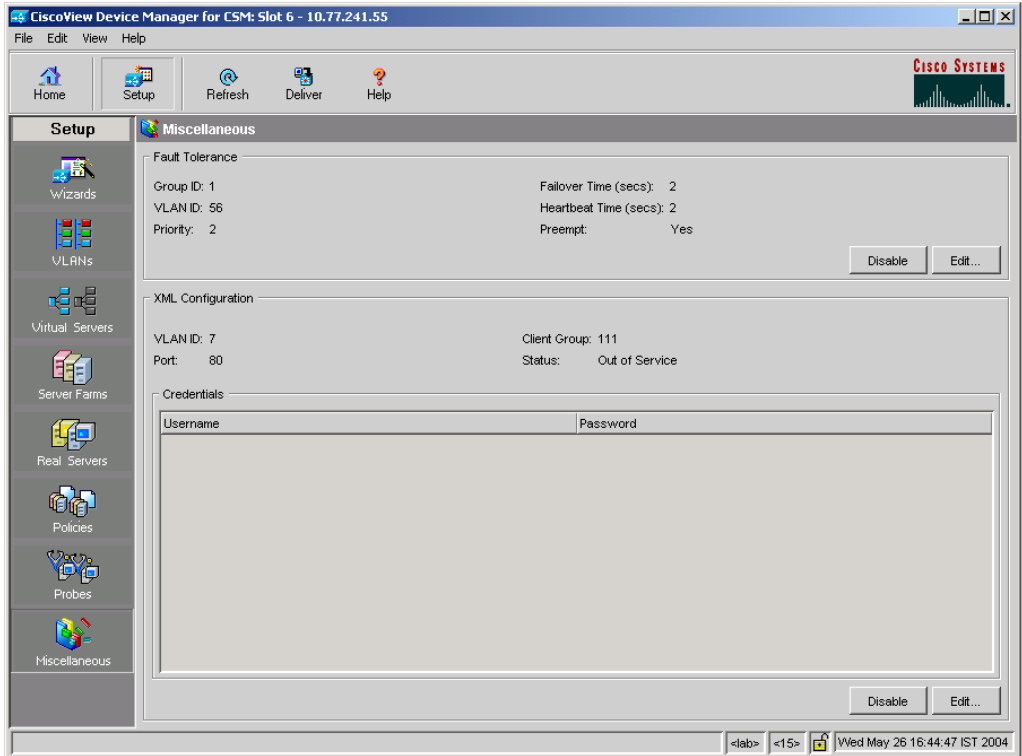# Managing Fault Tolerance and XML Configuration

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

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

✎

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

✎

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 switching 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 bottom 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.