

Step 1 Click **Home** at the top of the window.

Step 2 Click **Real Server** under **Services Dashboard**.

Step 3 Select an unnamed Real Server.

Or:

Step 1 Click **Setup** from the task bar and click **Unnamed Real Servers** in the left-most pane.

Step 2 Select an unnamed Real Server.

The following fields appear:

Field	Description
Real Server IP Address	IP address of the Real Server.
Server Farm	The name of the Server Farm to which the real server is associated.
Port	The port number of the real server.
Min. Connections	The minimum connections for the real server.
Max. Connections	The maximum connections for the real server.
Weight	The weight of the real server.
Admin Status	The admin status of the real server with respect to the server farm.
Operational Status	The operational status of the real server with respect to the server farm.

Field	Description
Set Admin Status	Lets you set the admin status. When you select the options you will be prompted with a confirmation box. Click on **Yes** to set the appropriate admin status. Select **No** to keep the admin status unchanged.
Details	The details pertaining to the named real server.

Adding a Real Server

To add Real Servers.

Step 1 Click **Home** at the top of the window.

Step 2 Click **Real Server** under **Services Dashboard**.

Step 3 Click the **Add** button provided at the end of the table to create a new Real Server.

Or:

Step 1 Click **Setup** from the task bar and click **Real Servers** in the left-most pane.

Step 2 Click the **Add** button provided at the end of the table to create a new Real Server.

The following fields appear:

Field	Description
Name	Enter the name of the Real Server.
IP Address	Enter the IP Address of the Real Server.
Location	Enter the location of the Real Server.
Status	Specify the status.

Editing a Real Server

To edit Real Server information:

Step 1 Click **Home** at the top of the window.

Step 2 Click **Real Server** under **Services Dashboard**.

Step 3 From the table, select the Real Server that you want to modify.

Step 4 Click the **Edit** button provided at the end of the table to edit a Real Server.

Or:

Step 1 Click **Setup** from the task bar, click **Real Servers** in the left-most pane.

Step 2 From the table, select the Real Server that you want to modify.

Step 3 Click the **Edit** button provided at the end of the table to edit a Real Server.

The following fields appear:

Field	Description
IP Address	Enter the IP Address of the Real Server.
Location	Enter the location of the Real Server.
Service	Specify the status.

Managing Policies

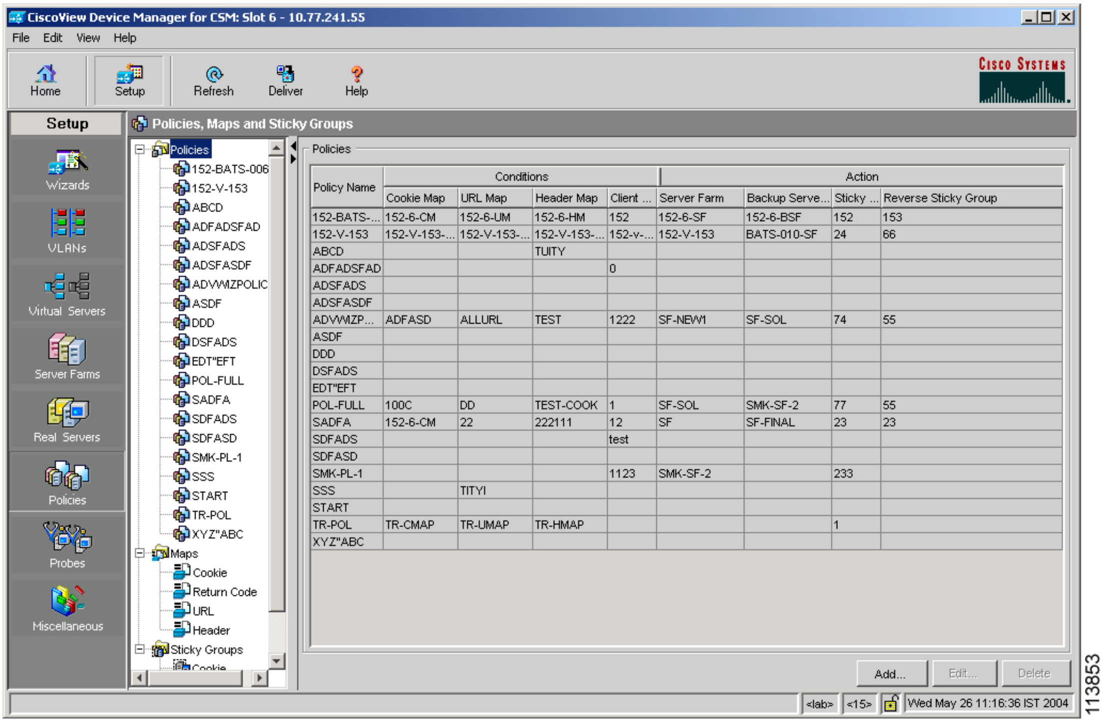
Policies are access rules that traffic must match when load balancing to a server farm. Policies allow the CSM to balance Layer 7 traffic. Multiple policies can be assigned to one virtual server, creating multiple access rules for that virtual server.

When configuring policies, you must first configure the access rules (maps and / or client-groups) and then you combine these access rules under a particular policy.

This section includes the following topics:

Viewing Policies

Figure 7-1 Policies Page



Policies

Policy Name	Conditions				Action			
	Cookie Map	URL Map	Header Map	Client ...	Server Farm	Backup Serve...	Sticky ...	Reverse Sticky Group
152-BATS-...	152-6-CM	152-6-UM	152-6-HM	152	152-6-SF	152-6-BSF	152	153
152-V-153	152-V-153-...	152-V-153-...	152-V-153-...	152-v-...	152-V-153	BATS-010-SF	24	66
ABCD			TUITY					
ADFADSFAD				0				
ADSFADS								
ADSFASDF								
ADVWIZP...	ADFASD	ALLURL	TEST	1222	SF-NEW1	SF-SOL	74	55
ASDF								
DDD								
DSFADS								
EDT"EFT								
POL-FULL	100C	DD	TEST-COOK	1	SF-SOL	SMK-SF-2	77	55
SADFA	152-6-CM	22	222111	12	SF	SF-FINAL	23	23
SDFADS				test				
SDFASD								
SMK-PL-1				1123	SMK-SF-2		233	
SSS		TITYI						
START								
TR-POL	TR-CMAP	TR-UMAP	TR-HMAP				1	
XYZ"ABC								

You can view all policies configured in the device.

To view policies:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Policies** under the **Services Dashboard**.

Or:

Step 1 Click **Setup** from the task bar, then click **Policies** in the left-most pane.

Step 2 Select **Policies** from the object selector.

The following fields appear:

s

Field	Action/Description
Policy Name	Policy associated with a virtual server.The string is limited to 15 characters.
Conditions	
Cookie Map	Name of the cookie map associated with a policy. Only one Cookie map can be associated with a policy.
URL Map	Name of the URL map associated with a policy. Only one URL map can be associated with a policy.
Header Map	Name of the Header map associated with a policy. Only one Header map can be associated with a policy.
Client Group	Client-group can be either standard access-list name or ID (from 1 to 99). Only one client-group can be associated with a given SLB policy.
Action	
Server Farm	Name of the server farm associated to the real server. You can choose one Server Farm and/or Backup Server Farm to associate to the Policy.
Backup Server Farm	
Sticky Group	Number identifying the sticky group to which the virtual server belongs.
Reverse Sticky	Ensures that CSM switches connections in the opposite direction back to the original source.

From the main Policies page, you can access functions to do the following:

- Click **Add** to add new policies. For more information, see "Adding Policies" section on page 7-4.
- Click **Edit** to edit policies. For more information, see "Editing Policies" section on page 7-9.
- Select a row and click **Delete** to delete policies.

Adding Policies

You can add a policy, and you can associate one map of each type and one Sticky group to the policy.

To create new policies:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Click **Add** to add policies.

Or:

Step 1 Click **Setup** from the task bar, then click **Policies** in the left-most pane.

Step 2 Select **Policies** from the object selector.

Step 3 Click **Add** to add policies.

The following fields appear:

Field	Description
Policy Name	Enter the policy associated with a virtual server. The string is limited to 15 characters.
Cookie Map	From the list, select the name of the cookie map to be associated with the policy. Only one Cookie map can be associated with a policy. Click ▽... and select one of the following: • **Select Cookie Map** to select from a list of configured Cookie Maps. • **Create Cookie Map** to create a Cookie Map. For more information on creating Cookie Maps, see "Adding a Cookie Map" section on page 8-9. • **Clear Cookie Map** to clear the field.
URL Map	From the list, select the name of the URL map to be associated with the policy. Only one URL map can be associated with a policy Click ▽... and select one of the following: • **Select URL Map** to select from a list of configured URL Maps. • **Create URL Map** to create a URL Map. For more information on creating URL Maps, see "Adding a URL Map" section on page 8-23. • **Clear URL Map** to clear the field.

Field	Description
Header Map	From the list, select the name of the Header map to be associated with the policy. Only one Header map can be associated with a policy. Click ▽... and select one of the following: • **Select Header Map** to select from a list of configured Header Maps. • **Create Header Map** to create a Header Map. For more information on creating Header Maps, see "Adding a Header Map" section on page 8-26. • **Clear Header Map** to clear the field.
Client Group	From the list, select the client group number or name. Only one client-group can be associated with a given server-load balancing (SLB) policy. Click ▽... and select one of the following: • **Create Client Group** to create a Client group. Enter the Client group ID or Name. • **Clear Client Group** to clear the Client group.
Server Farm	
Server Farm	From the list, select the name of the server farm associated to the real server. You can choose one Server Farm to associate to the Policy. Click ▽... and select one of the following: • **Select Server Farms** to select from a list of configured Server Farms. • **Create Server Farms** to create the Server Farms. For more information on creating Server Farms, see "Adding Server Farms" section on page 5-4. • **Clear Server Farms** to clear the field.

Field	Description
Backup Server Farm	From the list, select the name of the backup server farm associated to the real server. You can choose one Backup Server Farm to associate to the Policy. Click ▽... and select one of the following: • **Select Server Farms** to select from a list of configured Backup Server Farms. • **Create Server Farms** to create the Backup Server Farm. For more information on creating Backup Server Farm, see "Adding Server Farms" section on page 5-4. • **Clear Server Farms** to clear the field.
Sticky	Select this check box to ensure that connections from the same client that match the same SLB policy use the same real server on subsequent connections.
Sticky Group	

Field	Description
Sticky Group	From the list, select the number identifying the sticky group to which the virtual server belongs. The range is from 0 to 255. Click ▽... and select one of the following: • **Select Sticky Groups** to select from a list of configured Sticky Groups. • **Create Sticky Groups** to create Sticky Groups. For more information on creating Sticky Groups, see "Adding a Sticky Group" section on page 9-5. • **Clear Sticky Groups** to clear the field.
Reverse Sticky Group	From the list, select the number identifying the reverse sticky group to which the virtual server belongs. The range is from 0 to 255. Click ▽... and select one of the following: • **Select Sticky Groups** to select from a list of configured Sticky Groups. • **Create Sticky Groups** to create Sticky Groups. For more information on creating Sticky Groups, see "Adding a Sticky Group" section on page 9-5. • **Clear Sticky Groups** to clear the field.

Editing Policies

To edit policies:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Select a row in the table and click **Edit** to launch Edit dialog for the selected Policy.

Or:

Step 1 Click **Setup** from the task bar, then click **Policies** in the left-most pane.

Step 2 Select **Policies** from the object selector.

Step 3 Select a row in the table and click **Edit** to launch Edit dialog for the selected Policy.

The following fields appear:

Field	Description
Policy Name	Name of the policy associated with a virtual server. The string is limited to 15 characters.
Cookie Map	From the list, select the name of the cookie map associated with a policy. Only one Cookie map can be associated with a policy. Click ▽... and select one of the following: • **Select Cookie Map** to select from a list of configured cookie maps. • **Create Cookie Map** to create a Cookie Map. For more information on creating Cookie Maps, see "Adding a Cookie Map" section on page 8-9. • **Clear Cookie Map** to clear the field.
URL Map	From the list, select the name of the URL map associated with a policy. Only one URL map can be associated with a policy. Click ▽... and select one of the following: • **Select URL Map** to select from a list of configured URL Maps. • **Create URL Map** to create a URL Map. For more information on creating URL Maps, see "Adding a URL Map" section on page 8-23. • **Clear URL Map** to clear the field.
Header Map	From the list, select the name of the Header map associated with a policy. Only one Header map can be associated with a policy. Click ▽... and select one of the following: • **Select Header Map** to select from a list of configured Header Maps. • **Create Header Map** to create a Header Map. For more information on creating Header Maps, see "Adding a Header Map" section on page 8-26. • **Clear Header Map** to clear the field.

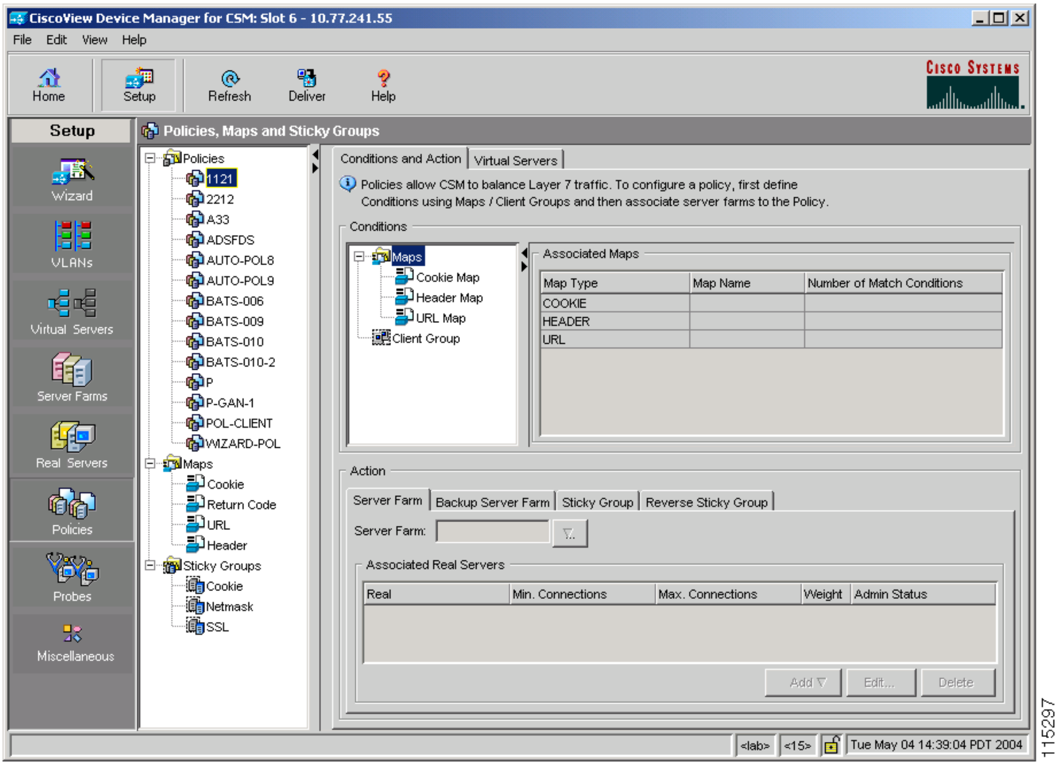
Field	Description
Client Group	From the list, select the client group number or name. Only one client-group can be associated with a given server-load balancing (SLB) policy. Click ▽... and select one of the following: - **Create Client group** to create a Client group. Enter the Client group ID. - **Clear Client group** to clear the Client group.
Server Farm	
Server Farm	From the list, select the name of the server farm associated to the real server. You can choose one Server Farm to associate to the Policy. Click ▽... and select one of the following: - **Select Server Farms** to select from a list of configured Server Farms. - **Create Server Farms** to create the Server Farms. For more information on creating Server Farms, see "Adding Server Farms" section on page 5-4. - **Clear Server Farms** to clear the field.
Backup Server Farm	From the list, select the name of the backup server farm associated to the real server. You can choose one Backup Server Farm to associate to the Policy. Click ▽... and select one of the following: - **Select Server Farms** to select from a list of configured Backup Server Farms. - **Create Server Farms** to create the Backup Server Farm. For more information on creating Backup Server Farm, see "Adding Server Farms" section on page 5-4. - **Clear Server Farms** to clear the field.
Sticky	Select this to ensure that connections from the same client that match the same SLB policy use the same real server on subsequent connections.
Sticky Group	

Field	Description
Sticky Group	From the list, select the number identifying the sticky group to which the virtual server belongs. Click ▽... and select one of the following: • **Select Sticky Groups** to select from a list of configured Sticky Groups. • **Create Sticky Groups** to create Sticky Groups. For more information on creating Sticky Groups, see "Adding a Sticky Group" section on page 9-5. • **Clear Sticky Groups** to clear the field.
Reverse Sticky Group	From the list, select the number identifying the reverse sticky group to which the virtual server belongs. Click ▽... and select one of the following: • **Select Sticky Groups** to select from a list of configured Sticky Groups. • **Create Sticky Groups** to create Sticky Groups. For more information on creating Sticky Groups, see "Adding a Sticky Group" section on page 9-5. • **Clear Sticky Groups** to clear the field.

Viewing Policy Nodes

You can view all policies configured in the device.

Figure 7-2 Policy Node Page



Policies allow CSM to balance Layer 7 traffic. To configure a policy, first define Conditions using Maps / Client Groups and then associate server farms to the Policy.

Map Type	Map Name	Number of Match Conditions
COOKIE		
HEADER		
URL		

Real	Min. Connections	Max. Connections	Weight	Admin Status

To view policies:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Click any of the Policy nodes.

Or:

Step 1 Click **Setup** from the task bar, then click **Policies** in the left-most pane.

Step 2 Select **Policies** from the object selector. Click any of the Policy nodes.

The following tabs appear:

- Conditions And Action
- Virtual Servers

Conditions And Action

Click **Conditions and Action** to see the various conditions and their actions. The fields under the Conditions table will change when you select the different maps and client groups.

When you click **Maps**, you will see a table with a summary of details of all the associated maps like map type, name, and the number of map conditions. You can associate the different types of maps when you click **Cookie Maps**, **Header Maps**, or **URL Maps** under **Maps** .

The following fields appear when you click **Maps**:

Field	Description
Map Type	Specifies if it a Cookie, Header or a URL type map.
Map Name	Name of the map.
Number of Match Conditions	Specifies the total number of match conditions.

Note When you click the Map tree, a list of maps and icons are displayed. The icons have a color status display, for example, the icons are white by default. When you associate a map to it, it turns green. This icon is displayed for all the three types of maps, such as, Cookie, Header, and URL maps.

You have the following types of **Conditions**:

- Cookie Maps
- Header Maps

- URL Maps
- Client Group

Cookie Maps

From the **Conditions** tab, when you choose the **Cookie Maps** the following fields appear:

Field	Description
Cookie Map	Name of the cookie map associated with the policy selected in the object selector. Click ▽... and select one of the following: • **Select Cookie Map** to select from a list of configured Cookie Maps. • **Create Cookie Map** to create Cookie Maps. For more information on creating Cookie Maps, see "Adding a Cookie Map" section on page 8-9. • **Clear Cookie Map** to clear the field.
Cookie Name	Cookie Name String. This is limited to 15 characters.
Cookie Value	Cookie Value

From this page, you can access functions to do the following:

- Click **Add** to add new match conditions by entering the name and value.
- Click **Edit** to edit match conditions.
- Select a match condition and click **Delete** to delete it.

Header Maps

From the **Conditions** tab, when you choose the **Header Maps** the following fields appear:

Field	Description
Header Map	Click ▽... and select one of the following: • **Select Header Map** to select from a list of configured Header Maps. • **Create Header Map** to create Header Maps. For more information on creating Header Maps, see "Adding a Header Map" section on page 8-26. • **Clear Header Map** to clear the field.
Header Name	The Header name. The string is limited to 15 characters.
Header Value	The Header Value.

From this page, you can access functions to do the following:

- Click **Add** to add new header fields and values by entering the name and value.
- Click **Edit** to edit the header fields and values.
- Select a row and click **Delete** to delete it.

URL Maps

From the **Conditions** tab, when you choose the **URL Maps** the following fields appear:

Field	Description
URL Map	Click ▽... and select one of the following: • **Select URL Map** to select from a list of configured URL Maps. • **Create URL Map** to create URL Maps. For more information on creating URL Maps, see "Adding a URL Map" section on page 8-23. • **Clear URL Map** to clear the field.
URL Method	Specifies the method in incoming HTTP requests.
URL	Specifies the URL in incoming HTTP requests.

From this page, you can access functions to do the following:

- Click **Add** to add new URL expressions by entering the name and value.
- Click **Edit** to edit the URL expressions.
- Select a row and click **Delete** to delete it.

Client Group

From the **Conditions** tab, when you choose the **Client Group** the following fields appear:

Field	Description
Client Group	Client-group can be either standard access-list name or ID (from 1 to 99). Only one client group can be associated with a given server-load balancing (SLB) policy. Click ▽... and select one of the following: • **Create Client Group** to create Client Group by entering the Client Group ID. • **Clear Client Group** to clear the field.

Action

The following tabs appear under the **Actions** section:

- Server Farms and Backup Server Farms
- Sticky Group
- Reverse Sticky Group

Server Farms and Backup Server Farms

Note You can configure a Backup Server Farm only after you configure a Server Farm.

Click **Server Farms** and/or **Backup Server Farms** to view all the Server Farms and Backup Server Farm that are associated to this policy.

The following fields appear:

Field	Description
Server Farm/Backup Server Farm	You can choose one Server Farm and/or Backup Server Farm to associate to the Policy. Click ▽... and select one of the following: • **Select Server Farm** to select from a list of configured Server Farms. • **Create Server Farm** to create Server Farms or Backup Server Farms. For more information on creating Server Farms, see "Adding Server Farms" section on page 5-4. • **Clear Server Farm** to clear the field.

From this dialog, you can access functions to do the following:

- Click **Add** and do one of the following:

  - Select **Create Named Real Server** to create a named real server. For more information, see "Adding Named Real Server" section on page 5-17.
  - Select **Create Unnamed Real Server** to create an unnamed real server. For more information, see "Adding Unnamed Real Server" section on page 5-20.
- Select a Real Server and click **Edit** to edit the configuration values.
- Select a Real Server and click **Delete** to delete the Real Server.

For more information on Server Farms, see "Viewing Server Farms" section on page 5-2.

Sticky Group

Click **Sticky Groups** to view all the sticky groups that are associated to this policy.

The following fields appear:

Field	Description
Sticky Groups	Number identifying the sticky group to which the virtual server belongs. The range is from 0 to 255. Click ▽... and select one of the following: • **Select Sticky Groups** to select from a list of configured Sticky Groups. • **Create Sticky Groups** to create Sticky Groups. For more information on creating Sticky Groups, see "Adding a Sticky Group" section on page 9-5. • **Clear Sticky Groups** to clear the field.
Type	Type of Sticky Group.
Timeout	Time in seconds to wait before a connection is considered unreachable.

Reverse Sticky Group

Click **Reverse Sticky Groups** to view all the Sticky Group that are associated to this policy.

The following fields appear:

Field	Description
Reverse Sticky Groups	Number identifying the sticky group to which the virtual server belongs. The range is from 0 to 255. Click ▽... and select one of the following: • **Select Sticky Groups** to select from a list of configured Sticky Groups. • **Create Sticky Groups** to create Sticky Groups. For more information on creating Sticky Groups, see "Adding a Sticky Group" section on page 9-5. • **Clear Sticky Groups** to clear the field.
Type	Type of reverse sticky group.
Timeout	Time in seconds to wait before a connection is considered unreachable.

Virtual Servers

Click the **Virtual Servers** tab to view the details of all the virtual servers to which the policy selected in the object selector is associated to. For more information on Virtual Servers, see "Viewing Virtual Servers" section on page 4-2.

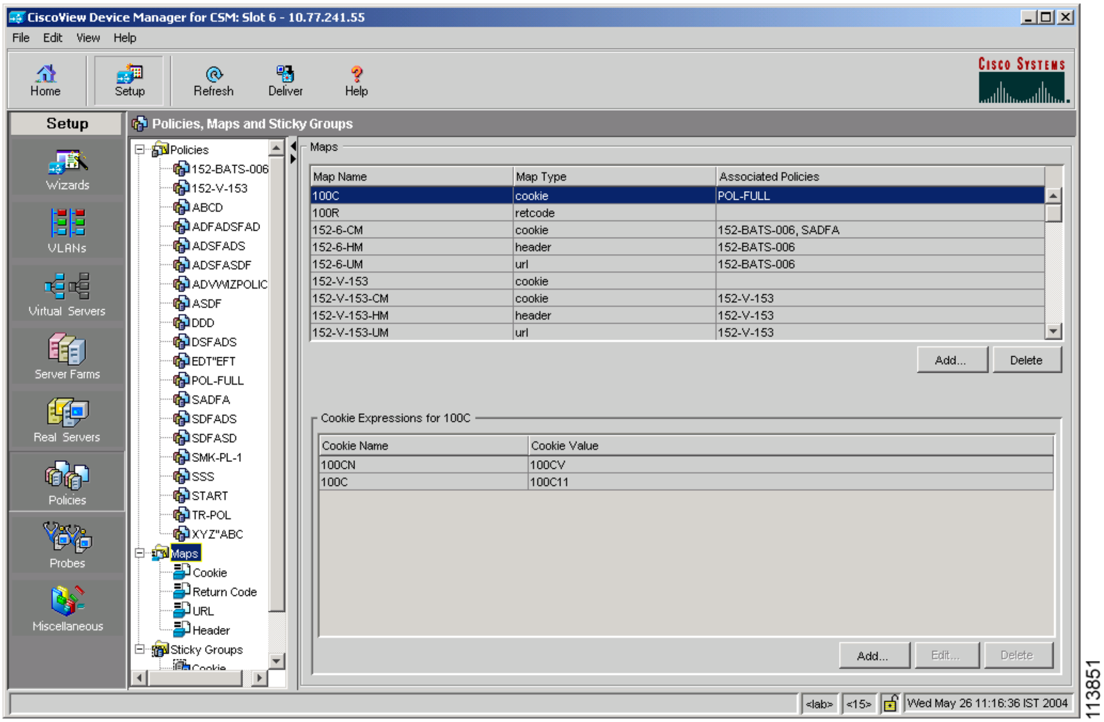
Managing Maps

You can configure maps to define multiple URLs, cookies, HTTP headers, and return codes as groups that can be associated with a policy when configured.

This section contains the following topics:

Viewing Maps

Figure 8-1 Maps Page



Maps

Map Name	Map Type	Associated Policies
100C	cookie	POL-FULL
100R	retcode	
152-6-CM	cookie	152-BATS-006, SADFA
152-6-HM	header	152-BATS-006
152-6-UM	url	152-BATS-006
152-V-153	cookie	
152-V-153-CM	cookie	152-V-153
152-V-153-HM	header	152-V-153
152-V-153-UM	url	152-V-153

Cookie Expressions for 100C

Cookie Name	Cookie Value
100CN	100CV
100C	100C11

You can view information about all Maps on the device.

To view the maps:

Step 1 Click **Home** at the top of the window

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Click **Maps**. A table with details of all configured Maps appears.

Or:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Policies > Maps**, the screen is displayed on the right pane.

Step 3 Click **Maps**. A table with details of all configured Maps appears.

The following fields are displayed:

Field	Description
Map Name	Displays the map name.
Map Type	Displays the type for the corresponding map name.
Associated Policies	Displays the associated policies for the map type.
Add	Click this button to add new map names and map types. For more information, see the "Adding a Map" section on page 8-6.
Delete	Select the Map Name you wish to delete and click on this button to delete the existing map type.

The lower pane of the Map window displays the various match conditions of the selected map.

The match conditions will differ according to the type of map that you select in the table.

1. If you choose Cookie Map, the following fields appear:

Field	Description
Cookie Name	Name of the cookie.
Cookie Value	Value of the cookie.

From this section, you can access functions to do the following:

- Click **Add** to add cookie match conditions by entering the cookie name and value.

- Click **Edit** to edit cookie match conditions.
- Select a match condition, then click **Delete** to delete the cookie match conditions.

2. If you choose Return Code Map, the following fields appear:

Field	Description
Match Conditions	
Lowest Return Code	The lowest return code.
Highest Return Code	The highest return code.
Action for Return Codes	Action for the return code.
Return Code Instances	Instances of the return code.
Reset Time after Threshold	Time for the reset.

From this section, you can access functions to do the following:

- Click **Add** to add match conditions. For more information, see "Adding Match Conditions for a Return Code Map" section on page 8-15.
- Click **Edit** to edit cookie match conditions.
- Select a match condition, then click **Delete** to delete the match condition.

3. If you choose URL Map, the following fields appear:

Field	Description
URL Method	The URL method to be used.
URL	The URL associated with the map.

From this section, you can access functions to do the following:

- Click **Add** to add URL expressions by entering the URL method and URL.
- Click **Edit** to edit URL expressions.
- Select a URL expression, then click **Delete** to delete it.

4. If you choose Header Map, the following fields appear:

Field	Description
Header Name	Name of the header.
Header Value	Value of the header.

From this section, you can access functions to do the following:

- Click **Add** to add header match conditions by entering the cookie name and value.
- Click **Edit** to edit header match conditions.
- Select a header match condition, then click **Delete** to delete the match condition.

From the main Maps page, you can access functions to do the following:

- Click **Add** to add a new Map. For more information, see "Adding a Map" section on page 8-6.
- Select a row and click **Delete** to delete a Map.
- View a Cookie Map. For more information, see "Viewing Cookie Maps" section on page 8-7.
- View a Return Code Map. For more information, see "Viewing Return Code Maps" section on page 8-11.
- View a URL Map. For more information, see "Viewing URL Maps" section on page 8-21.
- View a Header Map. For more information, see "Viewing Header Maps" section on page 8-24.

Adding a Map

To add a map:

Step 1 Click **Home** at the top of the window

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Click **Maps**. A table with details of all configured Maps appears.

Step 4 Click **Add**. The Add Map dialog box appears.

Or:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Policies**, the Policies screen is displayed in the right pane.

Step 3 Click **Maps**. A table with details of all configured Maps appears

Step 4 Click **Add**. The Add Map dialog box appears.

The following fields are displayed:

Field	Description
Map Type	Specify the map type. The map types are, Cookies, Header, URL, and Return Code.
Map Name	Enter the map name.

The fields will differ according to the type of map that you select in the table.

For more information on adding a Cookie Map, see "Adding a Cookie Map" section on page 8-9.

For more information on adding a Return Code Map, see "Adding a Return Code Map" section on page 8-13.

For more information on adding a URL Map, see "Adding a URL Map" section on page 8-23.

For more information on adding a Header Map, see "Adding a Header Map" section on page 8-26.

Viewing Cookie Maps

To view Cookie maps:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Policies**, the Policies screen is displayed in the right pane.

Step 3 Click **Maps**. A table with details of all configured Maps appears.

Step 4 Select **Cookie Maps** from the object selector.

The following fields appear:

Field	Description
Map Name	Enter the map name.
Associated Policies	The policy associated to the Cookie Map.

From the main Cookie Map page, you can access functions to do the following:

- Click **Add** to add a new Cookie Map. For more information, see "Adding a Cookie Map" section on page 8-9.
- Select a row and click **Delete** to delete a Cookie Map.

Step 5 Select one of the map names from the table.

The following information is displayed:

Field	Description
Cookie Expressions	
Cookie Name	The name of the cookie map.
Cookie Value	The value of the cookie map.

From this section, you can access functions to do the following:

- Click **Add** to add cookie match condition to enter the Cookie Name and Value. For more information see the table below **Step 6** in "Adding a Cookie Map" section on page 8-9.
- Click **Edit** to edit the cookie value.
- Select a Cookie Name, then click **Delete** to delete a Cookie.

Adding a Cookie Map

To add a new Cookie Map:

Step 1 Click **Home** at the top of the window.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Click **Maps.** A table with details of all configured Maps appears.

Step 4 Select **Cookie Maps** from the object selector.

Step 5 Click the **Add** button provided at the end of the table to add a new Cookie Map.

Or:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Policies**, the Policies screen is displayed in the right pane.

Step 3 Click **Maps.** A table with details of all configured Maps appears.

Step 4 Select **Cookie Maps** from the object selector.

Step 5 Click the **Add** button provided at the end of the table. The Add Cookie Map page is displayed and the following fields appear:

Field	Description
Cookie Map Name	Enter the cookie map name.

Step 6 To add a cookie name and value click the **Add** button provided at the end of the table. The Match Conditions page is displayed and the following fields appear.

Note The Cookie Map can have a maximum of five match conditions.

Field	Description
Cookie Name	Enter a name for the cookie.
Cookie Value	Enter a value for the cookie.

From this page, you can access functions to do the following:

- Select a row and click **Delete** to delete a Cookie Map.

Viewing Return Code Maps

To view Return Code Map:

Step 1 Click **Home** at the top of the window

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Click **Maps**. A table with details of all configured Maps appears

Step 4 Select **Return Code Map** from the object selector.

Or:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Policies**, the Policies screen is displayed in the right pane.

Step 3 Click **Maps**. A table with details of all configured Maps appears

Step 4 Select **Return Code Map** from the object selector.

The following fields appear:

Field	Description
Map Name	Name of the map
Associated Server Farms	Server Farms associated with the map.

From the main Return Code Map page, you can access functions to do the following:

- Click **Add** to add a new Return Code Map. For more information, see "Adding a Return Code Map" section on page 8-13.
- Select a row and click **Delete** to delete a Return Code Map.

Step 5 Select one of the maps from the table.

The following details appears below:

Field	Description
Match Conditions	
Lowest Return Code	The lowest return code.
Highest Return Code	The highest return code.
Action for Return Codes	Action for the return code.
Return Code Instances	Instances of the return code.
Reset Time after Threshold	Time for the reset.

From this section, you can access functions to do the following:

- Click **Add** to add match conditions. For more information, see "Adding Match Conditions for a Return Code Map" section on page 8-15.
- Click **Edit** to edit match conditions. For more information, see "Editing Match Conditions for a Return Code Map" section on page 8-18.
- Select a match condition, then click **Delete** to delete the match condition.

Adding a Return Code Map

To add a new Return Code:

Step 1 Click **Home** at the top of the window

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Click **Maps**. A table with details of all configured Maps appears.

Step 4 Select **Return Code Map** from the object selector.

Step 5 Click **Add**. The Add Return Code Map dialog box appears.

Or:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Policies**, the Policies screen is displayed in the right pane.

Step 3 Click **Maps.** A table with details of all configured Maps appears.

Step 4 Select **Return Code Map** from the object selector.

Step 5 Click **Add**. The Add Return Code Map dialog box appears.

The following fields appear:

Field	Description
Map Name	Enter a map name. Then click **Add** to add match conditions. For more information, see "Adding Match Conditions for a Return Code Map" section on page 8-15.
Lowest Return Code	The lowest return code for the map.
Highest Return Code	The highest return code for the map.
Action for Return Codes	The action for the return code.
Return Code Instances	This feature is enabled depending on the Action for Return Code. Enter the instances of the return code.
Reset Time after Threshold	The time for the reset.

From this page, you can access functions to do the following:

- Click **Add** to add match conditions. For more information, see "Adding Match Conditions for a Return Code Map" section on page 8-15.
- Select a row and click **Delete** to delete a match condition.

Adding Match Conditions for a Return Code Map

To add match conditions for a Return Code Map:

Step 1 Click **Home** at the top of the window.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Click **Maps.** A table with details of all configured Maps appears.

Step 4 Select **Return Code Map** from the object selector.

Step 5 Click **Add**. The Add Return Code Map dialog box appears.

Step 6 Click **Add** in the dialog box to add match condition for the selected type of Return Code Map.

Or:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Policies**. The Policies screen is displayed in the right pane.

Step 3 Click on **Maps.** A table with details of all configured Maps appears.

Step 4 Select **Return Code Map** from the object selector.

Step 5 Click **Add**. The Add Return Code Map dialog box appears.

Step 6 Click **Add** in the dialog box to add match condition for the selected type of Return Code Map.

The following field appears:

Field	Description
Match Conditions	
Lowest Return Code	Enter the lowest return code. **Note** Overlapping return codes cannot be configured.
Highest Return Code	Enter the highest return code. Maximum no. of return codes that can be configured is 100. **Note** Overlapping return codes cannot be configured. `Example: If you have 100-116,200-216 already, you cannot configure more than (100 - (116-100+1) - (216-200+1) ) = 66. So, you can have 300 -365. If you add 300-366, an error message will popup.`
Action for Return Codes	Action for the return code. You can choose from Count, Log, and Remove. The return code instance and return code reset fields will be enabled only when you choose Remove or Log.
Return Code Instances	Enter the instances of the return code. **Note** This field is disabled if the Action for the Return Code is Count.

Field	Description
Return Code Reset	Select this check box to enable reset time after threshold. **Note** This field is disabled if the Action for the Return Code is Count.
Reset Time after Threshold	Enter the time for the reset.

Editing Match Conditions for a Return Code Map

To edit match conditions for a Return Code Map:

Step 1 Click **Home** at the top of the window.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Click **Maps.** A table with details of all configured Maps appears.

Step 4 Select **Return Code Map** from the object selector.

Step 5 Click **Add**. The Add Return Code Map dialog box appears.

Step 6 Click **Edit** to edit match conditions for the selected Return Code Map.

Or:

Step 1 Click **Setup** from the task bar.

Step 2 Click on **Policies**, the Policies screen is displayed in the right pane.

Step 3 Click on **Maps.** A table with details of all configured Maps appears.

Step 4 Select **Return Code Map** from the object selector.

Step 5 Click **Add**. The Add Return Code Map dialog box appears.

Step 6 Click **Edit** to edit match conditions for the selected Return Code Map.

The following field appears:

Field	Description
Match Conditions	
Lowest Return Code	Modify the lowest return code. **Note** Overlapping return codes cannot be configured.
Highest Return Code	Modify the highest return code. **Note** Overlapping return codes cannot be configured. `Example: If you have 100-116,200-216 already, you cannot configure more than (100 - (116-100+1) - (216-200+1) ) = 66. So, you can have 300 -365. If you add 300-366, an error message will popup.`
Action for Return Codes	Action for the return code. You can choose from Count, Log, and Remove. The return code instance and return code reset fields will be enabled only when you choose Remove or Log.
Return Code Instances	Modify the instances of the return code. **Note** This field is disabled if the Action for the Return Code is Count.

Field	Description
Return Code Reset	Select the check box to reset the time after threshold. **Note** This field is disabled if the Action for the Return Code is Count.
Reset Time after Threshold	Modify the time for the reset.

Viewing URL Maps

To view the URL Maps:

Step 1 Click **Home** at the top of the window

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Click **Maps**. A table with details of all configured Maps appears.

Step 4 Select **URL Maps** from the object selector.

Or:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Policies**, the Policies screen is displayed in the right pane.

Step 3 Click **Maps**. A table with details of all configured Maps appears.

Step 4 Select **URL Maps** from the object selector.

The following fields appear:

Field	Description
Map Name	The name of the map
Associated Policies	Policies associated with the map.

From the main URL Map page, you can access functions to do the following:

- Click **Add to** add a new URL Map. For more information, see "Adding a URL Map" section on page 8-23.
- Select a row and click **Delete** to delete a URL Map.

Step 5 Select one of the maps from the table.

The following information is displayed:

Field	Description
Match Conditions	
URL Method	URL Method to be used.
URL	URL associated with the map.

From this section, you can access functions to do the following:

- Click **Add** to add match condition to enter the URL method and URL. For more information see the table below **Step 6** in "Adding a URL Map" section on page 8-23.
- Click **Edit** to edit the match conditions to edit the URL.
- Select a URL expression, then click **Delete** to delete a match condition.

Adding a URL Map

To add a new URL Map:

Step 1 Click **Home** at the top of the window

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Click **Maps.** A table with details of all configured Maps appears

Step 4 Select **URL Maps** from the object selector.

Step 5 Click the **Add** button provided at the end of the table to add a new URL Map.

Or:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Policies**, the Policies screen is displayed in the right pane.

Step 3 Click **Maps.** A table with details of all configured Maps appears

Step 4 Select **URL Maps** from the object selector.

Step 5 Click the **Add** button provided at the end of the table. The Add URL Map page is appears and the following field is displayed:

Field	Description
URL Map Name	Enter the URL Map Name.

Step 6 To add a URL Method and URL, click the **Add** button provided at the end of the table. The Match Conditions page is displayed and the following fields appear.

Field	Description
URL Method	Click ▽... and from the list select a URL Method or enter the URL Method to be used.
URL	Enter the URL associated with the map.

Viewing Header Maps

To view the Header Maps:

Step 1 Click **Home** at the top of the window

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Click **Maps**. A table with details of all configured Maps appears.

Step 4 Select **Header Maps** from the object selector.

Or:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Policies**, the Policies screen is displayed in the right pane.

Step 3 Click **Maps**. A table with details of all configured Maps appears.

Step 4 Select **Header Maps** from the object selector.

The following fields appear:

Field	Description
Map Name	The name of the map.
Associated Policies	The policies associated with the map.

From the main Header Map page, you can access functions to do the following:

- Click **Add to** add a new Header Map. For more information, see "Adding a Header Map" section on page 8-26.
- Select a map and click **Delete** to delete a Header Map.

Step 5 Select one of the maps from the table.

The following fields appear below:

Field	Description
Match Conditions	
Header Name	The header name of the map.
Header Value	The header value of the map.

From this section, you can access functions to do the following:

- Click **Add** to add match condition to enter the Header name and value. For more details see the table below **Step 6** in "Adding a Header Map" section on page 8-26.
- Click **Edit** to edit the match conditions to edit the Header Value.
- Select a match condition, then click **Delete** to delete a match condition.

Adding a Header Map

To add a new Header Map:

Step 1 Click **Home** at the top of the window

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Click **Maps.** A table with details of all configured Maps appears

Step 4 Select **Header Maps** from the object selector.

Step 5 Click **Add**. The Add Header Map dialog box appears.

Or:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Policies**, the Policies screen is displayed in the right pane.

Step 3 Click **Maps.** A table with details of all configured Maps appears

Step 4 Select **Header Maps** from the object selector.

Step 5 Click **Add**. The Add Header Map dialog box appears and the following field is displayed:

Field	Description
Header Map Name	Click ▽... and from the list and select a Header name or enter a header name.

Step 6 To add a Header Name and Value, click the **Add** button provided at the end of the table. The Match Conditions page is displayed and the following fields appear.

Note The Header Map can have a maximum of five match conditions.

Field	Description
Header Name	Click ▽... and from the list select a Header Name or enter the Header Name to be used.
Header Value	Enter the value for the Header Map.

Managing Sticky Groups

Sticky connections limit traffic to individual servers by allowing multiple connections from the same client to stick to the same real server using source IP addresses, source IP subnets, cookies, and the secure socket layer (SSL) or by redirecting these connections using HTTP redirect messages.

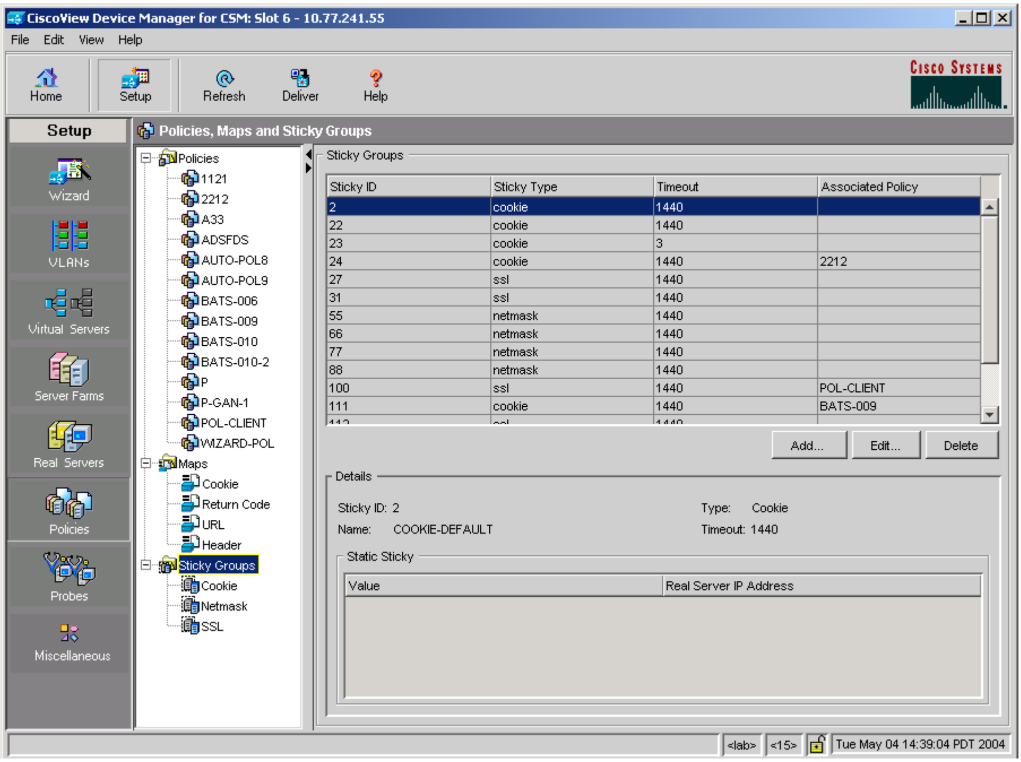
Configuring a sticky group involves configuring the attributes of that group and associating it with a policy. This ensures that connections from the same client matching the same policy use the same real server.

The default sticky time value is 1440 minutes (24 hours).

This section contains the following topics:

Viewing Sticky Groups

Figure 9-1 Sticky Groups Page



Sticky ID	Sticky Type	Timeout	Associated Policy
2	cookie	1440	
22	cookie	1440	
23	cookie	3	
24	cookie	1440	2212
27	ssl	1440	
31	ssl	1440	
55	netmask	1440	
66	netmask	1440	
77	netmask	1440	
88	netmask	1440	
100	ssl	1440	POL-CLIENT
111	cookie	1440	BATS-009
112	ssl	1440	

Sticky ID: 2 Type: Cookie
Name: COOKIE-DEFAULT Timeout: 1440

Value	Real Server IP Address

115296

You can view the existing configuration details in the configuration dialog and edit the specified fields.

To view the Sticky Groups:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Select **Policies > Sticky Groups** from the object selector.

Or:

Step 1 Click **Setup** from the task bar, then click **Policies** in the left-most pane.

Step 2 Select **Policies > Sticky Groups** from the object selector.

The following fields appear:

Field	Action/Description
Sticky ID	Number of the sticky group to which the virtual server belongs.
Sticky Type	Type of Sticky Group. The different types are: • Cookie • SSL • Net Mask
Timeout	Time (in seconds) to wait before a connection is considered unreachable.
Associated Policy	The list of policies to which this sticky group is associated.

Step 3 When you select any row, the configuration details of the corresponding Sticky Group are displayed with the following fields:

Field	Action/Description
Sticky ID	A unique ID for the sticky group.
Name	Name of the sticky group.
Type	Type of sticky group. The different types are: • Cookie • SSL • Net Mask
Value	Value of the static sticky.
Timeout	Time (in seconds) to wait before a connection is considered unreachable.

Field	Action/Description
Static Sticky	
Value	Value of the static sticky.
Real Server IP Address	IP Address of the real server.

Step 4 Select **Cookie**, **SSL**, or **Netmask** from the object selector under **Sticky Groups**, to view the configuration details of the corresponding Sticky Group.

From the main Sticky Group page, you can access functions to do the following:

- Click **Add to** add a new Sticky Group. For more information, see "Adding a Sticky Group" section on page 9-5.
- Click **Edit** to edit a Sticky Group. For more information, see "Editing a Sticky Group" section on page 9-6.
- View an SSL Sticky Group. For more information, see "Viewing SSL Sticky Groups" section on page 9-18.
- View a Netmask Sticky Group. For more information, see "Viewing Netmask Sticky Groups" section on page 9-12.

Adding a Sticky Group

To add a new Sticky Group:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Select **Policies > Sticky Groups** from the object selector.

Or:

Step 1 Click **Setup** from the task bar, then click **Policies** in the left-most pane.

Step 2 Select **Sticky Groups** from the object selector.

Step 3 Click **Add**. The Add Sticky Group dialog box appears.

The following fields appear:

Field	Action/Description
Sticky Type	From the list, select the type of sticky group. The type can be Cookie, SSL, or Netmask.
Sticky ID	Enter the unique ID of the sticky group.
Name	Enter the name of the sticky group.
Timeout	Enter the time (in seconds) to wait before a connection is considered unreachable.
Static Sticky	
Value	Specify the value of the static sticky.
Real Server IP Address	IP Address of the real server.

From this page, you can access functions to do the following:

- Click **Add** to add a static sticky by entering the value and the real IP address.
- Select a row and click **Delete** to delete a static sticky.

Editing a Sticky Group

To edit the configuration values of a selected Sticky Group:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Select **Policies > Sticky Groups** from the object selector.

Or:

Step 1 Click **Setup** from the task bar, then click **Policies** in the left-most pane.

Step 2 Select **Sticky Groups** from the object selector.

Step 3 Do one of the following:

- Click **Edit** to edit the configuration values of the selected type of Sticky Group.
- Double click the selected Sticky Group. The fields that appear in the table could vary, depending on the type of Sticky Group selected.

Step 4 To edit a Cookie Sticky Group, see "Editing a Cookie Sticky Group" section on page 9-10.

To edit a Netmask Sticky Group, see "Editing a Netmask Sticky Group" section on page 9-16.

To edit an SSL Sticky Group, see "Editing an SSL Sticky Group" section on page 9-21.

From this page, you can access functions to do the following:

- Click **Add** to add a static sticky by entering the value and the real IP address.
- Select a row and click **Delete** to delete a static sticky.

Viewing Cookie Sticky Groups

To view the Cookie Sticky Groups:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Select **Policies > Sticky Groups > Cookies** from the object selector.

Or:

Step 1 Click **Setup** at the top of the window, then click **Policies** in the left-most pane.

Step 2 Select **Policies > Sticky Groups > Cookies** from the object selector.

The following fields appear:

Field	Action/Description
Sticky ID	ID number of the sticky group to which the virtual server belongs.
Timeout	Time (in seconds) to wait before a connection is considered unreachable.
Associated Policy	The list of policies to which this sticky group is associated.

Step 3 When you select any row, the configuration details of the corresponding Cookie Sticky Group are displayed with the following fields:

Field	Action/Description
Sticky ID	The unique ID number of the sticky group.
Type	Type of Sticky Group. Here it would be Cookie.
Name	Name of the Cookie Sticky Group.
Timeout	Time (in seconds) to wait before a connection is considered unreachable.
Static Sticky	
Value	Value of the static sticky.
Real Server IP Address	IP Address of the Real Server.

From the main Cookie Sticky Group page, you can access functions to do the following:

- Click **Add** a new Cookie Sticky Group. For more information, see "Adding a Cookie Sticky Group" section on page 9-9.
- Click **Edit** a Cookie Sticky Group. For more information, see "Editing a Cookie Sticky Group" section on page 9-10.
- Select a row and click **Delete** to delete Cookie Sticky Group.

Adding a Cookie Sticky Group

To add a Cookie Sticky Group:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Select **Policies > Sticky Groups > Cookies** from the object selector.

Step 4 Click **Add** to add a new Cookie Sticky Group.

Or:

Step 1 Click **Setup** at the top of the window, then click **Policies** in the left-most pane.

Step 2 Select **Policies > Sticky Groups > Cookies** from the object selector.

Step 3 Click **Add** to add a new Cookie Sticky Group.

The following fields appear:

Field	Action/Description
Sticky ID	Enter the ID number of the sticky group to which the virtual server belongs.
Name	Enter the name of the Cookie Sticky Group.
Timeout	Enter the time (in seconds) to wait before a connection is considered unreachable.
Static Sticky	
Value	Value of the static sticky.
Real Server IP Address	IP Address of the Real Server.

From this page, you can access functions to do the following:

- Click **Add** to add a static sticky by entering the value and real server IP address.

- Select a row and click **Delete** to delete a static route.

Editing a Cookie Sticky Group

To edit a Cookie Sticky Group:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Select **Policies > Sticky Groups > Cookies** from the object selector.

Step 4 Click **Edit** to edit a Cookie Sticky Group.

Or:

Step 1 Click **Setup** at the top of the window, then click **Policies** in the left-most pane.

Step 2 Select **Policies > Sticky Groups > Cookies** from the object selector.

Step 3 Click **Edit** to edit a Cookie Sticky Group.

The following fields appear:

Field	Action/Description
Sticky ID	ID number of the sticky group to which the virtual server belongs. The range is from 0 to 255.
Name	Enter the name of the Cookie Sticky Group. The number of characters can range between 1 to 63.
Type	Type of Sticky Group. Here it will be Cookie.
Timeout	Enter the time (in seconds) to wait before a connection is considered unreachable. The range is from 1 to 65535.
Static Sticky	
Value	Value of the static sticky.
Real Server IP Address	IP Address of the Real Server.

From this page, you can access functions to do the following:

- Click **Add** to add a static sticky by entering the value and real server IP address.
- Select a row and click **Delete** to delete a static route.

Viewing Netmask Sticky Groups

To view Netmask Sticky Groups:

Step 1 Click **Home** at the top of the window

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Select **Policies > Sticky Groups > Netmask** from the object selector.

Or:

Step 1 Click **Setup** at the top of the window, then click **Policies** in the left-most pane.

Step 2 Select **Policies > Sticky Groups > Netmask** from the object selector.

The following fields appear:

Field	Action/Description
Sticky ID	ID of the Netmask Sticky Group.
Timeout	Time (in seconds) to wait, before a connection is considered unreachable.
Associated Policy	Policy associated with the Netmask Sticky Group.

Step 3 When you select any row, the configuration details of the corresponding Netmask Sticky Group are displayed with the following fields:

Field	Action/Description
Sticky ID	ID associated with the Netmask Sticky Group.
Type	Type of Sticky Group. Here it will be Netmask.
Mask Type	It can be source, destination or both.
Mask	Type of IP mask applied. It can be from Class A, Class B, Class C or Class D masks. If it is not specified, the default for network mask is 255.255.255.255.
Timeout	Time (in seconds) to wait before a connection is considered unreachable.
Static Sticky	
Source IP	IP address of the source.
Destination IP	IP address of the destination.
Real Server IP	IP address of the real server.

From this page, you can access functions to do the following:

- Click **Add** to add a Netmask Sticky Group. For more information, see "Adding a Netmask Sticky Group" section on page 9-14.
- Click **Edit** to edit a Netmask Sticky Group. For more information, see "Editing a Netmask Sticky Group" section on page 9-16.
- Select a row and click **Delete** to delete Netmask Sticky Group.

Adding a Netmask Sticky Group

To add a Netmask Sticky Group:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Select **Policies > Sticky Groups > Netmask** from the object selector.

Step 4 Click **Add** to add a new Netmask Sticky Group.

Or:

Step 1 Click **Setup** at the top of the window, then click **Policies** in the left-most pane.

Step 2 Select **Policies > Sticky Groups > Netmask** from the object selector.

Step 3 Click **Add** to add a new Netmask Sticky Group.

The following fields appear:

Field	Action/Description
Sticky ID	Enter the ID of the Netmask Sticky Group.
Mask Type	From the list, select source, destination or both.
Mask	Specify the type of IP mask to be applied. It can be Class A, Class B, Class C or Class D mask. If it is not specified, the default for network mask is 255.255.255.255.
Timeout	Enter the time (in seconds) to wait before a connection is considered unreachable. The range is from 1 to 65535.
Static Sticky	
Source IP	IP address of the source.
Destination IP	IP Address of the destination.
Real Server IP	IP address of the real server.

From this page, you can access functions to do the following:

- Add a static sticky by entering the source IP, destination IP and the real server IP address.
- Select a row and click **Delete** to delete a static sticky.

Editing a Netmask Sticky Group

To edit a Netmask Sticky Group:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Select **Policies > Sticky Groups > Netmask** from the object selector.

Step 4 Click **Edit** to edit a Netmask Sticky Group

Or:

Step 1 Click **Setup** at the top of the window, then click **Policies** in the left-most pane.

Step 2 Select **Policies > Sticky Groups > Netmask** from the object selector.

Step 3 Click **Edit** to edit a Netmask Sticky Group.

The following fields appear:

Field	Action/Description
Sticky ID	ID of the Netmask Sticky Group.
Type	Type of Sticky Group. Here it will be Netmask.
Mask Type	From the list, select source, destination or both.
Mask	Specify the type of IP mask to be applied. It can be Class A, Class B, Class C or Class D masks. If it is not specified, the default for network mask is 255.255.255.255.
Timeout	Enter the time (in seconds) to wait before a connection is considered unreachable. The range is from 1 to 65535.
Static Sticky	
Source IP	IP address of the source.
Destination IP	IP Address of the destination.
Real Server IP	IP address of the real server.

From this page, you can access functions to do the following:

- Click **Add** to add a static sticky by entering the source IP, destination IP and the real server IP address.
- Select a row and click **Delete** to delete a static sticky.

Viewing SSL Sticky Groups

To view the SSL Sticky Groups:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Select **Policies > Sticky Groups** from the object selector.

Or:

Step 1 Click **Setup** at the top of the window, then click **Policies** in the left-most pane.

Step 2 Select **Policies > Sticky Groups > SSL** from the object selector. The configuration table of the SSL Sticky Group is displayed.

The following fields appear:

Field	Action/Description
Sticky ID	Number of the sticky group to which the virtual server belongs.
Timeout	Time (in seconds) to wait before a connection is considered unreachable.
Associated Policy	Policy associated with the SSL Sticky Group.

Step 3 When you select any row, the configuration details of the corresponding SSL Sticky Group are displayed with the following fields:

Field	Action/Description
Sticky ID	ID of the SSL Sticky Group.
Type	Type of Sticky Group. Here it will be SSL.
Timeout	Time (in seconds) to wait before a connection is considered unreachable.
Static Sticky	
SSL ID	ID of the SSL map.
Real Server IP Address	IP Address of the Real Server.

From the main SSL Sticky Group page, you can access functions to do the following:

- Click **Add** to add a new SSL Sticky Group. For more information, see "Adding an SSL Sticky Group" section on page 9-20.
- Click **Edit** to edit an SSL Sticky Group. For more information, see "Editing an SSL Sticky Group" section on page 9-21.
- Select a row and click **Delete** to delete SSL Sticky Group.

Adding an SSL Sticky Group

To create an SSL Sticky Group:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Select **Policies > Sticky Groups** from the object selector.

Step 4 Click **Add** to add a new SSL Sticky Group.

Or:

Step 1 Click **Setup** at the top of the window, then click **Policies** in the left-most pane.

Step 2 Select **Policies > Sticky Groups > SSL** from the object selector.

Step 3 Click **Add** to add a new SSL Sticky Group.

The following fields appear:

Field	Action/Description
Sticky ID	Enter the ID of the SSL Sticky Group.
Timeout	Enter the time (in seconds) to wait before a connection is considered unreachable. The range is from 1 to 65535.
Static Sticky	
SSL ID	ID of the SSL map.
Real Server IP Address	IP Address of the Real Server.

From this page, you can access functions to do the following:

- Click **Add** to add a static sticky by entering the SSL ID and real server IP address.
- Select a row and click **Delete** to delete the static route.

Editing an SSL Sticky Group

To edit an SSL Sticky Group:

Step 1 Click **Home** at the top of the page.

Step 2 Click **Policies** under **Services Dashboard**.

Step 3 Select **Policies > Sticky Groups** from the object selector.

Or:

Step 1 Click **Setup** at the top of the window, then click **Policies** in the left-most pane.

Step 2 Select **Policies > Sticky Groups > SSL** from the object selector.

Step 3 Click **Edit** to edit a SSL Sticky Group.

The following fields appear:

Field	Action/Description
Sticky ID	ID associated with the SSL Sticky Group.
Type	Type of Sticky Group. Here it will be SSL.
Timeout	Enter the time (in seconds) to wait before a connection is considered unreachable. The range is from 1 to 65535.
Static Sticky	
SSL ID	ID of the SSL map.
Real Server IP Address	IP Address of the Real Server.

From this page, you can access functions to do the following:

- Click **Add** to add a static sticky by entering the SSL ID and real server IP address.
- Select a row and click **Delete** to delete a static sticky.

Managing Probes

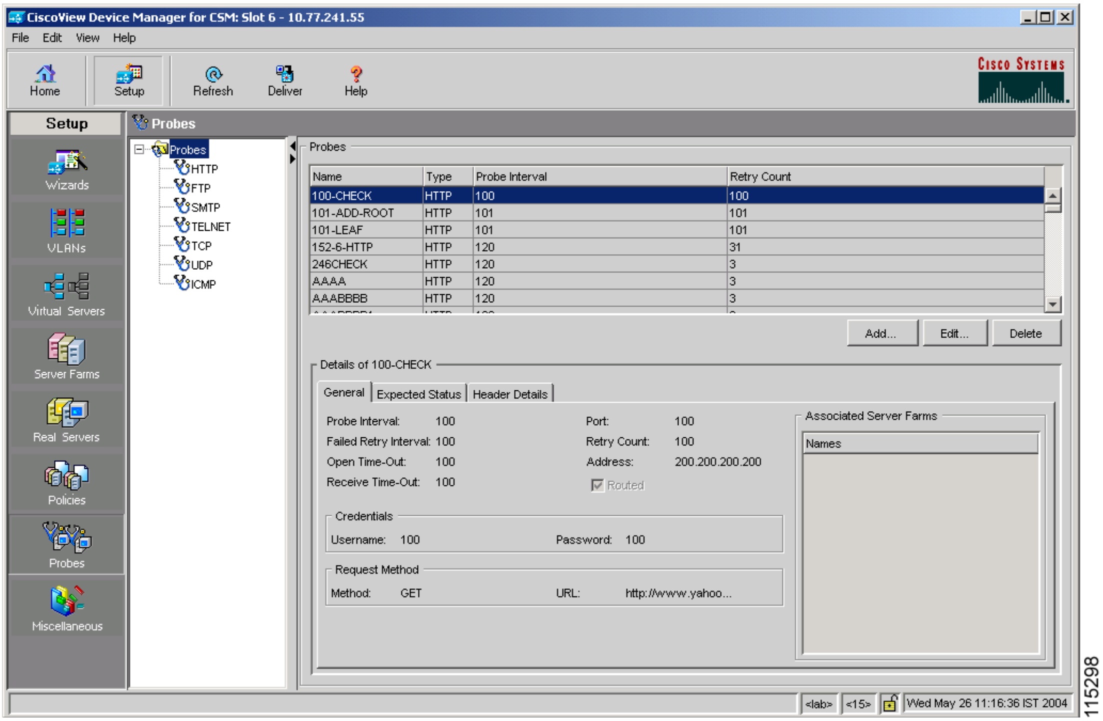
Associating probes to the real servers and server farms allows you to determine if the real servers are operating correctly.

CVDM-CSM supports probes to monitor real servers and lets you to configure them through CVDM-CSM.

This section includes the following topics:

- Viewing Probes, page 10-2
  - Viewing HTTP Probes, page 10-7
  - Viewing FTP Probes, page 10-17
  - Viewing SMTP Probes, page 10-26
  - Viewing TELNET Probes, page 10-34
  - Viewing TCP Probes, page 10-42
  - Viewing UDP Probes, page 10-47
  - Viewing ICMP Probes, page 10-52
- Adding Probes, page 10-4
- Editing Probes, page 10-6

Viewing Probes



Probes

Name	Type	Probe Interval	Retry Count
100-CHECK	HTTP	100	100
101-ADD-ROOT	HTTP	101	101
101-LEAF	HTTP	101	101
152-6-HTTP	HTTP	120	31
246CHECK	HTTP	120	3
AAAA	HTTP	120	3
AAABBBB	HTTP	120	3

Details of 100-CHECK

Probe Interval: 100
Failed Retry Interval: 100
Open Time-Out: 100
Receive Time-Out: 100

Port: 100
Retry Count: 100
Address: 200.200.200.200
☑ Routed

Credentials
Username: 100
Password: 100

Request Method
Method: GET
URL: http://www.yahoo...

Associated Server Farms

Names

You can view information about all probes on the device.

To view the probes:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Probes** in the left-most pane. A table with details of all configured Probes appears.

The following fields are displayed:

Field	Action/Action/Description
Probes	
Name	Name of the Probe. The character string is limited to 15 characters.
Type	Type of probe. The different types are http, ftp, smtp, telnet, telnet, tcp, udp and icmp.
Probe Interval	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe.
Retry Count	Number of probes to wait before marking a server as failed.
Details	The details of the selected Probe is displayed. For more information on HTTP, see "Viewing HTTP Probes" section on page 10-7. For more information on FTP, see "Viewing FTP Probes" section on page 10-17. For more information on SMTP, see "Viewing SMTP Probes" section on page 10-26. For more information on TELNET, see "Viewing TELNET Probes" section on page 10-34. For more information on TCP, see Viewing TCP Probes. For more information on UDP, see "Viewing UDP Probes" section on page 10-47. **Note** UDP probes cannot be viewed in the following IOS versions: 12.1(13)E, 12.2(14)SY and 12.2(14)SX1. For more information on ICMP, see "Viewing ICMP Probes" section on page 10-52.

From this page, you can access functions to do the following:

- Click **Add** to add probes. For more information, see "Adding Probes" section on page 10-4.
- Click **Edit** to add probes. For more information, see "Editing Probes" section on page 10-6.
- Select a Probe, then click **Delete** to delete the probe.

Adding Probes

To add Probes:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Probes** in the left-most pane. A table with details of all configured Probes appears.

Step 3 Click **Add**. The Add Probes dialog box appears.

In the **Type** field, choose the type of Probe which you wish to add.

They are: HTTP,FTP,SMTP,TELNET,TCP,UDP,andICMP.

The fields in the pane changes as per the type of the Probe.

For more information on adding a HTTP Probe, see "Adding HTTP Probes" section on page 10-11.

For more information on adding a FTP Probe, see "Adding FTP Probes" section on page 10-20.

For more information on adding a SMTP Probe, see "Adding SMTP Probes" section on page 10-29.

For more information on adding a TELNET Probe, See "Adding TELNET Probes" section on page 10-37

For more information on adding a TCP Probe, see "Adding TCP Probes" section on page 10-44.

For more information on adding a UDP Probe, see "Adding UDP Probes" section on page 10-49.

For more information on adding a ICMP Probe, see "Adding ICMP Probes" section on page 10-54.

Editing Probes

To edit Probes:

Step 1 Click **Setup** from the task bar.

Step 2 Click **Probes** in the left-most pane. A table with details of all configured Probes appears.

Step 3 Select the Probe that you wish to modify and click **Edit**. The Edit Probes dialog box appears.

Step 4 In the **Edit Probe** pane, the field **Type** shows the type of Probe.

They are: HTTP,FTP,SMTP,TELNET,TCP,UDP,andICMP.

The fields in the pane changes as per the type of the Probe.

For more information on editing a HTTP Probe, see "Editing HTTP Probes" section on page 10-14.

For more information on editing a FTP Probe, see "Editing FTP Probes" section on page 10-23.

For more information on editing a SMTP Probe, see "Editing SMTP Probes" section on page 10-31.

For more information on editing a TELNET Probe, see "Editing TELNET Probes" section on page 10-39

For more information on editing a TCP Probe, see "Editing TCP Probes" section on page 10-46.

For more information on editing a UDP Probe, see "Editing UDP Probes" section on page 10-51.

For more information on editing a ICMP Probe, see "Editing ICMP Probes" section on page 10-56.

Viewing HTTP Probes

To view HTTP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > HTTP** in the object selector.

The following fields appear:

Field	Action/Description
Name	Name of the probe.
Probe Interval	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe.
Retry Count	Number of probes to wait before marking a server as failed.

Details

More details about the selected probe appear at the bottom of the table. These are of three types:

- General
- Expected Status
- Header Details

General

The following details appears:

Field	Action/Description
Details	
Probe Interval	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe.
Port	Decimal TCP/UDP port number or port name.
Failed Retry Interval	Time in seconds before retrying a failed server.
Retry Count	Number of probes to wait before marking a server as failed.
Open Time- Out	Maximum time in seconds to wait for a TCP connection.
Address	IP address of the real server .
Receive Time-Out	Maximum time in seconds to wait for a reply from real server.
Routed	Displays the check box status, Selected or unselected. Specifies that the probe is routed according to the CSM routing table.
User Credentials	
Username	Name that appears in the HTTP header.

Field	Action/Description
Password	Password that appears in the HTTP header.
Associated Server Farms	Server Farm associated with the probe. All servers in the server farm receive probes of the probe types that are associated with that server farm. You can associate one or more probe types with a server farm.

Expected Status

The following details appears:

Field	Action/Description
Expected Status	
Minimum Value	Minimum status code in a range. There will be only a single status code if max-number is not specified.
Maximum Value	Maximum status code in a range.

Header Details

The following details appears:

Field	Action/Description
Header name and value	
Name	Name for the header being defined.
Value	Content for the header.

From this page, you can access functions to do the following:

- Click **Add** to add HTTP Probes. For more information, see "Adding HTTP Probes" section on page 10-11.
- Click **Edit** to edit an HTTP Probes. For more information, see "Editing HTTP Probes" section on page 10-14.
- Select a HTTP Probe, then click **Delete** to delete the Probe.

Adding HTTP Probes

To add HTTP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > HTTP** in the object selector.

Step 3 Click **Add**. The Add Probe dialog box appears.

The following details appears:

Field	Action/Description
Name	Enter the name of the probe. The character string is limited to 15 characters.
Type	The type HTTP is displayed.
Port l	Enter the decimal TCP/UDP port number or port name. The range is from 1 to 65535.
Retry Count	Enter the number of probes to wait before marking a server as failed. The range is from 0 to 65535. The defualt value is 3.
Probe Interval	Enter the number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe. The range is from 2 to 65535. The default value is 120.
Failed Retry Interval	Enter the time in seconds before retrying a failed server. The range is from 2 to 65535. The default value is 300.
Open Time- Out	Enter the maximum time in seconds to wait for a TCP connection. The range is from 1 to 65535 Secs. The default value is 10.
Receive Time-Out	Enter the maximum time in seconds to wait for a reply from real server The range is from 1 to 65535 Secs. The default value is 10.
Address	Enter the IP address of the real server. The check box for Routed adjacent to this field shows if the probe is routed according to the CSM routing table
User Credentials	
Username	Enter the name that appears in the HTTP header.
Password	Enter the password that appears in the HTTP header.
Expected Status	

Field	Action/Description
Minimum Value	Click **Add** and enter the minimum status code in a range. There will be only a single status code if max-number is not specified. The default range is 0 to 999. **Note** You cannot add overlapping status code. The range should be outside what you have already added.
Maximum Value	Enter the maximum status code in a range. The default range is 0 to 999. **Note** You cannot add overlapping status code. The range should be outside what you have already added.
Header name and value	
Name	Click **Add**, then enter the name for the header being defined.
Value	Enter the content for the header.

Editing HTTP Probes

To edit HTTP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > HTTP** in the object selector.

Step 3 Click **Edit**. The Edit Probe dialog box appears.

The following details appears:

Field	Action/Description
Name	The name of the probe.
Port	Modify the decimal TCP/UDP port number or port name. The range is from 0 to 65535.
Type	Type of probe. Here it will be HTTP.
Retry Count	Enter the number of probes to wait before marking a server as failed. The range is from 0 to 65535.
Probe Interval	Enter the number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe. The range is from 2 to 65535.
Failed Retry Interval	Enter the time in seconds before retrying a failed server. The range is from 2 to 65535.
Open Time- Out	Enter the maximum time in seconds to wait for a TCP connection. The range is from 1to 65535 Secs.
Receive Time-Out	Enter the maximum time in seconds to wait for a reply from real server. The range is from 1to 65535 Secs.
Address	Modify the IP address of the real server. The check box for Routed adjacent to this field shows if the probe is routed according to the CSM routing table
User Credentials	
Username	Modify the name that appears in the HTTP header.

Field	Action/Description
Password	Modify the password that appears in the HTTP header.
Expected Status	
Minimum Value	Click **Add**. Modify the minimum status code in a range. There will be only a single status code if max-number is not specified. The default range is 0 to 999. **Note** You cannot add overlapping status code. The range should be outside what you have already added.
Maximum Value	Modify the maximum status code in a range. The default range is 0 to 999. **Note** You cannot add overlapping status code. The range should be outside what you have already added.
Header name and value	
Name	Click **Add**. Modify the name for the header being defined.
Value	Modify the content for the header.

Viewing FTP Probes

To view FTP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > FTP** in the object selector.

The following fields appears:

Field	Action/Description
Name	Name of the probe.
Probe Interval	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe.
Retry Count	Number of probes to wait before marking a server as failed.

Details

More details about the selected probe appear at the bottom of the table. These are of two types:

- General
- Expect Status

General

The following details appears:

Field	Action/Description
Port	Decimal TCP/UDP port number or port name.
Retry Count	Number of probes to wait before marking a server as failed.
Probe Interval	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe.
Failed Retry Interval	Time in seconds before retrying a failed server.
Open Time-Out	Maximum time in seconds to wait for a TCP connection.
Receive Time-Out	Maximum time in seconds to wait for a reply from real server.
Associated Server Farm	The Server Farm associated with the probe. All servers in the server farm receive probes of the probe types that are associated with that server farm. You can associate one or more probe types with a server farm.

Expect Status

The following details appears:

Field	Action/Description
Minimum Value	Minimum status code in a range. There will be only a single status code if max-number is not specified.
Maximum Value	Maximum status code in a range.

From this page, you can access functions to do the following:

- Click **Add** to add FTP Probes. For more information, see "Adding FTP Probes" section on page 10-20
- Click **Edit** to edit a FTP Probes. For more information, see "Editing FTP Probes" section on page 10-23.
- Select a FTP Probe, then click **Delete** to delete the probe.

Adding FTP Probes

To add FTP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > FTP** in the object selector.

Step 3 Click **Add**. The Add Probe dialog box appears.

The following fields appears:

Field	Action/Description
Name	Enter the name of the probe. The character string is limited to 15 characters.
Type	Displays the type of probe. Here it will be FTP.
Probe Interval	Enter the number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe. The range is from 2 to 65535. The default value is 120.
Failed Retry Interval	Enter the time in seconds before retrying a failed server; the range is from 2 to 65535. The default value is 300.
Open Time- Out	Enter the maximum time in seconds to wait for a TCP connection. The range is from 1 to 65535 Secs. The default value is 10.
Receive Time-Out	Enter the maximum time in seconds to wait for a reply from real server. The range is from 1 to 65535 Secs. The default value is 10.
Port	Enter the decimal TCP/UDP port number or port name. The range is from 1 to 65535.
Retry Count	Enter the number of probes to wait before marking a server as failed. The range is from 0 to 65535. The default value is 3.
Expected Status	

Field	Action/Description
Minimum Value	Click **Add**. Enter the minimum status code in a range. There will be only a single status code if max-number is not specified. The default range is 0 to 999. **Note** You cannot add overlapping status code. The range should be outside what you have already added.
Maximum Value	Enter the maximum status code in a range. The default range is 0 to 999. **Note** You cannot add overlapping status code. The range should be outside what you have already added.

From this page, you can access functions to do the following:

- Click **Add** to add expect status details by adding the minimum and maximum expect status.
- Select a row and click **Delete** to delete the expect status.

Editing FTP Probes

To edit FTP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > FTP** in the object selector.

Step 3 Click **Edit**. The Edit Probe dialog box appears.

The following details appears:

Field	Action/Description
Name	The name of the probe.
Type	Type of probe. Here it will be FTP.
Probe Interval	Modify the number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe. The range is from 2 to 65535.
Failed Retry Interval	Modify the time in seconds before retrying a failed server; the range is from 2 to 65535.
Open Time- Out	Modify the maximum time in seconds to wait for a TCP connection. The range is from 1 to 65535 Secs.
Receive Time-Out	Modify the maximum time in seconds to wait for a reply from real server. The range is from 1 to 65535 Secs.
Port	Modify the decimal TCP/UDP port number or port name. The range is from 1 to 65535.
Retry Count	Modify the number of probes to wait before marking a server as failed. The range is from 0 to 65535.
Expected Status	

Field	Action/Description
Minimum Value	Click **Add**. Modify the minimum status code in a range. There will be only a single status code if max-number is not specified. The default range is 0 to 999. **Note** You cannot add overlapping status code. The range should be outside what you have already added.
Maximum Value	Modify the maximum status code in a range. The default range is 0 to 999. **Note** You cannot add overlapping status code. The range should be outside what you have already added.

Viewing SMTP Probes

To view SMTP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > SMTP** in the object selector.

The following details appears:

Field	Action/Description
Name	Name of the probe.
Probe Interval	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe.
Retry Count	Number of probes to wait before marking a server as failed.

Details

More details about the selected probe appear at the bottom of the table. These are of two types:

- General
- Expect Status

General

The following details appears:

Field	Action/Description
Probe Interval	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe.
Port	Decimal TCP/UDP port number or port name.
Failed Retry Interval	Time in seconds before retrying a failed server.
Retry Count	Number of probes to wait before marking a server as failed.
Open Time- Out	Maximum time in seconds to wait for a TCP connection.
Receive Time-Out	Maximum time in seconds to wait for a reply from real server.
Associated Server Farm	The Server Farm associated with the probe. All servers in the server farm receive probes of the probe types that are associated with that server farm. You can associate one or more probe types with a server farm.

Expect Status

The following details appears.

Field	Action/Description
Minimum Value	Minimum status code in a range. There will be only a single status code if max-number is not specified.
Maximum Value	Maximum status code in a range.

From this page, you can access functions to do the following:

- Click **Add** to add SMTP Probes. For more information, see "Adding SMTP Probes" section on page 10-29.
- Click **Edit** to edit a SMTP Probe. For more information, see "Editing SMTP Probes" section on page 10-31.
- Select a SMTP Probe, then click **Delete** to delete the Probe.

Adding SMTP Probes

To add SMTP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > SMTP** in the object selector.

Step 3 Click **Add**. The Add Probe dialog box appears.

The following details appears.

Field	Action/Description
Name	Enter the name of the probe. The character string is limited to 15 characters.
Type	Displays the type of probe. Here it will be SMTP.
Probe Interval	Enter the number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe. The range is from 2 to 65535. The default value is 120.
Failed Retry Interval	Enter the time in seconds before retrying a failed server; the range is from 2 to 65535. The default value is 300.
Open Time- Out	Enter the maximum time in seconds to wait for a TCP connection. The range is from 1 to 65535 Secs. The default value is 10.
Receive Time-Out	Enter the maximum time in seconds to wait for a reply from real server. The range is from 1 to 65535 Secs. The default value is 10.

Field	Action/Description
Port	Enter the decimal TCP/UDP port number or port name. The range is from 1 to 65535.
Retry Count	Enter the number of probes to wait before marking a server as failed. The range is from 0 to 65535. The default value is 3.
Expected Status	
Minimum Value	Click **Add**. Enter the minimum status code in a range. There will be only a single status code if max-number is not specified. The default range is 0 to 999. **Note** You cannot add overlapping status code. The range should be outside what you have already added.
Maximum Value	Enter the maximum status code in a range. The default range is 0 to 999. **Note** You cannot add overlapping status code. The range should be outside what you have already added.

From this page, you can access functions to do the following:

- Click **Add** to add expect status details by adding the minimum and maximum expect status.

- Select a row and click **Delete** to delete the expect status.

Editing SMTP Probes

To edit SMTP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > SMTP** in the object selector.

Step 3 Click **Edit**. The Edit Probe dialog box appears.

The following details appears:

Field	Action/Description
Name	Name of the probe.
Type	Type of probe. Here it will be SMTP.
Probe Interval	Modify the number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe. The range is from 2 to 65535.
Failed Retry Interval	Modify the time in seconds before retrying a failed server; the range is from 2 to 65535.
Open Time- Out	Modify the maximum time in seconds to wait for a TCP connection. The range is from 1 to 65535 Secs.
Receive Time-Out	Modify the maximum time in seconds to wait for a reply from real server. The range is from 1 to 65535 Secs.
Port	Modify the decimal TCP/UDP port number or port name. The range is from 1 to 65535.
Retry Count	Modify the number of probes to wait before marking a server as failed. The range is from 0 to 65535.
Expected Status	

Field	Action/Description
Minimum Value	Click **Add**. Modify the minimum status code in a range. There will be only a single status code if max-number is not specified. The default range is 0 to 999. **Note** You cannot add overlapping status code. The range should be outside what you have already added.
Maximum Value	Modify the maximum status code in a range. The default range is 0 to 999. **Note** You cannot add overlapping status code. The range should be outside what you have already added.

Viewing TELNET Probes

To view TELNET Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > TELNET** in the object selector.

The following details appears:

Field	Action/Description
Name	Name of the probe.
Interval	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe.
Retry Count	Number of probes to wait before marking a server as failed.

Details

More details about the selected probe appear at the bottom of the table. These are of two types:

- General
- Expect Status

General

The following details appears:

Field	Action/Description
Probe Interval	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe.
Port	Decimal TCP/UDP port number or port name.
Failed Retry Interval	Time in seconds before retrying a failed server.
Retry Count	Number of probes to wait before marking a server as failed.
Open Time- Out	Maximum time in seconds to wait for a TCP connection.
Receive Time-Out	Maximum time in seconds to wait for a reply from real server.
Associated Server Farm	The Server Farm associated with the probe. All servers in the server farm receive probes of the probe types that are associated with that server farm. You can associate one or more probe types with a server farm.

Expect Status

The following details appears:

Field	Action/Description
Minimum Value	Minimum status code in a range. There will be only a single status code if max-number is not specified.
Maximum Value	Maximum status code in a range.

From this page, you can access functions to do the following:

- Click **Add** to add TELNET probes. For more information, see "Adding TELNET Probes" section on page 10-37.
- Click **Edit** to edit a TELNET probe. For more information, see "Editing TELNET Probes" section on page 10-39.
- Select a TELNET probe, then click **Delete** to delete the Probe.

Adding TELNET Probes

To add TELNET Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > TELNET** in the object selector.

Step 3 Click **Add**. The Add Probe dialog box appears.

The following details appears:

Field	Action/Description
Name	Enter the name of the probe. The character string is limited to 15 characters.
Type	Displays the type of probe. Here it will be TELNET.
Probe Interval	Enter the number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe. The range is from 2 to 65535. The default value is 120.
Failed Retry Interval	Enter the time in seconds before retrying a failed server; the range is from 2 to 65535. The default value is 300.
Open Time- Out	Enter the maximum time in seconds to wait for a TCP connection. The range is from 1-65535 Secs. The default value is 10.
Receive Time-Out	Enter the maximum time in seconds to wait for a reply from real server. The range is from 1-65535 Secs. The default value is 10.

Field	Action/Description
Port	Enter the decimal TCP/UDP port number or port name.
Retry Count	Enter the number of probes to wait before marking a server as failed. The range is from 0 to 65535. The default value is 3.
Expected Status	
Minimum Value	Click **Add**. Enter the minimum status code in a range. There will be only a single status code if max-number is not specified. The default range is 0 to 999. **Note** You cannot add overlapping status code. The range should be outside what you have already added.
Maximum Value	Enter the maximum status code in a range. The default range is 0 to 999. **Note** You cannot add overlapping status code. The range should be outside what you have already added.

From this page, you can access functions to do the following:

- Click **Add** to add expect status details by adding the minimum and maximum expect status.
- Select a row and click **Delete** to delete the expect status.

Editing TELNET Probes

To edit TELNET Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > TELNET** in the object selector.

Step 3 Click **Edit**. The Edit Probe dialog box appears.

The following details appears:

Field	Action/Description
Name	Name of the probe.
Type	Type of probe. Here it will be TELNET.
Probe Interval	Modify the number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe. The range is from 2 to 65535.
Failed Retry Interval	Modify the time in seconds before retrying a failed server; the range is from 2 to 65535.
Open Time- Out	Modify the maximum time in seconds to wait for a TCP connection. The range is from 1 to 65535 Secs.
Receive Time-Out	Modify the maximum time in seconds to wait for a reply from real server. The range is from 1 to 65535 Secs.
Port	Modify the decimal TCP/UDP port number or port name. The range is from 1 to 65535.
Retry Count	Modify the number of probes to wait before marking a server as failed. The range is from 0 to 65535.
Expected Status	

Field	Action/Description
Minimum Value	Click **Add**. Modify the minimum status code in a range. There will be only a single status code if max-number is not specified. The default range is 0 to 999. **Note** You cannot add overlapping status code. The range should be outside what you have already added.
Maximum Value	Modify the maximum status code in a range. The default range is 0 to 999. **Note** You cannot add overlapping status code. The range should be outside what you have already added.

Viewing TCP Probes

To view TCP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > TCP** in the object selector.

The following details appears:

Field	Action/Description
Name	Name of the probe.
Interval	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe.
Retry Count	Number of probes to wait before marking a server as failed.

Details

More details about the selected probe appear at the bottom of the table.

The following details appears:

Field	Action/Description
Probe Interval	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe.
Port	Decimal TCP/UDP port number or port name.
Failed Retry Interval	Time in seconds before retrying a failed server.
Retry Count	Number of probes to wait before marking a server as failed.
Open Time- Out	Maximum time in seconds to wait for a TCP connection.
Receive Time-Out	Maximum time in seconds to wait for a reply from real server.
Associated Server Farm	The Server Farm associated with the probe. All servers in the server farm receive probes of the probe types that are associated with that server farm. You can associate one or more probe types with a server farm.

From this page, you can access functions to do the following:

- Click **Add** to add TCP probes. For more information, see "Adding TCP Probes" section on page 10-44.
- Click **Edit** to edit a TCP probe. For more information, see "Editing TCP Probes" section on page 10-46.
- Select a TCP probe, then click **Delete** to delete the probe.

Adding TCP Probes

To add TCP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > TCP** in the object selector.

Step 3 Click **Add**. The Add Probe dialog box appears.

The following details appears:

Field	Action/Description
Name	Enter the name of the probe. The character string is limited to 15 characters.
Type	Type of probe. Here it will be TCP.
Probe Interval	Enter the number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe. The range is from 2 to 65535. The default value is 120.
Failed Retry Interval	Enter the time in seconds before retrying a failed server; the range is from 2 to 65535. The default value is 300.
Open Time- Out	Enter the maximum time in seconds to wait for a TCP connection. The range is from 1-65535 Secs. The default value is 10.
Port	Enter the decimal TCP/UDP port number or port name. The range is from 1 to 65535.

Editing TCP Probes

To edit TCP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > FTP** in the object selector.

Step 3 Click **Edit**. The Edit Probe dialog box appears.

The following details appears:

Field	Action/Description
Name	Name of the probe.
Type	Type of probe. Here it will be TCP.
Probe Interval	Modify the number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe. The range is from 2 to 65535.
Failed Retry Interval	Modify the time in seconds before retrying a failed server; the range is from 2 to 65535.
Open Time- Out	Modify the maximum time in seconds to wait for a TCP connection. The range is from 1 to 65535 Secs.
Port	Modify the decimal TCP/UDP port number or port name. The range is from 1 to 65535.

Viewing UDP Probes

Note UDP probes cannot be viewed in the following IOS versions: 12.1(13)E, 12.2(14)SY and 12.2(14)SX1.

To view UDP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > UDP** in the object selector.

The following details appears:

Field	Action/Description
Name	Name of the probe.
Interval	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe.
Retry Count	Number of probes to wait before marking a server as failed.

Details

More details about the selected probe appear at the bottom of the table.

The following details appears:

Field	Action/Description
Probe Interval	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe.
Port	Decimal TCP/UDP port number or port name.
Failed Retry Interval	Time in seconds before retrying a failed server.
Retry Count	Number of probes to wait before marking a server as failed.
Receive Time-Out	Maximum time in seconds to wait for a reply from real server.
Associated Server Farm	The Server Farm associated with the probe. All servers in the server farm receive probes of the probe types that are associated with that server farm. You can associate one or more probe types with a server farm.

From this page, you can access functions to do the following:

- Click **Add** to add UDP Probes. For more information, see "Adding UDP Probes" section on page 10-49.
- Click **Edit** to edit a UDP Probe. For more information, see "Editing UDP Probes" section on page 10-51.
- Select a UDP probe, then click **Delete** to delete the Probe.

Adding UDP Probes

To add UDP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > UDP** in the object selector.

Step 3 Click **Add**. The Add Probe dialog box appears.

The following details appears:

Field	Action/Description
Name	Enter the name of the probe. The character string is limited to 15 characters.
Type	Type of probe. Here it will be UDP.
Probe Interval	Enter the number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe. The range is from 2 to 65535. The default value is 120.
Failed Retry Interval	Enter the time in seconds before retrying a failed server; the range is from 2 to 65535. The default value is 300.
Receive Time-Out	Enter the maximum time in seconds to wait for a reply from real server. The range is from 1 to 65535 Secs. The default value is 10.
Port	Enter the decimal TCP/UDP port number or port name. The range is from 1 to 65535.

Editing UDP Probes

To edit UDP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > UDP** in the object selector.

Step 3 Click **Edit**. The Edit Probe dialog box appears.

The following details appears:

Field	Action/Description
Name	Name of the probe.
Type	Type of probe. Here it will be UDP.
Probe Interval	Modify the number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe. The range is from 2 to 65535.
Failed Retry Interval	Modify the time in seconds before retrying a failed server; the range is from 2 to 65535.
Receive Time-Out	Modify the maximum time in seconds to wait for a reply from real server. The range is from 1-65535 Secs.
Port	Modify the decimal TCP/UDP port number or port name. The range is from 1 to 65535.

Viewing ICMP Probes

To view ICMP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > ICMP** in the object selector.

The following details appears:

Field	Action/Description
Name	Name of the probe.
Probe Interval	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe.
Retry Count	Number of probes to wait before marking a server as failed.

Details

More details about the selected probe appear at the bottom of the table

The following details appears:

Field	Action/Description
Probe Interval	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe.
Retry Count	Number of probes to wait before marking a server as failed.
Failed Retry Interval	Time in seconds before retrying a failed server.
Address	The IP address of the probes.
Receive Time-Out	Maximum time in seconds to wait for a reply from real server.
Routed	Displays the check box status, Selected or unselected. Specifies that the probe is routed according to the CSM routing table.
Associated Server Farm	The Server Farm associated with the probe. All servers in the server farm receive probes of the probe types that are associated with that server farm. You can associate one or more probe types with a server farm.

From this page, you can access functions to do the following:

- Click **Add** to add ICMP probes. For more information, see "Adding ICMP Probes" section on page 10-54.
- Click **Edit** to edit an ICMP probe. For more information, see "Editing ICMP Probes" section on page 10-56.

- Select a ICMP probe, then click **Delete** to delete the probe.

Adding ICMP Probes

To add ICMP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > ICMP** in the object selector.

Step 3 Click **Add**. The Add Probe dialog box appears.

The following details appears:

Field	Action/Description
Name	Enter the name of the probe. The character string is limited to 15 characters.
Type	Type of probe. Here it will be ICMP.
Probe Interval	Enter the number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe. The range is from 2 to 65535. The default value is 120.
Failed Retry Interval	Enter the time in seconds before retrying a failed server; the range is from 2 to 65535. The default value is 300.
Receive Time-Out	Enter the maximum time in seconds to wait for a reply from real server The range is from 1 to 65535 Secs. The default value is 10.
Retry Count	Enter the number of probes to wait before marking a server as failed. The range is from 0 to 65535. The defualt value is 3.
Address	Enter the IP address of the real server .
Routed	Select the check box to specify that the probe should be routed according to the CSM routing table.

Editing ICMP Probes

To edit ICMP Probes:

Step 1 Click **Setup** from the task bar. Click Probes in the left-most pane.

Step 2 Select **Probes > FTP** in the object selector.

Step 3 Click **Edit**. The Edit Probe dialog box appears.

The following details appears:

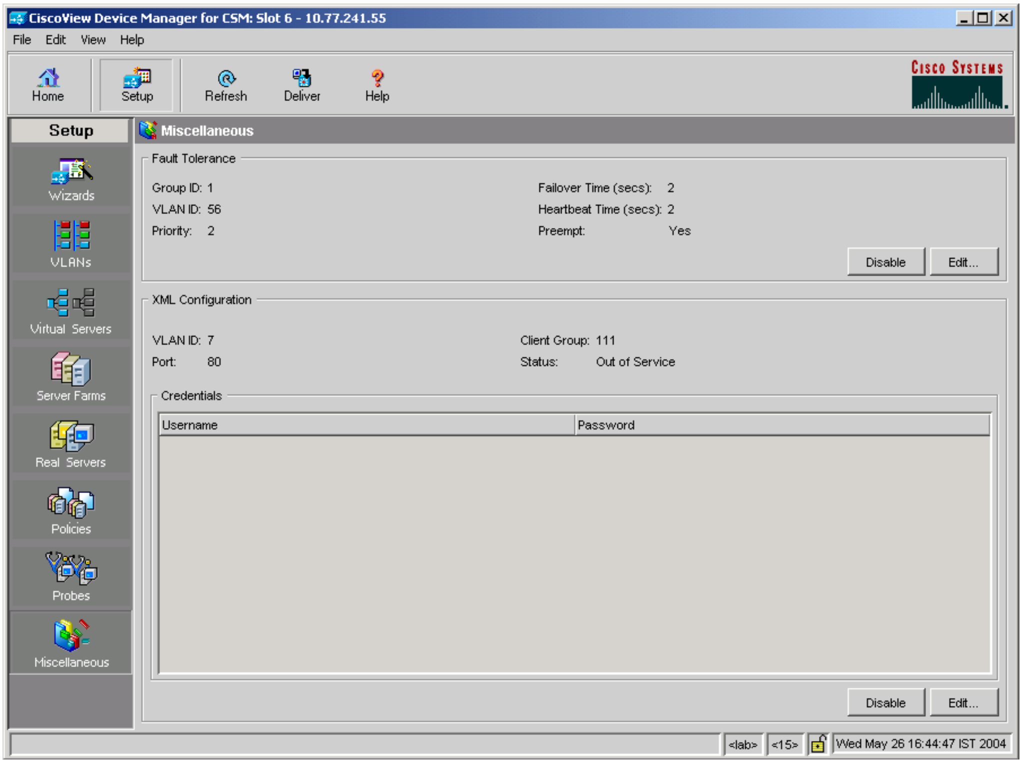
Field	Action/Description
Name	Name of the probe.
Type	Type of probe. Here it will be icmp.
Probe Interval	Modify the number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe. The range is from 2 to 65535.
Failed Retry Interval	Modify the time in seconds before retrying a failed server; the range is from 2 to 65535.
Receive Time-Out	Modify the maximum time in seconds to wait for a reply from real server. The range is from 1 to 65535 Secs.
Retry Count	Enter the number of probes to wait before marking a server as failed. The range is from 0 to 65535.
Address	Modify the IP address of the real server.
Routed	Displays the check box status, Selected or unselected. Specifies that the probe is routed according to the CSM routing table.

Managing Fault Tolerance and XML Configuration

The Miscellaneous section in the CSM describes the following:

- Understanding Fault Tolerance, page 11-3
- Understanding XML Configuration, page 11-7

Figure 11-1   Miscellaneous Page



Miscellaneous

Fault Tolerance

Group ID: 1
VLAN ID: 56
Priority: 2

Failover Time (secs): 2
Heartbeat Time (secs): 2
Preempt: Yes

XML Configuration

VLAN ID: 7
Port: 80

Client Group: 111
Status: Out of Service

Credentials

Username	Password

115294

Understanding Fault Tolerance

In the secure (router) mode, the client-side and server-side VLANs provide the fault-tolerant (redundant) connection paths between the CSM and the routers on the client side and the servers on the server side. In a redundant configuration, two CSMs perform active and standby roles. Each CSM contains the same IP, virtual server, server pool, and real server information. From the client-side and server-side networks, each CSM is configured identically. The network sees the fault-tolerant configuration as a single CSM.

Two CSMs can be configured in a fault-tolerant mode to share state information about user sessions and provide connection redundancy. When the active CSM fails, open connections are handled by the standby CSM without interruption, and users experience hitless failover.

Fault-tolerant configuration can be done with two CSMs in two Cisco Catalyst 6500 Series devices or in a single chassis. Configuration can also be done in either the secure (router) mode or nonsecure (bridge) mode.

Configuring fault tolerance requires the following:

- Two CSMs that are installed in the same or different Catalyst 6500 series chassis.
- Identically configured CSMs. One CSM is configured as active; the other is configured as standby.
- Each CSM connected to the same client-side and server-side VLANs.
- Communication between the CSMs provided by a shared private VLAN.
- A network that sees the redundant CSMs as a single entity.

Related Topics:

- Configuring Fault Tolerance, page 11-4
- Editing Fault Tolerance Configuration, page 11-6

Configuring Fault Tolerance

Note Click the **Enable** button to enable the Fault Tolerance Configuration in the CSM module. When it is enabled this button turns to **Disable** and the **Edit** button is now enabled to allow modifications to the Fault tolerance configuration values. To disable the Fault Tolerance Configuration click the **Disable** button.

To configure Fault Tolerance:

Step 1 Click **Setup** from the task bar, then click **Miscellaneous** in the left-most pane.

The Fault tolerance details are displayed at the top.

The following fields appear:

Field	Description
Group ID	ID of the fault-tolerant group. Both CSMs must have the same group ID.
VLAN ID	ID of the VLAN over which heartbeat messages are sent. Both CSMs must have the same VLAN ID.
Failover Time	Amount of time for a standby CSM to wait before becoming active. The default failover time is 3 seconds.
Heartbeat Time	Time interval between heartbeat transmissions (in seconds).
Priority	Priority of a CSM.
Preempt	Choose Preempt to allow a higher priority CSM to take control of a fault-tolerant group when it comes online.

From here, you can do the following functions:

- Click **Edit** to edit the fault tolerance configuration. For more information, see "Editing Fault Tolerance Configuration" section on page 11-6.
- Click **Disable** to disable the Fault Tolerance Configuration in the CSM Module.

Editing Fault Tolerance Configuration

To edit Fault Tolerance configuration:

Step 1 Click **Setup** from the task bar, then click **Miscellaneous** in the left-most pane.

Step 2 Click **Edit** under the fault tolerance section.

The following fields appear:

Field	Description
Group ID	Enter the ID of the fault-tolerant group. Both CSMs must have the same group ID. The range is from 1 to 254.
VLAN ID	Enter the ID of the VLAN over which heartbeat messages are sent. Both CSMs must have the same VLAN ID. The range is from 2 to 4095.
Failover Time	Enter the failover time. The range is from 1 to 65535 seconds. The default failover time is 3 seconds.
Heartbeat Time	Enter the heartbeat time. The range is from 1 to 65535 seconds.
Priority	Enter the priority of the CSM. The range is from 1 to 254.
Preempt	Specify Yes or No to allow a higher priority CSM to take control of a fault-tolerant group when it comes online.

Understanding XML Configuration

Earlier, the only method was available for configuration of the CSM was the IOS command line interface. With XML, you can configure the CVDM-CSM using a Document Type Definition or DTD.

Related Topics:

- Viewing XML Configuration, page 11-8
- Editing XML Configuration, page 11-9

Viewing XML Configuration

Note Click the **Enable** button to enable the XML Configuration in the CSM module. When it is enabled this button turns to **Disable** and the **Edit** button is now enabled to allow modifications to the XML configuration values.To disable the XML Configuration click the **Disable** button.

To view XML configuration:

Step 1 Click **Setup** from the task bar, then click **Miscellaneous** in the left-most pane.

XML configuration details are displayed in the botton half of the page.

The following fields appear:

Field	Description
VLAN ID	ID of the VLAN.
Client Group	Client-group can be either standard access-list name or ID (from 1 to 99).
Port	The port number.
Status	Status of XMLservice.
Credentials	
User Name	Name of the credentials user.
Password	Password of the credentials user.

From the main XML Configuration page, you can access functions to do the following:

- Click **Edit** to edit the XML Configuration. For more information, see "Editing XML Configuration" section on page 11-9.
- Click **Disable** to disable the XML Configuration in the CSM Module.

Editing XML Configuration

To edit XML configuration:

Step 1 Click **Setup** from the task bar, click**Miscellaneous** in the left-most pane.

XML configuration details are displayed in the botton half of the page.

Step 2 Click **Edit**. The Edit XML Configuration dialog appears.

The following fields appear:

Field	Description
VLAN ID	Enter the ID of the VLAN.
Client Group	Enter the name or ID of the client group. If ID, the range is from 1 to 99.
Port	Enter the decimal TCP/UDP port number. The range is from 0 to 65535.
Status	Specify, from the list, the status of XML Service. You can choose between In Service or Out of Service.
Credentials	
User Name	Name of the credentials user.
Password	Password of the credentials user.

From this page, you can access functions to do the following:

- Click **Add** to add the credentials by entering the username and the password.
- Select a row and click **Delete** to delete the corresponding credential.

INDEX