Avaya P580/P882 Manager User Guide

August 2003

Avaya P580/P882 Manager User Guide

Release 2.002

Table of Contents

Preface

Welcome to Avaya P580/P882 Manager. This chapter provides an introduction to the structure and assumptions of this guide. It includes the following sections:

- **The Purpose of this Guide** - A description of the goals of this guide.
- **Who Should Use this Guide** - The intended audience of this guide.
- **Organization of this Guide** - A brief description of the subjects contained in the various sections of this guide.

The Purpose of this Guide

The Avaya P580/P882 Manager guide contains information needed to use the management system efficiently and effectively.

Who Should Use this Guide

This guide is intended for network managers familiar with network management and its fundamental concepts.

Organization of this Guide

This guide is structured to reflect the following conceptual divisions:

- **Avaya P580/P882 Manager** - Information pertaining to the entire Avaya P580/P882 Manager application and all of its aspects.
  - **Preface** - This section describes the guide's purpose, intended audience and organization.
  - **Introduction** - An introduction to the Avaya P580/P882 Manager, including instructions on starting the Avaya P580/P882 Manager.

- **Avaya P580/P882 Device Manager** - Information pertaining to Avaya P580/P882 Device management.
  - **Device Manager** - An introduction to the Avaya P580/P882 Device Manager, including a description of the user interface.
  - **Device Configuration** - Viewing and modifying the various device configurations.
  - **Port RMON** - Viewing graphical representations of the traffic on the ports/LAGs of the Avaya P580/P882 Device.
  - **Link Aggregation Groups** - Viewing and editing LAG information.
  - **VLANs** - Viewing and editing VLAN information.
  - **Port Mirroring** - Setting up port mirroring for ports and LAGs in an Avaya P580/P882 Device.
  - **Trap Managers Configuration** - Viewing and modifying the Trap Managers table.
  - **Port Security** - Viewing and configuring port security.
  - **Switch Connected Addresses** - Viewing devices connected to selected ports.
- **Avaya P580/P882 Routing Manager** - Information pertaining to Avaya P580/P882 routing management.
  - **Routing Manager** - An introduction to configuring routing with Avaya P580/P882R modules, and a description of the Avaya P580/P882R Routing Manager user interface.
  - **IP Routing** - Detailed descriptions of IP route configuration that enable you to display and update IP interfaces, the IP routing table, the ARP table, DHCP/BOOTP parameters, RIP interfaces, OSPF interfaces, area parameters, link-state database and neighbors, the IP access control table, DVMRP parameters, IGMP configuration, and redundancy parameters.
  - **IPX Routing** - Detailed descriptions of IPX route configuration that enable you to display and update IPX, IPX RIP, and IPX SAP interfaces.
  - **AppleTalk Routing** - Detailed descriptions of AppleTalk route configuration that enable you to display and update AppleTalk interfaces, static routes, NBP filters, and zone filters.

  - **L3 Forwarding Cache** - Detailed descriptions of the Layer-3 forwarding cache that enable you to configure the Layer-3 forwarding cache, display forwarding statistics, search for cache entries, and display cache statistics.

- **Appendices** - Additional information about the Avaya P580/P882 Manager.

  - **Menus** - The full structure of the menus in the Avaya P580/P882 Manager.

1 Introduction

This chapter provides an introduction to the Avaya P580/P882 Manager. It includes the following sections:

- **Avaya P580/P882 Manager Overview** - An overview explaining the different aspects of Avaya P580/P882 Device management.
- **Starting the Avaya P580/P882 Manager** - Instructions on how to access Avaya P580/P882 Manager from your management platform.
- **The User Interface** - Detailed descriptions of the user interface common to all applications in the Avaya P580/P882 Manager.

Avaya P580/P882 Manager Overview

The Avaya P580/P882 Manager provides full management capabilities for Avaya P580/P882 Devices. This includes the ability to view three aspects of device management:

- **Device Manager** - Provides a view of the configuration of the device including VLAN configuration, configured LAGs, and traps. For information specific to the Avaya P580/P882 Device Manager, refer to Chapter 2 - Chapter 13.
- **Routing Manager** - Provides a view of the third layer routing and forwarding functions of the device. For information specific to the Avaya P580/P882 Routing Manager, refer to Chapter 16 - Chapter 20.
- **Device SMON** - Provides advanced monitoring capabilities for the device. For information specific to Avaya P580/P882 Device SMON, refer to *Avaya P580/P882 Device SMON User Guide*.

For information on switching between the different views, refer to “Application Tabs” on page 6.

Starting the Avaya P580/P882 Manager

This section provides instructions for starting the Avaya P580/P882 Manager.

Running Avaya P580/P882 Manager from Avaya Network Management Console

In the Network Tree or Table:

1. Double-click the label representing the Avaya P580/P882 Device you want to manage.

Or

1. Select the label representing the Avaya P580/P882 Device you want to manage.
2. Click  or select **Tools > Device Manager**.

Running Avaya P580/P882 Manager from HP-OV NNM

From the management platform map:

1. Select the Avaya P580/P882 Device you want to manage.
2. Click  in the OpenView toolbar.

   Or

   Select **Tools > Avaya > Device Manager.**

Or

1. Right-click on the Avaya P580/P882 Device you want to manage.
2. Select **Avaya > Device Manager**.

The User Interface

The Avaya P580/P882 Manager user interface is different for each of its management applications. However, the following elements of the user interface are common to all views:

- **Application Tabs** - Tabs for accessing the Device Manager, Routing Manager, and SMON for the Avaya P580/P882 Device.
- **Application Area** - An area where the selected application opens.
- **Status Line** - Displays the communication status between the Avaya P580/P882 Manager and the Avaya P580/P882 Device.
- **Admission Level** - Displays the permission level with which you have accessed the Avaya P580/P882 Device.

Figure 1-1. Avaya P580/P882 Manager User Interface

Application Tabs

You can access the three main components of device management using the following Application Tabs in the Avaya P580/P882 Manager:

- **Device Manager** - View the Avaya P580/P882 Device Manager for device configuration and Port RMON.
- **Routing Manager** - View the Avaya P580/P882 Routing configuration.
- **Device SMON** - View SMON (Switch Monitoring) information for the Avaya P580/P882 Device.

To switch to a different view, click on the appropriate Application Tab. The selected application opens.

Status Line

The Status Line shows the communication status between the application and the Avaya P580/P882 Device. The Status Line displays a status message and an appropriate graphic. The table below shows the possible statuses with their corresponding graphics, and provides an explanation for each status.

Table 1-1. Communication Statuses

Status	Graphic	Description
Ready		The application is ready to communicate with the Avaya P580/P882 Device.
Communicating		The application is currently communicating with the Avaya P580/P882 Device.
Communication Error		The last attempted communication with the Avaya P580/P882 Device was not successful.

In addition, the Status Line displays your admission level. For more information about admission levels, refer to "Admission Level" on page 4.

Admission Level

You can define a user's admission level in Avaya P580/P882 Device Manager. A user can access the device as **User** or **Administrator**. An **Administrator** has permission to reset the device and is able to manage traps.

The Admission Level is based on the community name used to log into the device. For information on configuring admission level communities, refer to the Avaya P580/P882 CLI guide. For information on configuring your network management application (Avaya Network Management in Standalone Mode or HP-OV NNM) with the community names, refer to the network management application's documentation.

HTTP Login Security and SNMP version

Depending on the level of security you desire, you can define a user's configuration to use SNMPv1 or SNMPv3 for login to Device Manager, and HTTP or HTTPS for login to Routing Manager.

- A user who logs in to Device Manager using SNMPv1 may use HTTP for login to Routing Manager.
- A user who logs in to Device Manager using SNMPv3 must use HTTPS for login to Routing Manager.

*** Note:** If you define a user ID to log in using SNMPv3 for Device Manager, that user ID will automatically be assigned to use HTTPS for Routing Manager. You will not have to define a new HTTPS ID for that user.

For instructions on configuring HTTP/HTTPS access and SNMP version, refer to the *Avaya P580/P882Administrator's Guide*.

2 Device Manager

This chapter provides an introduction to the Avaya P580/P882 Device Manager. It includes the following sections:

- **The User Interface** - An introduction to the Avaya P580/P882 Device Manager user interface, including instructions on selecting elements and using the toolbar buttons.
- **Avaya P580/P882 Modes** - Instructions about switching between the configuration and Port RMON modes in the Avaya P580/P882 Device Manager.
- **Managing Tables** - An explanation of the symbols used to label table rows.
- **Using Dialog Boxes and Tables** - An explanation of the icons found in the dialog boxes and tables in the Avaya P580/P882 Device Manager.
- **Using Avaya P580/P882 Device Manager Help** - An explanation of the options for accessing on-line help in the Avaya P580/P882 Device Manager.

The User Interface

The Avaya P580/P882 Device Manager user interface consists of the following elements:

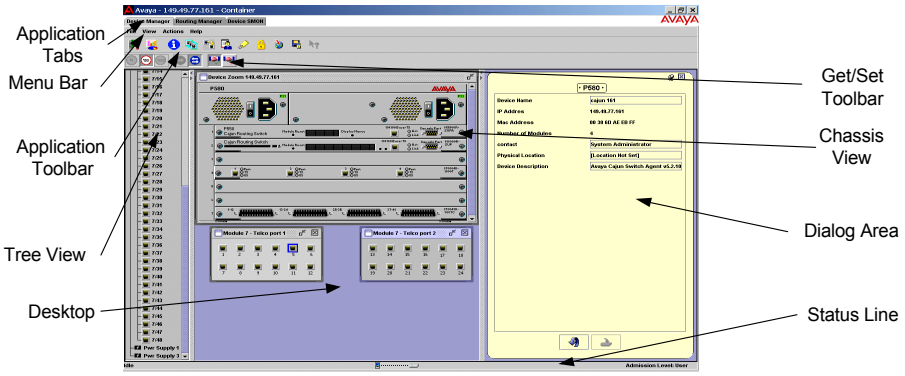
- **Menu Bar** - Menus for accessing Avaya P580/P882 Device management functions. For more information, refer to Appendix A, *Menus*
- **Application Toolbar** - Toolbar buttons for accessing Avaya P580/P882 Device management functions.
- **Get/Set Toolbar** - Toolbar buttons for viewing and changing the configuration of ports and LAGs.
- **Tree View** - A resizeable window containing a hierarchical representation of the modules, ports, LAGs, and power supplies of the Avaya P580/P882 Device.

- **Desktop** - A resizeable window where the Chassis View and all floating and minimized dialog boxes and tables are displayed.
- **Chassis View** - A graphical representation of the Avaya P580/P882 Device.
- **Dialog Area** - A resizeable window where all dialog boxes and tables first open.

For information on other parts of the user interface, refer to "The User Interface" on page 3.

The figure below shows the user interface, with its various parts labeled.

Figure 2-1. The Avaya P580/P882 Device Manager User Interface



To resize the three main areas of the user interface, the Tree View, the Chassis View, and the Dialog Area, use the splitter bars and their arrows.

Application Toolbar

The Application Toolbar provides shortcuts to the main Device Manager functions. The table below describes the buttons on the Application Toolbar and gives the equivalent menu options.

Table 2-1. Application Toolbar

Button	Description	Menu Item
	Sets the device manager to Configuration Mode.	**View > Configuration**
	Sets the device manager to Port RMON mode.	**View > Port RMON**

Table 2-1. Application Toolbar (Continued)

Button	Description	Menu Item
	Displays the device information dialog box.	**Actions > Device Information**
	Displays the VLAN window.	**Actions > Virtual LANs**
	Displays the LAG table.	**Actions > Port LAG**
	Displays the Port Mirroring table.	**Actions > Port Mirroring**
	Displays the Trap Manager Table.	**Actions > Trap Managers**
	Displays addresses of devices connected to the switch.	**Actions > Switch Connected Addresses**
	Opens a web browser to the device's web site.	**Actions > Device Web Site**
	Saves the current configuration to the device.	**Actions > Save Running Configuration**
	Opens the on-line help.	**Help > Contents**
	Selects a VLAN. Ports that are not on the selected VLAN appear dark gray in the Chassis View.	

When you place the cursor on a toolbar icon for one second, a label appears with the name of the button.

Get/Set Toolbar

The Get/Set Toolbar provides buttons for getting and setting configuration parameters for selected ports and LAGs. When a port or LAG is selected, its configuration is reflected on the Get/Set Toolbar. Each group of buttons represents the various possible states of a configuration parameter. For example, the first group of buttons represents the possible speed of a port - 10 Mbps, 100 Mbps, or 1000 Mbps. If the center button is depressed, the port is currently configured to operate at 100 Mbps.

Selected ports and LAGs can be configured using the Get/Set Toolbar. To change the configuration of a port or LAG, click the button which represents the value of the parameter you want to apply to the port or LAG. Click **apply** to update the device with the changes. Click **cancel** to discard the changes. Options not applicable to the selected port or LAG are dimmed.

To configure the ports of a LAG, select the LAG icon in the Tree View or the Chassis View. Ports belonging to a LAG may not be configured by selecting the port.

Multiple ports and LAGs can be simultaneously configured using the Get/Set Toolbar. When multiple ports or LAGs with non-identical configurations are selected, only the parameters whose settings are identical on the selected ports or LAGs are reflected in the Get/Set Toolbar. For example, if a port operating at full duplex and a port operating at half duplex are selected, neither of the duplex mode buttons on the Get/Set Toolbar are depressed.

The table below displays the buttons on the Get/Set Toolbar and explains their functions and settings.

Table 2-2. Get/Set Toolbar

Button	Description
	Get and set the port/LAG's speed: 10 Mbps, 100 Mbps, 1000 Mbps.
	Get and set the port/LAG's mode: Half duplex, Full duplex.
	Get and set the port/LAG's auto-negotiation status: Auto-negotiation Enabled, Auto-negotiation Disabled.
	Apply or cancel the configuration changes made with the Get/Set Toolbar.

Tree View

The Tree View shows a hierarchical representation of the structure of the Avaya P580/P882 Device. To select LAGS, modules, TelCo banks, power supplies, or ports, click on their icons in the Tree View. When an element is selected in the Tree View, the corresponding element is selected in the Chassis View.

*** Note:** Only LAGs with member ports appear in the Tree View.

The highest level of the Tree View represents the device. The second level shows modules and LAGs. The third level shows ports and TelCo port banks.

To expand the view of a contracted element in the tree or to contract the view of an expanded element in the tree:

Double-click the element.

Or

Click the handle next to the element you want to expand or contract.

Desktop

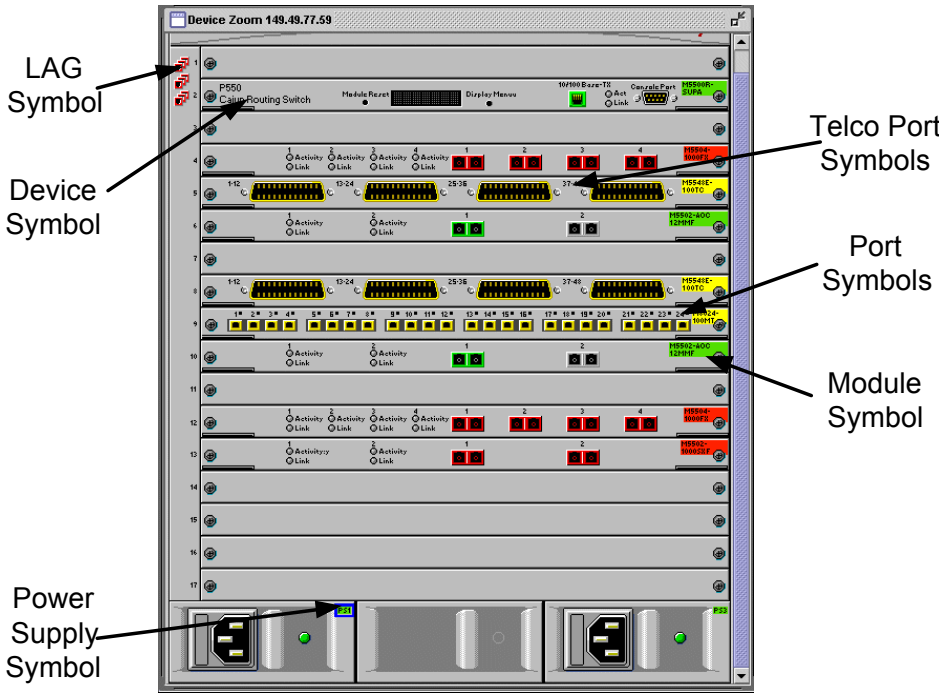
The central section of the application window is the Desktop. This area can be resized by dragging the vertical splitter bars with the mouse. Floating dialog boxes and tables can be resized. The Chassis View, floating dialog boxes, and tables can also be minimized. Minimized windows appear at the bottom of the Desktop.

Chassis View

The Chassis View is a graphical representation of the Avaya P580/P882 Device. The Avaya P580/P882 Device can contain several Avaya P580/P882 modules. The Chassis View shows all of the device's modules, LAGs, and ports. The colors of the modules, LAGs, and ports in the Chassis View reflect their status.

*** Note:** Only LAGs with member ports appear in the Tree View.

Figure 2-2. Avaya P882 Chassis View



When you hold the cursor over a port's icon in the Chassis View, a label appears with the port number, its VLAN ID, and the last fault that occurred on the port. When you hold the cursor over a LAG's icon in the Chassis View, lines extend from the LAG icon to the ports in the LAG, and a label appears with the name and status of the LAG.

When viewing selected tables, the color of the port or LAG indicates the standing of the port or LAG with regard to the application. For example: When creating a Link Aggregation Group (LAG), ports that can be selected appear white in the Chassis View. The port selected to be the base port appears dark blue. The ports selected to be additional ports appear cyan. This color scheme applies to the lines extending from LAG icons to their member ports.

The following table provides a list of the possible port and LAG colors in the Chassis View and their meaning.

Table 2-3. Chassis View Port/LAG Colors

Color	Meaning
Green	The port/LAG is enabled, and its status is Okay.
Yellow	The port/LAG is enabled, and its status is Warning.

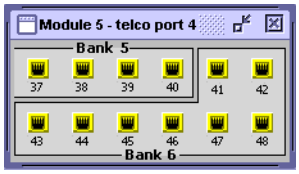
Table 2-3. Chassis View Port/LAG Colors (Continued)

Color	Meaning
Red	The port/LAG is enabled, and its status is Fatal.
Light Gray	The port/LAG is disabled.
Dark Gray	The port/LAG is not associated with the selected VLAN.
White	The port/LAG is logically available for assignment.
Dark Blue	The port/LAG has been assigned the primary position in an application.
Cyan	The port/LAG has been assigned a secondary position in an application.

Viewing TelCo Ports

Some modules have TelCo ports. Each TelCo port symbol represents 12 TelCo ports. To view and configure a TelCo port, click the Telco port symbol in the Chassis View. The TelCo Port window opens on the Desktop.

Figure 2-3. TelCo Port Window



On some TelCo modules, the ports are divided into Banks of 8 ports. Each TelCo Port window shows one and a half TelCo Banks. The ports in the TelCo Port window are divided into their respective Banks, and the Banks are labeled.

Selecting Elements

You can select the device, modules, LAGs, ports, and TelCo banks.

To select the device:

In the Chassis View, click the device's label.

Or

In the Tree View, click the device's icon. The device's label is highlighted in the Chassis View and the Tree View.

To select a module:

In the Chassis View, click the module's label.

Or

In the Tree View, click the module's icon. The module's label is highlighted in the Chassis View and the Tree View.

To select a LAG:

In the Chassis View, click the LAG's icon.

Or

In the Tree View, click the LAG's icon. The LAG is highlighted in the Chassis View and the Tree View.

To select a port:

In the Chassis View, click the port.

Or

In the Tree View, click the port's icon. The port is highlighted in the Chassis View and the Tree View.

— To select multiple elements, press **CTRL** while clicking on each element to be selected.

To select a Telco bank:

In the Tree View, click the bank's label. The bank's label is highlighted in the Tree View.

Dialog Area

The area to the right of the Chassis View is where all dialog boxes, tables, and wizards first appear. This area can be resized by dragging the vertical splitter bar with the mouse. When a dialog box, table, or wizard opens, it replaces the current dialog box open in the Dialog Area. To view more than one dialog box or table simultaneously, click the pushpin in the upper right-hand corner of the dialog box. The dialog box becomes a floating dialog box and moves to the Desktop.

To restore a dialog box to the Dialog Area, click the toolbar button or icon that opened the dialog box. The dialog box returns to the Dialog Area.

Avaya P580/P882 Modes

The Avaya P580/P882 Device Manager has two modes:

- Configuration mode
- Port RMON mode

When in configuration mode, you can view and change the configuration of the Avaya P580/P882 Device and individual ports. When in Port RMON mode, you can view graphical representations of the traffic on individual ports/LAGs.

To switch to configuration mode:

Click  .

Or

Select **View > Configuration**.

To switch to Port RMON mode:

Click  .

Or

Select **View > Port RMON**.

Managing Tables

The Avaya P580/P882 Manager interface displays the status of each row in a table. The following table shows a list of symbols which can appear at the start of a table row, with their corresponding explanations.

Table 2-4. Table Symbols

Symbol	Explanation
	The row has not changed since the device was last updated.
	The row is a new entry.
	The row is to be deleted.
	The information in the row has been changed by the user.

To undo all the changes made to a table, click Refresh. To undo changes made to a selected row, click Undo. When all changes are finalized, click Apply to update the device.

Using Dialog Boxes and Tables

Dialog boxes and tables in the Avaya P580/P882 Manager application have a common set of icons. The following table displays the icons and explains their functions:

Table 2-5. Dialog Box Buttons

Button	Function
Refresh	Refreshes the information in the table or dialog box. This clears any changes made to the table or dialog box and not yet sent to the device.
Apply	Sends the information from the table or dialog box to update the device.
Insert	Adds a row to the table.
Wizard	Starts a wizard.
Delete	Deletes the selected rows of the table.
Undo	Undoes all changes to the selected row in a table.

Using Avaya P580/P882 Device Manager Help

This section explains how to use the on-line help in the Avaya P580/P882 Device Manager. The on-line help can be opened to the contents page or directly to a topic of interest.

Opening the Help to the Contents Page

To open the help to the contents page, select **Help > Contents**. The on-line help opens to the contents page.

Opening the Help to a Topic of Interest

To open the help directly to a topic of interest:

1. Click . The cursor changes to the shape of an arrow with a question mark.

2. Click a point of interest in the Avaya P580/P882 Device Manager. The on-line help opens to a topic explaining the feature that was clicked.

3 Device Configuration

This chapter explains how to view and set the various configuration parameters relevant to the Avaya P580/P882. It includes the following sections:

- **Viewing Device Information** - View high-level information about the Avaya P580/P882 Device.
- **Viewing Power Supply Information** - View power supply information about the Avaya P580/P882 Device.
- **Viewing Module Configuration** - View information specific to an Avaya P580/P882 module in the device.
- **Viewing LAG Configuration** - View information specific to a LAG on an Avaya P580/P882 module in the device.
- **Viewing TelCo Bank Configuration** - View information specific to the TelCo banks on the Avaya P580/P882 Device.
- **Viewing Port Configuration** - View information specific to the ports on the Avaya P580/P882 Device.
- **Saving the Running Configuration** - Save the current configuration of the Avaya P580/P882 Device.
- **Resetting the Device** - Reset the Avaya P580/P882 Device.

To view configuration information, you must be in Configuration mode. To switch to Configuration mode:

Click  .

Or

Select **View > Configuration**.

Viewing Device Information

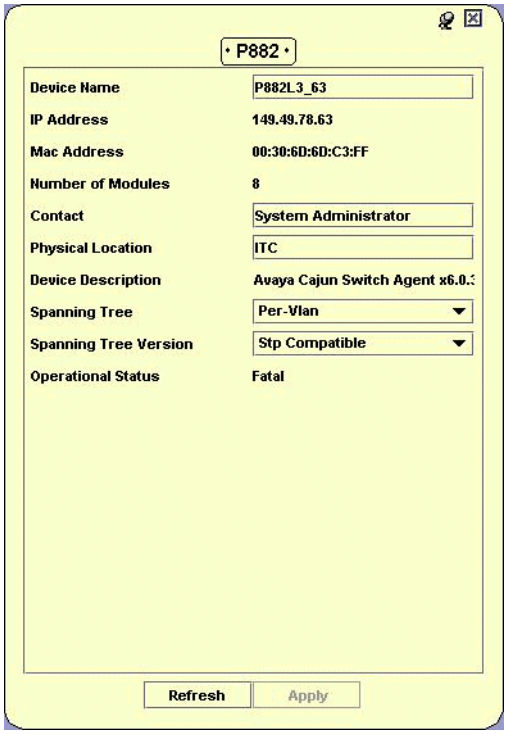
The Device Information dialog box provides you with high-level information specific to the Avaya P580/P882 Device. To view information about the Avaya P580/P882 Device:

Click  .

Or

Click the Device Symbol in the Chassis View. The Device Information dialog box opens.

Figure 3-1. Device Information Dialog Box



The Device Information dialog box provides detailed information about the device. The following table lists the fields in the Device Information dialog box and their descriptions.

Table 3-1. Device Information Dialog Box Fields

Field	Description
Device Name	The user defined name of the device.
IP Address	The IP address of the device.

Table 3-1. Device Information Dialog Box Fields (Continued)

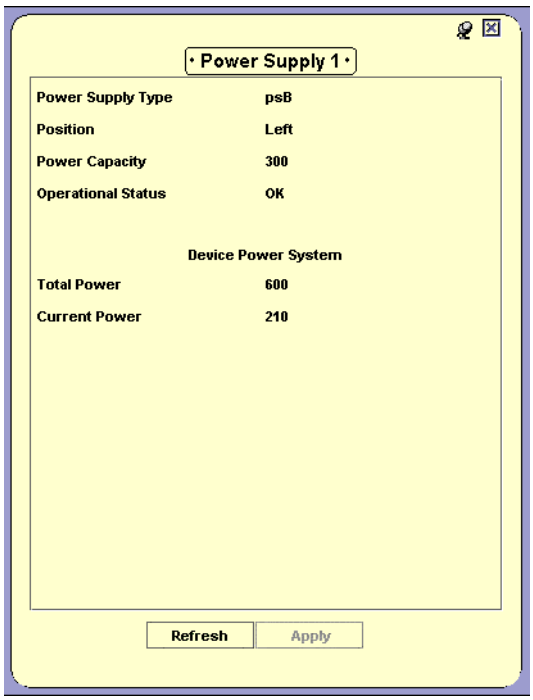
Field	Description
MAC Address	The MAC address of the device.
Number of Modules	The number of modules in the device.
Contact	Individual responsible for the management and maintenance of the device.
Physical Location	The physical location of the device.
Device Description	A detailed description of the device.
Spanning Tree	Spanning Tree setting of the device. Possible values are: • **IEEE 802.1D** • **Per-Vlan** • **Dual-Layer** • **Disable**
Spanning Tree Version	The Spanning Tree version. Possible values are: • **Stp Compatible** • **rstp**
Operational Status	The operational status of the device. Possible values are: • **OK** • **Fatal**

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 15.

Viewing Power Supply Information

The Power Supply dialog box provides you with information about the power supplies in the Avaya P580/P882 Device. To view information on a specific Power Supply, click a Power Supply label in the Chassis View or icon in the Tree View. The Power Supply dialog box opens with the information on the specific Power Supply.

Figure 3-2. Power Supply Dialog Box



The Power Supply dialog box provides detailed information about the device hardware. The following table provides a list of the fields in the Power Supply dialog box and their descriptions.

Table 3-2. Power Supply Dialog Box Fields

Field	Description
Power Supply Type	The model of the power supply.
Position	The position of the power supply. Possible values are: • **Left** • **Center** • **Right**
Power Capacity	The power capacity, in watts.

Table 3-2. Power Supply Dialog Box Fields (Continued)

Field	Description
Operational Status	The operational status of the power supply. Possible values are: • **OK** • **Fatal**
Total Power	The maximum amount of power, in Watts, that can be provided by the power supplies currently in the device.
Current Power	The amount of power, in Watts, currently being used by the device.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 15.

Viewing Module Configuration

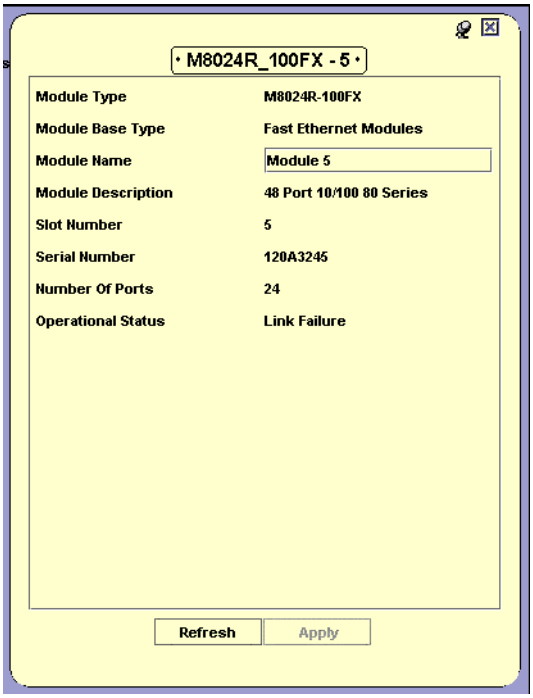
The Module Configuration dialog box provides you with information specific to a selected module. To view the configuration of a module:

Click the module symbol in the Tree View.

Or

Click the module's label in the Chassis View. The Module Configuration dialog box opens.

Figure 3-3. Module Configuration Dialog Box



The Module Configuration dialog box provides detailed information about the module. The following table provides a list of the fields in the Module Configuration dialog box and their descriptions.

Table 3-3. Module Configuration Dialog Box Fields

Field	Description
Module Type	The model of the module.

Table 3-3. Module Configuration Dialog Box Fields (Continued)

Field	Description
Module Base Type	The family of modules to which the module belongs. Module families include: • **Ethernet Modules** • **Fast Ethernet Modules** • **Gigabit Ethernet Modules** • **Supervisor Modules** • **Uplink Modules** • **Unspecified Base**
Module Name	The user defined name of the module.
Module Description	A description of the module.
Slot Number	The slot number where the module is located.
Serial Number	A unique number assigned by Avaya Inc. to the selected module.
Number of Ports	The number of ports on the module.
Operational Status	The operational status of the module. Possible values are: • **OK** • **Fatal** • **Link Failure**

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 15.

Viewing LAG Configuration

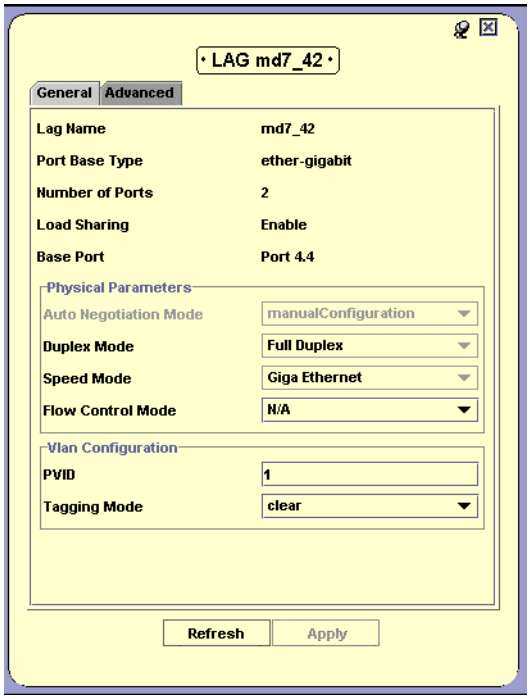
The LAG Configuration dialog box provides you with information specific to a selected LAG. To view the configuration of a LAG:

Click the LAG's symbol in the Tree View.

Or

Click the LAG's icon in the Chassis View. The LAG Configuration dialog box opens to the General tab.

Figure 3-4. LAG Configuration Dialog Box - General Tab



LAG Configuration - General Tab

The General tab of the LAG Configuration dialog box provides detailed information about the LAG, such as the LAG's status, name, physical parameters, VLAN tagging mode, and VLAN ID. The following table lists the fields in the General tab of the LAG Configuration dialog box and their descriptions.

Table 3-4. LAG Configuration - General Tab Fields

Field	Description
LAG Name	The user defined name of the LAG.

Table 3-4. LAG Configuration - General Tab Fields (Continued)

Field	Description
Port Base Type	The type of port serving as the base port of the LAG.
Number of Ports	The number of ports in the LAG.
Load Sharing	The LAG's state. Possible states include: • **Enable** - The LAG is enabled. • **Disable** - The LAG is disabled, and its ports are functioning independently of the LAG.
Base Port	The port serving as the base port of the LAG.
Auto Negotiation Mode	The configured state of the Autonegotiation protocol between two stations. When enabled, Auto-Negotiation detects the highest common denominator for the flow control capabilities of the endstations, and sets both to the same highest common setting. It also delivers remote link status. Possible Auto Negotiation Modes include: • **autoNegotiate** - Autonegotiation is enabled on the LAG. • **manualConfiguration** - Autonegotiation is disabled on the LAG. For more information, refer to *Auto-Negotiation* in *The Reference Guide*.
Duplex Mode	The state of communication of the selected port. Possible values are: **Full Duplex** - The LAG can send and receive simultaneously. **Half Duplex** - The LAG can either receive or send, but can not do both simultaneously.
Speed Mode	The speed of communication of the selected LAG. Possible values are: **Ethernet** - 10 Mbps. **Fast Ethernet** - 100 Mbps. **Gigabit Ethernet** - 1000 Mbps.
Flow Control Mode	The state of flow control on the selected LAG.
PVID	The Port VLAN ID (PVID) of the LAG. This is the VLAN of which the LAG is a member.

Table 3-4. LAG Configuration - General Tab Fields (Continued)

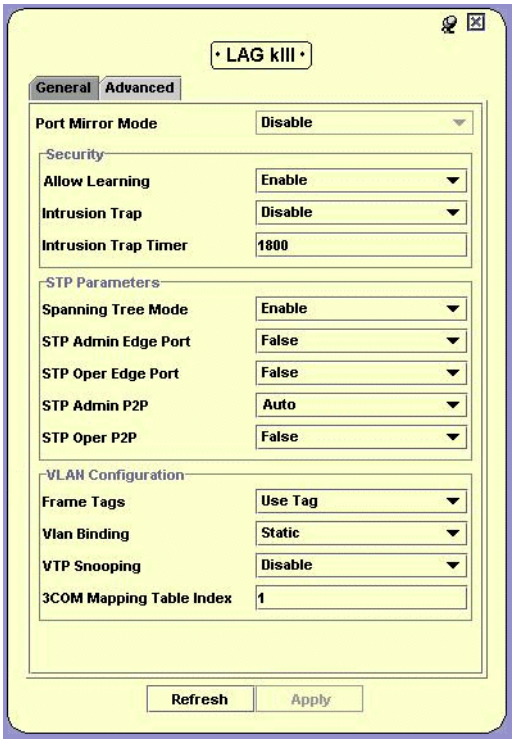
Field	Description
Tagging Mode	The tagging mode of the LAG. For information on tagging modes, refer to "Port Configuration Area" on page 56.

The Get/Set Toolbar provides an alternative, quick method to view and change a LAG's configuration. For more information on the Get/Set Toolbar, refer to "Get/Set Toolbar" on page 8.

LAG Configuration - Advanced Tab

The Advanced tab of the LAG Configuration dialog box provides information about the LAG's Port Mirroring Mode, Security and STP parameters, and VLAN configuration.

Figure 3-5. LAG Configuration Dialog Box - Advanced Tab



The following table lists the fields in the Advanced tab of the LAG Configuration dialog box and their descriptions.

Table 3-5. LAG Configuration - Advanced Tab Fields

Field	Description
Port Mirror Mode	The state of Port Mirroring on the LAG. Possible values are: • **Enabled** - Port Mirroring is enabled. • **Disabled** - Port Mirroring is disabled.
Allow Learning	The LAG's method of handling packets from unknown sources. Possible states are: • **Enable** - The LAG can learn new addresses and receive packets from them. • **Disable** - The LAG is prevented from learning new addresses. It does not accept packets from unknown addresses. This is a useful security feature. For more information, refer to *Security* in *The Reference Guide*.
Intrusion Trap	The state of Intrusion Trap on the LAG. Possible values are: • **Enable** - A trap is sent when an unknown MAC address is received and **Allow Learning** is disabled. • **Disable** - Intrusion Trap is disabled. This is the default.
Intrusion Trap Timer	The amount of time, in seconds, between sending intrusion traps.
Spanning Tree Mode	The state of Spanning Tree on the LAG. Possible states include: • **Enable** - The LAG participates in the Cisco VTP protocol and allows VTP Snooping to run a reduced number of trunk ports. • **Disable** - The LAG does not participate in the Cisco VTP protocol.
STP Admin Edge Port	The STP Admin Edge Port status. Possible values are: • **True** • **False**

Table 3-5. LAG Configuration - Advanced Tab Fields (Continued)

Field	Description
STP Oper Edge Port	The STP Oper Edge Port status. Possible values are: • **True** • **False**
STP Admin P2P	The STP Admin P2P setting. Possible values are: • **Force True** • **Force False** • **Auto**
STP Oper P2P	The STP Oper P2P status. Possible values are: • **True** • **False**
Frame Tags	The port's VLAN framing operation mode regarding incoming packets. Possible modes are: **Use Tag** - Incoming packets remain bound to the tagged VLAN. **Ignore Tag** - Incoming packets are bound to the LAG's default VLAN.

Table 3-5. LAG Configuration - Advanced Tab Fields (Continued)

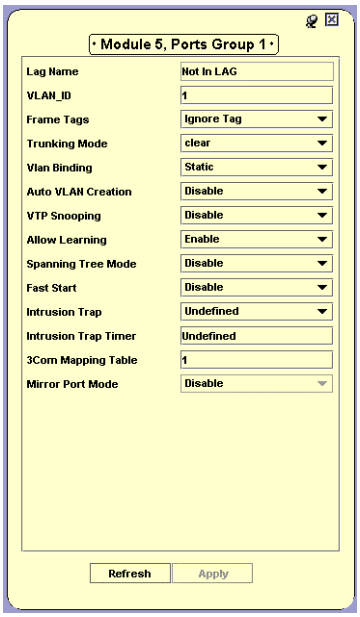
Field	Description
VLAN Binding	The method used by the LAG for VLAN binding. Possible methods include: • **Static** - VLANs can only be bound to the LAG manually. • **Persistent** - All VLANs known to the device are bound to the LAG. *** Note:** When a tagged IEEE 802.1Q packet arrives on a LAG that is configured to bind to all and the VLAN does not exist on the device, the packet is forwarded on the LAG's default VLAN. To prevent unintended forwarding of unknown VLAN traffic to the LAG's default VLAN, configure the LAG default VLAN to Discard. The automatic VLAN creation feature does not work if the LAG's default VLAN is the discard VLAN, because the device does not learn this VLAN. • **Dynamic** - Binds this LAG to any VLAN from which it receives traffic.
VTP Snooping	The state of VTP snooping on the LAG. Possible states include: • **Enable** - The LAG participates in the Cisco VTP protocol and allows VTP Snooping to run a reduced number of trunk ports. • **Disable** - The LAG does not participate in the Cisco VTP protocol.
3COM Mapping Table Index	The 3COM VLAN mapping table associated with the LAG.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 15.

Viewing TelCo Bank Configuration

The TelCo Bank Configuration dialog box provides you with information specific to a selected TelCo Bank. To view the configuration of a TelCo Bank, click the TelCo Bank's symbol in the Tree View. The TelCo Bank Configuration dialog box opens.

Figure 3-6. TelCo Bank Configuration Dialog Box



The TelCo Bank Configuration dialog box provides detailed information about the TelCo Bank, such as the VLAN tagging mode, VLAN ID, priority level, and mode of operation.

For information on the fields in the TelCo Bank Configuration dialog box, refer to "Viewing Port Configuration" on page 31.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 15.

Viewing Port Configuration

The Port Configuration dialog box provides you with information specific to a selected port. To view the configuration of a port:

Click the port symbol in the Tree View.

Or

Click the port in the Chassis View.

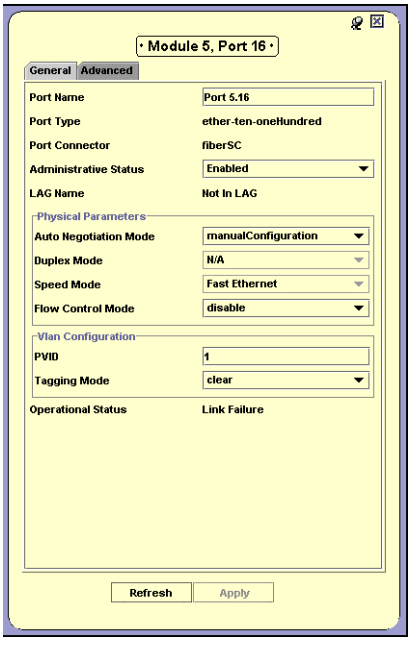
To view the configuration of a TelCo port:

Click the port symbol in the Tree View.

Or

1. Click the TelCo port symbol in the Chassis View. The TelCo Port window opens.
2. Click the TelCo port in the TelCo port window. The Port Configuration dialog box opens.

Figure 3-7. Port Configuration Dialog Box - General Tab



To switch between the General page and the Advanced page of the Port Configuration dialog box, click the appropriate tab.

Port Configuration - General Tab

The Port Configuration dialog box provides detailed information about the port. The General page of the Port Configuration dialog box provides basic information about the port.The following table provides a list of the fields in the Port Configuration dialog box General tab and their descriptions.

Table 3-6. Port Configuration Dialog Box Fields - General Tab

Field	Description
Port Name	The user defined name of the port.
Port Type	The type of port.
Port Connector	The port's connector type. Possible connector types include: • **Internal** • **RJ45** • **Fiber-ST** • **Fiber-SC** • **RS232** • **AUI** • **RJ71** • **GBIC-1000-SX** • **GBIC-1000-LX** • **GBIC-1000-LX-LH**
Administrative Status	The activity mode of the port. Possible modes include: • **Enabled** - The port is enabled. • **Disabled** - The port is disabled.
LAG Name	The name of the LAG in which the port is a member. If the port is not a member of a LAG, the Link Aggregation Name is **`Not In LAG`**.

Table 3-6. Port Configuration Dialog Box Fields - General Tab

Field	Description
Auto Negotiation Mode	The configured state of the Autonegotiation protocol between two stations. When enabled, Auto-Negotiation detects the highest common denominator for the flow control capabilities of the endstations, and sets both to the same highest common setting. It also delivers remote link status. Possible Auto Negotiation Modes include: • **autoNegotiate** - Autonegotiation is enabled on the port. • **manualConfiguration** - Autonegotiation is disabled on the port. For more information, refer to *Auto-Negotiation* in *The Reference Guide*.
Duplex Mode	The state of communication of the selected port. Possible values are: • **Full Duplex** - The port can send and receive simultaneously. • **Half Duplex** - The port can either receive or send, but can not do both simultaneously. • **N/A** - The port does not report duplex state.
Speed Mode	The speed of communication of the selected port. Possible values are: • **Ethernet** - 10 Mbps. • **Fast Ethernet** - 100 Mbps. • **Gigabit Ethernet** - 1000 Mbps.
Flow Control Mode	The state of flow control on the selected port. Possible values are: • **Enable** - Flow control is enable on this port. • **Disable** - Flow control is disabled on this port.
PVID	The number of the VLAN of which the port is a member.

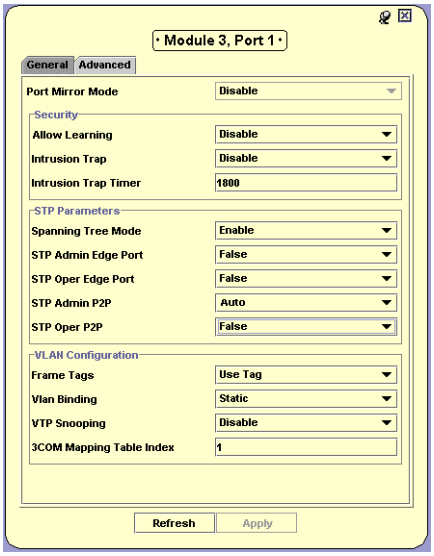
Table 3-6. Port Configuration Dialog Box Fields - General Tab

Field	Description
Tagging Mode	The tagging mode of the LAG. For information on tagging modes, refer to "Port Configuration Area" on page 56.
Operational Status	The operational status of the port.

Port Configuration - Advanced Tab

The Advanced tab of the PortConfiguration dialog box provides information about the port's Port Mirroring Mode, Security and STP parameters, and VLAN configuration.

Figure 3-8. Port Configuration Dialog Box - Advanced Tab



The following table provides a list of the fields in the Port Configuration dialog box Advanced tab and their descriptions.

Table 3-7. Port Configuration Dialog Box Fields - Advanced Tab

Field	Description
Port Mirror Mode	The state of Port Mirroring on the port. Possible values are: • **Enabled** - Port Mirroring is enabled. • **Disabled** - Port Mirroring is disabled.

Table 3-7. Port Configuration Dialog Box Fields - Advanced Tab

Field	Description
Allow Learning	The port's method of handling packets from unknown sources. Possible states are: • **Enabled** - The port can learn new addresses and receive packets from them. • **Off** - The port is prevented from learning new addresses. It does not accept packets from unknown addresses. This is a useful security feature. For more information, refer to *Security* in *The Reference Guide*.
Intrusion Trap	The state of Intrusion Trap on the port. Possible values are: • **Enable** - A trap is sent when an unknown MAC address is received on the port and **Allow Learning** is disabled. • **Disable** - Intrusion Trap is disabled. This is the default.
Intrusion Trap Timer	The amount of time, in seconds, between sending intrusion traps.
Spanning Tree Mode	The state of Spanning Tree Protocol. Possible states are: • **Disable** - STP is disabled. This is the default state. • **Enable** - STP is enabled. When activating STP, keep in mind that: • All bridges should run STP. • Redundancy applications and STP cannot co-exist. For more information refer to *Spanning Tree Algorithm (STA)* in *The Reference Guide*.
STP Admin Edge Port	The STP Admin Edge Port status. Possible values are: • **True** • **False**

Table 3-7. Port Configuration Dialog Box Fields - Advanced Tab

Field	Description
STP Oper Edge Port	The STP Oper Edge Port status. Possible values are: • **True** • **False**
STP Admin P2P	The STP Admin P2P setting. Possible values are: • **Force True** • **Force False** • **Auto**
STP Oper P2P	The STP Oper P2P status. Possible values are: • **True** • **False**
Frame Tags	The port's VLAN framing operation mode regarding incoming packets. Possible modes are: • **Ignore** - Incoming packets are bound to the port's default VLAN. • **Use Tag**- Incoming packets remain bound to the tagged VLAN.

Table 3-7. Port Configuration Dialog Box Fields - Advanced Tab

Field	Description
Vlan Binding	The method used by the port for VLAN binding. Possible methods include: • **Static** - VLANs can only be bound to the port manually. • **Bind to All** - All VLANs known to the device are bound to the port. *** Note:** When a tagged IEEE 802.1Q packet arrives on a port that is configured to bind to all and the VLAN does not exist on the device, the packet is forwarded on the port's default VLAN. To prevent unintended forwarding of unknown VLAN traffic to the port's default VLAN, configure the port default VLAN to Discard. The automatic VLAN creation feature does not work if the port's default VLAN is the discard VLAN, because the device does not learn this VLAN. • **Bind to Received** - Binds this port to any VLAN from which it receives traffic.
VTP Snooping	The state of VTP Snooping on the port. Possible states include: • **Enable** - The port participates in the Cisco VTP protocol and allows VTP Snooping to run a reduced number of trunk ports. • **Disable** - The port does not participate in the Cisco VTP protocol.
3COM Mapping Table Index	The number of incoming tagged frames from 3Com equipment are mapped to Avaya VLANs.

The Get/Set Toolbar provides an alternative, quick method to view and change the port's basic configuration. For more information on the Get/Set Toolbar, refer to "Get/Set Toolbar" on page 12.

*** Note:** The configuration of ports that participate in a LAG cannot be changed using the Port Configuration dialog box. Use the LAG Configuration dialog box instead.

*** Note:** The information fields in the Port Configuration dialog box vary according to the type of port selected.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 15.

Saving the Running Configuration

All changes to the configuration of the Avaya P580/P882 Device apply only to the Running Configuration. When the device is reset, all unsaved changes are lost. When the configuration is saved to the Startup Configuration, the saved configuration is used when the device is reset.

To save the Running Configuration to the Startup Configuration:

Click  .

Or

Select **Actions > Save Running Configuration**. The Running Configuration is saved to the Startup Configuration.

Resetting the Device

To reset the Avaya P580/P882 Device:

1. Select **Action > Reset Device**. A confirmation dialog box opens.
2. Click **Save and Reset** to save the running configuration before resetting the device.

   Or

   Click **Reset Only** to reset the device without saving the running configuration. The device resets.

*** Note:** You can only reset the device if you accessed the device as an administrator. For more information on admission levels, refer to "Admission Level" on page 4.

4 Port RMON

This chapter explains the port RMON options of the Avaya P580/P882 Device. It includes the following sections:

- **Displaying the Port RMON Window**- How to display the Port RMON window, and an explanation the Port RMON window.
- **Traffic Types** - How to select traffic to monitor in the Port RMON window.

*** Note:** In this chapter, ports include LAGs. i.e. Any mention of a port refers to a port or LAG.

To view Port RMON information, you must be in Port RMON mode. To switch to Port RMON mode:

Click  .

Or

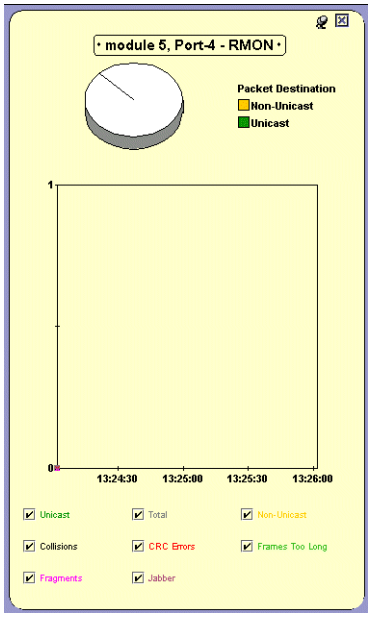
Select **View > Port RMON**.

For more information on RMON, refer to *RMON* in *The Reference Guide*.

Displaying the Port RMON Window

To display the Port RMON window, select a port or a LAG in the Chassis or Tree View. The Port RMON window opens.

Figure 4-1. Port RMON Window



The Port RMON window includes three sections. At the top of the window is a pie chart. In the center of the window is a graph section. At the bottom of the window is a list of traffic types.

The Pie Chart

The pie chart shows the relative amounts of Unicast and Non-Unicast traffic on a selected port or LAG. The legend to the right of the pie chart shows the color representing each of the traffic types.

The Traffic Graph

The graph charts various traffic types over time. Each traffic type is represented by a different colored line. Using the mouse, you can view traffic statistics, zoom in or out of the graph, and scroll within the graph to view parts of the graph that are currently hidden.

When changing the view on the graph, the graph freezes. To unfreeze the graph and restore the display to the default display, click on the graph.

Viewing Traffic Statistics

To view traffic statistics, hold the mouse over a point on the graph representing the traffic for which you would like to see statistics. After two seconds, an info box appears displaying the name of the traffic type represented by the line in the graphic, and the traffic rate at the selected point.

Zooming In and Out of the Graph

To zoom out and view a graph of all the traffic on the selected port from the time the application was opened, double-click the graph. The graph is compressed to show all of the traffic on the port from the time the application was opened until now.

To zoom in on a portion of the graph, press **SHIFT** and select a portion of the graph using the mouse. The graph zooms in and shows only the portion of the graph that was selected.

Scrolling within the Graph

To scroll within the graph, hold the left mouse button down while moving the mouse from the graph in the direction you want to scroll. The graph scrolls in the selected direction.

Unfreezing the Graph

When zooming or scrolling within the graph, the display freezes and is not updated with the current information. To reactivate the display, click anywhere in the graph. The graph display is restored to normal, and the graph is reactivated.

Traffic Types

The bottom of the Port RMON window contains a list of various types of traffic. Each traffic type has a checkbox next to it. Only traffic types whose checkboxes are checked are displayed in the Port RMON graph.

The following table provides a list of the available traffic types and their descriptions.

Table 4-1. Traffic Types

Field	Description
Collisions	Total number of Ethernet collisions in which the port was involved.
CRC Errors	Total number of Ethernet packets received at this port with FCS error and Framing error. This indicates the number of corrupted packets received.

Table 4-1. Traffic Types (Continued)

Field	Description
Fragments	Total number of Ethernet packets received at this port whose octet count is less than the minimum standard packet length.
Frames too Long	Total number of Ethernet packets received at this port whose octet count is more than the maximum standard packet length.
Jabber	Total number of Ethernet packets received at this port that are too long and include CRC errors.
Non-Unicast	Total number of good packets directed to non-unicast addresses that were received on the port.
Total	Total number of packets of valid frame length that were received on the port.
Unicast	Total number of good packets received that were directed to a unicast address.

5 Link Aggregation Groups

This chapter provides the information and instructions for creating and using Link Aggregation Groups (LAGs). It includes the following topics:

- **LAGs Overview** - An overview of LAGs.
- **Viewing the LAG Table** - Instructions on accessing the LAG Table and a description of the LAG Table.
- **Creating LAGs** - Instructions on creating LAGs.
- **Editing LAGs** - Instructions on editing LAGs.
- **The LAG Wizard** - Detailed descriptions of the screens in the LAG Wizard.
- **Deleting LAGs** - Instructions on deleting LAGs.

For information on configuring LAGs, refer to "Viewing LAG Configuration" on page 24"Viewing LAG Configuration" on page 24.

LAGs Overview

Link Aggregation Groups (LAGs) provide a method of creating a high-bandwidth link. A LAG consists of a group of ports acting as a single logical port. All ports participating must have the same configuration.

For more information on LAGs, refer to *Link Aggregation Groups (LAGs)* in *The Reference Guide*.

Viewing the LAG Table

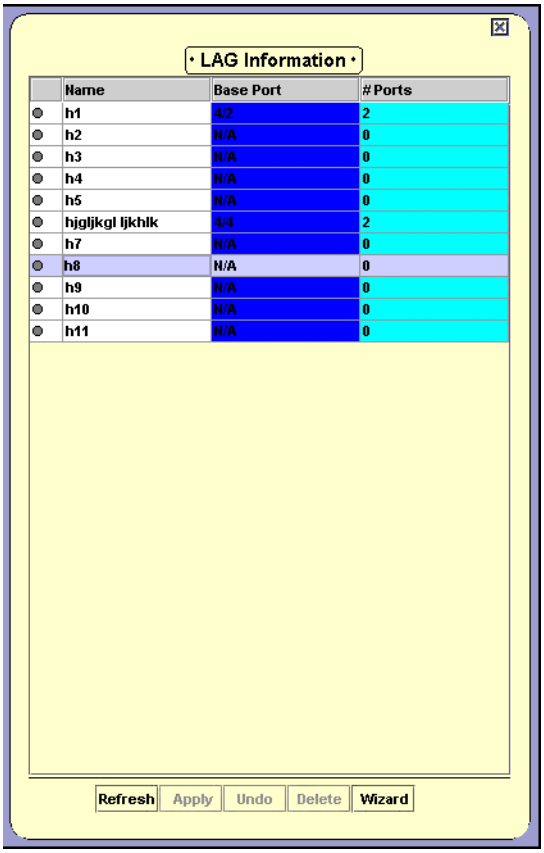
To view the LAG Table:

Click  .

Or

Select **Actions > Port LAGs**. The LAG Information table opens.

Figure 5-1. LAG Information Dialog Box



Each row of the LAG table represents a valid Link Aggregation Group and provides the following information:

- **Name** - The LAG name.
- **Base Port** - The number of the LAG's base port.
- **# Ports** - The number of ports assigned to the LAG.

When a LAG is selected, the ports in the LAG appear highlighted in the Chassis and Tree View.

Creating LAGs

To create a new LAG, click Wizard. The LAG Wizard starts.

For more information, refer to "The LAG Wizard" on page 45.

Editing LAGs

To edit an existing LAG:

1. Select a LAG by clicking on the row representing the LAG.
2. Click Wizard.
   - If the LAG contains ports, the LAG Wizard starts with the **LAG Wizard - Other Port Selection** screen.
   - If the LAG contains no ports, the LAG Wizard starts with the **LAG Wizard - Base-Port Selection** screen.

When editing a LAG, the LAG Wizard's dialog boxes display the current LAG configuration parameters. To keep the values currently displayed in one of the dialog boxes, click **Next**. If you have changed some of the LAG's parameters, and you want to keep the rest of the LAG's configuration, click **Finish**. The device is updated with the LAG's new configuration.

For more information, refer to "The LAG Wizard" on page 45.

The LAG Wizard

This section provides detailed information on each of the LAG Wizard's screens. To continue to the next screen, click **Next**. To return to an earlier screen, click **Back**. To exit the LAG Wizard without making any changes, click **Cancel**.

The LAG Wizard consists of the following screens:

- **Welcome**
- **Base Port Selection**
- **Other Port Selection**
- **LAG Name**

- **Confirmation**

The following sections describe each of the LAG Wizard screens.

LAG Wizard - Welcome

The LAG Wizard provides a simple, step-by-step method for creating a LAG.

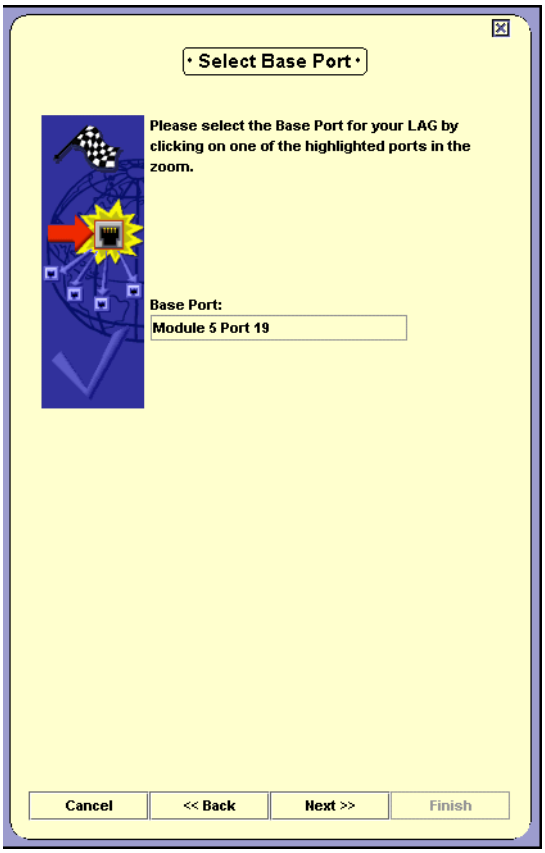
Figure 5-2. LAG Wizard - Welcome Screen

To continue, click **Next**. The LAG Wizard continues with the **LAG Wizard - Base-Port Selection** screen.

LAG Wizard - Base-Port Selection

The Base-Port Selection screen of the LAG Wizard helps you select a base port for the LAG. The attributes of the base port (port speed, port mode, etc.) are applied to the other member ports of the LAG. Ports which can be selected as base ports appear white in the Chassis View.

Figure 5-3. LAG Wizard - Base-Port Selection Screen



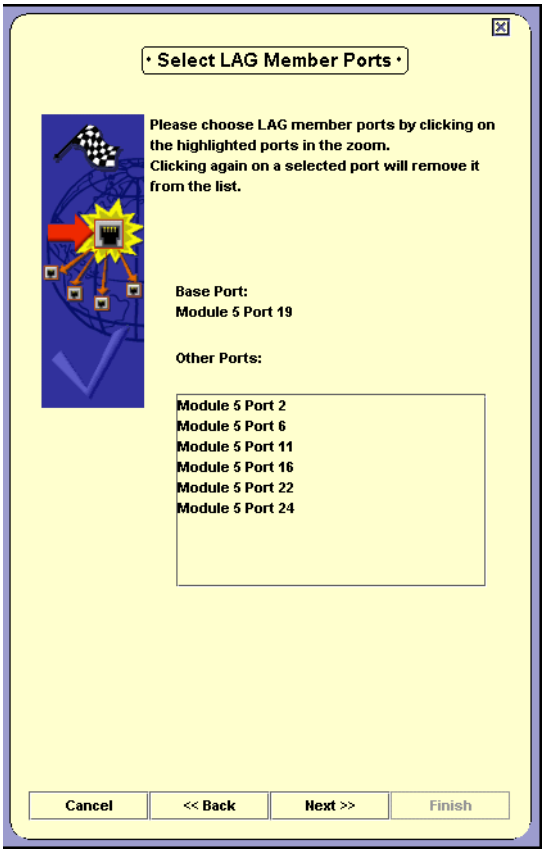
To select a base-port for the LAG, click a port in the Chassis View. The selected port is listed in the Base Port field of the wizard and appears blue in the Chassis View and Tree View.

When you have selected the base-port for the LAG, click **Next**. The LAG Wizard continues with the **LAG Wizard - Other Port Selection** screen.

LAG Wizard - Other Port Selection

The Other Port Selection screen of the LAG Wizard helps you select additional ports for the LAG. Ports which can be selected as additional ports appear in white in the Chassis View.

Figure 5-4. LAG Wizard - Other Port Selection Screen



To select additional ports for the LAG, click ports in the Chassis View. The selected ports appear cyan in the Chassis View Tree View and are listed in the Other Ports field in the wizard.

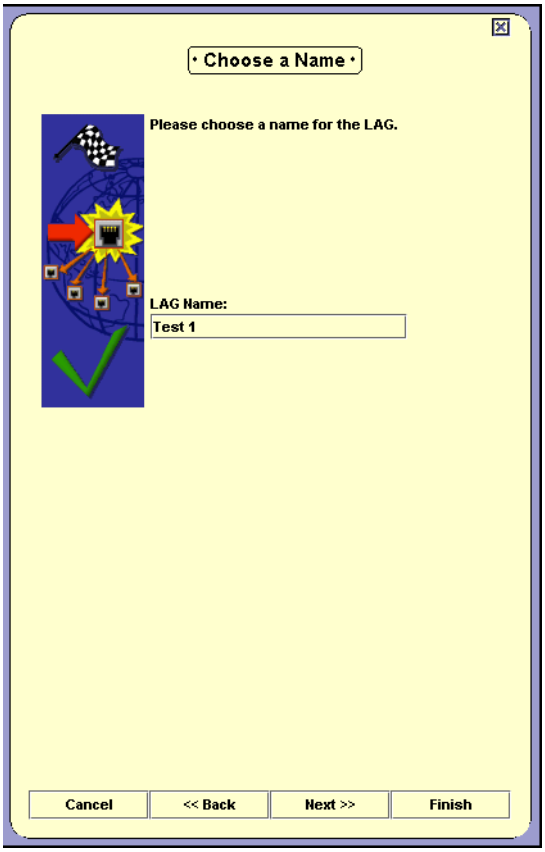
To remove selected ports from the list, click the selected ports in the Chassis View. The selected ports appear white in the Chassis View and Tree View and are removed from the Other Ports field in the wizard.

When you have finished selecting the additional ports for the LAG, click **Next**. The LAG Wizard continues with the **LAG Wizard - LAG Name** screen.

LAG Wizard - LAG Name

The LAG Name screen of the LAG Wizard enables you to assign a name to the LAG.

Figure 5-5. LAG Wizard - LAG Name Screen



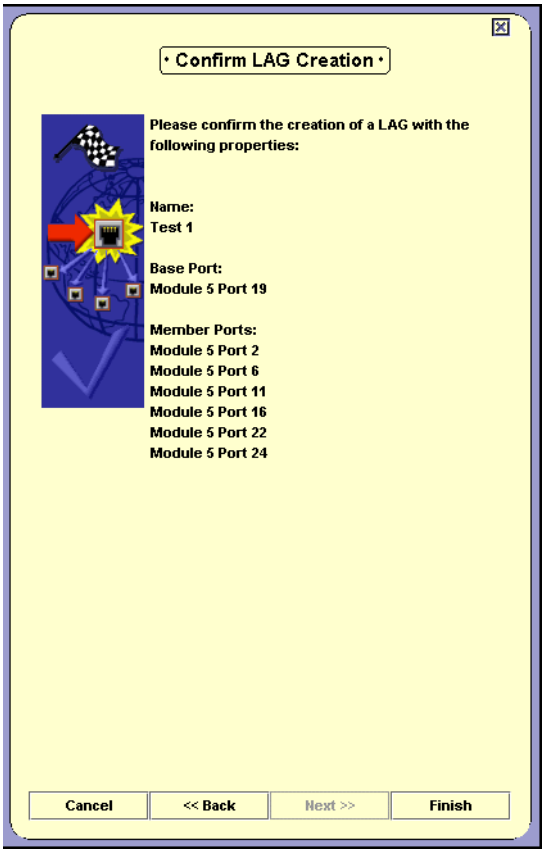
To assign a name to the LAG, enter the name for the LAG in the LAG Name field.

When you have entered a name for the LAG, click **Next**. The LAG Wizard continues with the **LAG Wizard - Confirmation** screen.

LAG Wizard - Confirmation

The LAG Wizard displays a summary of the LAG information entered using the previous screens. The LAG has not yet been created.

Figure 5-6. LAG Wizard - Confirmation Screen



To make any changes to the summary information:

1. Click **Back** until you reach the screen you want.
2. Change the LAG's parameters.
3. Click **Next** until you reach the Confirmation screen.

To create the LAG or apply the changes to the LAG's configuration, click **Finish**. The LAG information is uploaded to the device, and the LAG table is refreshed.

Deleting LAGs

To delete an existing LAG:

1. Select a LAG by clicking on the row representing the LAG.
2. Click Delete.
3. The LAG is marked with the ✕ symbol.
4. Click Apply to update the device.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 18.

For more information on tables, refer to "Managing Tables" on page 14.

6 VLANs

This chapter provides the information and instructions you need to use VLANs. It includes the following topics:

- **VLAN Configuration Overview** - An overview of VLANs and their components.
- **Viewing the VLAN Configuration Dialog Box** - Instructions on how to access the VLAN Configuration dialog box and a description of the VLAN Configuration dialog box.
- **Managing VLANs** - Instructions on how to create, delete, and rename VLANs.
- **Viewing Port VLAN Settings** - Instructions on how to view VLAN settings for ports on the device.
- **Managing Port VLAN Settings** - Instructions on how to configure VLAN settings for ports on the device.
- **Updating the Device** - Instructions on how to update the device with new VLAN information.

*** Note:** In this chapter, ports include LAGs. Any mention of a port refers to a port or LAG.

VLAN Configuration Overview

This section contains an overview of VLANs and how to configure them, and contains the following sections:

- **VLANs Overview**
- **Master VLAN List**
- **VLAN Tags**

VLANs Overview

The building blocks of VLANs are switch ports. To build a new VLAN you need to define a VLAN name and number. You can then add switch ports to the VLAN by configuring the PVID of the port to the VLAN number. The ports are members of the VLAN whose number is their PVID. In addition, you can configure the VLAN tagging mode and binding style of the switch ports. VLAN #1 is the default VLAN and is named **Default**.

For more information about VLANs, refer to *VLANs* in *The Reference Guide*.

Master VLAN List

The master VLAN list is a file on the network management station that contains a list of globally defined VLANs and their names. This list is only available when running Avaya Network Manager. It is not available when running an Embedded Web Manager. To manage the master VLAN list, use Avaya VLAN Manager. For information on Avaya VLAN Manager, refer to the *Avaya VLAN Manager User Guide*.

VLANs that are listed in the master VLAN list are called globally known VLANs. VLANs that are not in the master VLAN list but are configured on a device are called locally known VLANs.

VLAN Tags

Packets can be tagged with VLAN information. When a tagged packet enters a switch port, it maintains its tag. When an untagged packet enters a switch port, the packet is tagged with the port's PVID (Port VLAN ID).

When a packet arrives at the egress port, the VLAN Binding Style is checked. If the packet's VLAN tag does not match a VLAN to which the egress port is bound, the packet is discarded. If the tag matches a VLAN to which the egress port is bound, the Tagging Mode is used. If the Tagging Mode is Clear, the packet is forwarded with no VLAN tag. If the Tagging Mode is anything else, the packet is forwarded with its VLAN tag.

Viewing the VLAN Configuration Dialog Box

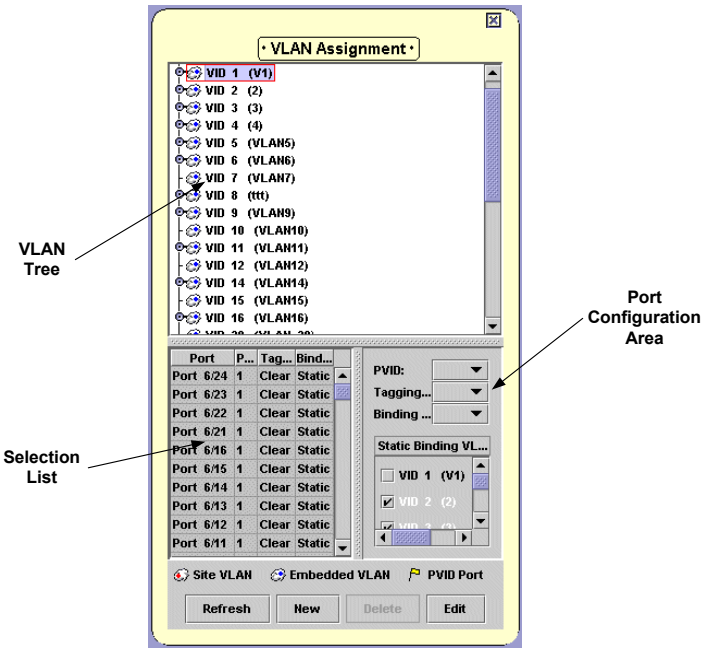
To view VLAN names, numbers, and component switch ports:

Click  .

Or

Select **Actions > VLAN Configuration**. The VLAN Configuration dialog box opens.

Figure 6-1. VLAN Configuration Dialog Box



The VLAN Configuration dialog box consists of the following components:

- **VLAN Tree**
- **Selection List**
- **Port Configuration Area**

To refresh the information in the VLAN Configuration dialog box and lose all unapplied changes, click **Refresh**.

To resize the three areas of the VLAN Configuration dialog box, use the splitter bars.

VLAN Tree

A tree providing a list of VLANs and their ports. The VLANs include all VLANs known on the network and all VLANs configured on the device. The ports listed under a VLAN include member ports and ports statically bound to the VLAN.

To expand or contract a branch of the table:

Double-click the VLAN's name.

Or

Click the handle next to the VLAN's name.

If the VLAN name on the device differs from the globally defined VLAN name, the local VLAN name appears after the VLAN number, followed by the global VLAN name in braces. For example, if VLAN 4 is locally named **RandD**, and globally named **Research**, the following string will appear in the VLAN Tree: **`4 RandD {Research}`**. To change all locally defined VLAN names to the globally defined names, you can synchronize the VLAN names on the device. For information on synchronizing VLAN names, refer to "Synchronizing VLAN Names" on page 59.

*** Note:** When using the Embedded Web Device Manager, global VLAN information is not available.

The VLAN's member ports appear with a yellow triangle and blue triangle next to the port name. Ports that are statically bound to the VLAN appear with a blue triangle attached to the port name. Member ports are automatically bound to the VLANs of which they are members. Ports whose VLAN information has changed but has not been applied, appear with gray triangles.

When a VLAN is selected in the VLAN Tree, member ports appear in the Chassis View with a yellow triangle and blue triangle on the port symbol, and statically bound ports appear in the Chassis View with a blue triangle on the port symbol. In addition, information about the member ports and statically bound ports appear in the Selection List.

For more information about the Selection List, refer to "Selection List" on page 56.

Selection List

The Selection List contains a table with VLAN information about the current selection. For example, if you select a module in the Tree View or Chassis View, a list of the ports in the module with their VLAN information appears in the Selection List.

The following table provides a list of the information fields in the Selection List and their descriptions.

Table 6-1. Selection List Fields

Field	Description
Port	The module and port number.
PVID	The Port VLAN ID (PVID) of the port. This is the VLAN of which the port is a member.
Tagging Mode	The tagging mode of the port. For information on tagging modes, refer to "Port Configuration Area" on page 56.
Binding Style	The binding style configured on the port. For information on binding styles, refer to "Port Configuration Area" on page 56.

To sort the Selection List table by any of its fields, click the field header. To reverse the order of the sort, click the field header a second time.

The information in the Selection List is read-only.

Port Configuration Area

The Port Configuration Area enables you to configure a port's VLAN configuration. The following table provides a list of the configuration parameters in the Port Configuration Area and their description.

Table 6-2. Port Configuration Area Parameters

Field	Description
PVID	The Port VLAN ID (PVID) of the port. This is the VLAN of which the port is a member. The PVID pull-down list contains all VLANs known to the network and VLANs on the device.

Table 6-2. Port Configuration Area Parameters (Continued)

Field	Description
Tagging Mode	The tagging mode of the port. The tagging mode controls the tagging of packets that can be forwarded by the port. The following tagging modes are available: • **Clear** - The packet is forwarded with no VLAN tag. • **IEEE-802.1Q** - The packet is forwarded with a VLAN tag in conformance with the IEEE-802.q standard.
Binding Style	The binding style configured on the port. The binding style defines which packets can be forwarded by the port. The following binding styles are available: • **Bind to All** - The port is bound to all VLANs known to the device. This is also known as persistent binding. If a packet is on a VLAN not known to the device, the packet is discarded. • **Bind to Received** - The port is bound to all VLANs known to the device and to the VLANs with which packets reaching the ports are tagged. This is also known as dynamic binding. If a packet is on a VLAN not known to the device, the packet is discarded. • **Static** - The port is bound to the VLANs checked in the Static Binding VLANs list. Packets on all other VLANs are discarded.
Static Binding VLANs	A list of VLANs known on the network and VLANs configured on the device. Each VLAN has an accompanying checkbox. Possible values are: • **Checked** - The VLAN is bound to the port being configured. • **Unchecked** - The VLAN is not bound to the port being configured. *** Note:** The settings are only used when the port is configured with the **Static** Binding Style.

Managing VLANs

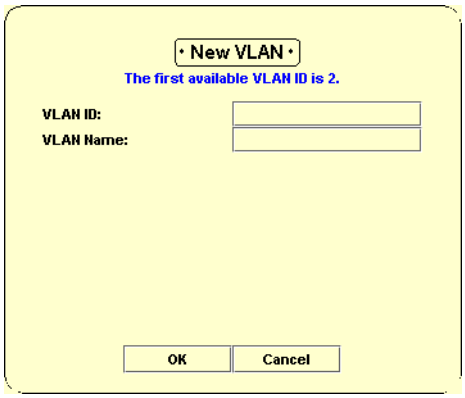
You can create, delete, and rename VLANs.

Creating VLANs

To create a new VLAN:

1. Click **New**. The Create VLAN dialog box opens.

Figure 6-2. Create VLAN Dialog Box



2. Enter a VLAN number in the VLAN ID field.

*** Note:** The range of valid VLAN numbers is 1 to 4095.

3. Enter a name for the VLAN in the VLAN Name field.
4. Click **OK**. The new VLAN is created.

Renaming VLANs

To rename a VLAN:

1. Select the VLAN whose name you want to edit.

2. Click **Rename**. The Rename VLAN dialog box opens.

Figure 6-3. Rename VLAN Dialog Box

3. Enter a name for the VLAN in the VLAN Name field.

4. Click **OK**. The VLAN is renamed.

Synchronizing VLAN Names

VLANs with the same VLAN number can be defined with different names on different devices in the network. In addition, VLAN names can be configured in the master VLAN list. This can cause confusion when referring to a VLAN by name rather than by number. The VLAN application enables you to synchronize the VLAN names on the device with those in the master VLAN list.

When synchronizing the VLAN names on the device with those in the master VLAN list, the VLANs on the device are renamed to provide consistency with the names in the master VLAN list.

To synchronize VLAN names on the device with the master VLAN list:

1. Click **Sync**. A confirmation dialog box opens.

2. Click **Yes**. The VLANs on the device are renamed with the VLAN names in the master VLAN list.

Deleting VLANs

To delete a VLAN:

1. Select the VLAN you want to delete.

2. Ensure that there are no member ports associated with the VLAN.

3. Click **Delete**. The VLAN is deleted.

Managing Port VLAN Settings

You can view and configure the PVID, Tagging Mode, and Binding Style of selected ports using the Selection List and Port Configuration Area. In addition, you can configure the PVID of selected ports using the drag-and-drop method.

Selecting Ports

This section explains how to select ports for VLAN configuration.

Ports can be selected from the Tree View, Chassis View, or VLAN Tree for VLAN Configuration.

- To select a port, click the port in the Tree View, Chassis View, or VLAN Tree.
- To select multiple ports, press **CTRL** while selecting additional ports.
- To select all of the ports on a module, click the module icon in the Tree View or Chassis View.
- To select all of the ports on the device, click the device icon in the Tree View or Chassis View.
- To select all of the ports associated with a VLAN (including member ports and statically bound ports), click the VLAN in the VLAN Tree.

Viewing Port VLAN Settings

To view the VLAN configuration of a port, select a port in the Tree View, Chassis View, or VLAN Tree. The port's VLAN configuration appears in the Selection List. If you select multiple ports in the Tree View, Chassis View, or VLAN Tree, the VLAN configurations for all of the selected ports appear in the Selection List. In addition, parameters that are common to all ports in the selection appear in the Port Configuration Area.

For details on the information provided in the Selection List, refer to "Selection List" on page 56.

Using the Port Configuration Area

To configure the VLAN setting for ports on the device using the Port Configuration Area:

1. Select the ports you want to configure in the Tree View, Chassis View, or VLAN Tree. The settings that are common to all of the selected ports appear in the fields in the Port Configuration Area. For information on selecting ports, refer to "Selecting Ports" on page 60.

2. Change the settings in the Port Configuration Area using the pull-down lists and checkboxes. For information on the settings in the Port Configuration Area, refer to "Port Configuration Area" on page 56. The VLAN configuration for the selected ports is changed.

*** Note:** When changing the PVID of the selected ports, the ports do not appear selected in the VLAN Tree. However, the ports remain in the Selection List.

Drag-and-Drop

To configure the PVID of ports using drag-and-drop:

1. Select the ports you want to configure in the Tree View, Chassis View, or VLAN Tree. For information on selecting ports, refer to "Selecting Ports" on page 60.

2. Drag the ports until they are over a VLAN icon in the VLAN Tree. The ports are added to the desired VLAN.

*** Note:** When dragging ports from the VLAN Tree, only ports represented by PVID symbols are added to the desired VLAN. Dragged static binding icons are ignored and do not change port PVIDs.

Updating the Device

Ports whose VLAN information has changed appear dimmed in the VLANs table. To update the device with the changes, click **Apply**.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 15.

7 Port Mirroring

This chapter provides the information and instructions for using the Port Mirroring feature. It includes the following topics:

- **Port Mirroring Overview** - An overview of port mirroring.
- **Viewing the Port Mirroring Table** - Instructions on accessing the Port Mirroring Table and a description of the Port Mirroring Table.
- **Creating Port Mirroring Pairs** - Instructions on creating Port Mirroring pairs
- **The Port Mirroring Wizard** - Detailed descriptions of the screens in the Port Mirroring Wizard.
- **Deleting Port Mirroring Pairs** - Instructions on deleting Port Mirroring pairs.

Port Mirroring Overview

Port Mirroring copies all received and transmitted packets (including local traffic) from a source port to a predefined destination port, in addition to the normal destination port of the packets. This is a useful method for monitoring all traffic traveling through a specific port.

For more information on Port Mirroring, refer to *Port Mirroring* in *The Reference Guide*.

CAUTION

Do not change the VLAN of the source or destination port while the port mirroring mechanism is operating.

Viewing the Port Mirroring Table

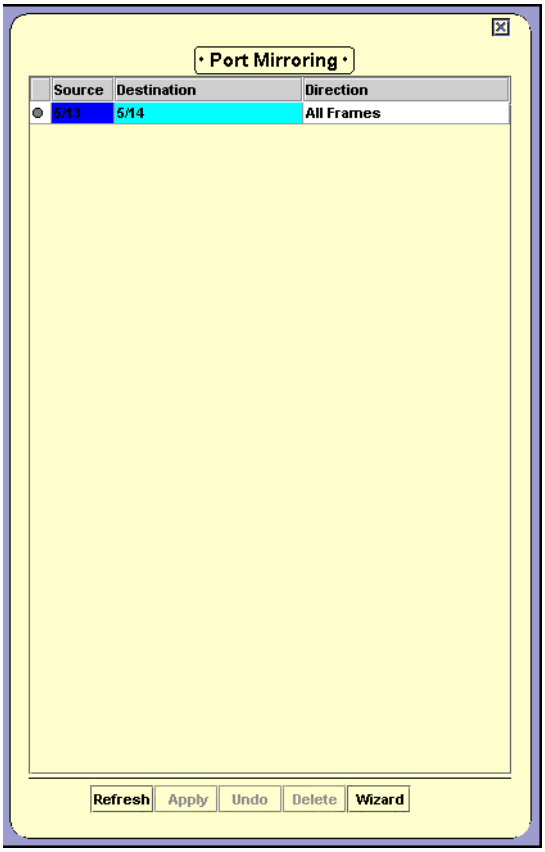
To view the Port Mirroring Table:

Click  .

Or

Select **Actions > Port Mirroring**. The Port Mirroring table opens.

Figure 7-1. Port Mirroring Table



Each row of the Port Mirroring table represents a Port Mirroring pair and provides the following information:

- **Source** - The port or group of ports from which packets are copied.
- **Destination** - The port to which the packets are copied.
- **Direction** - The direction in which packets are being monitored.

When a Port Mirroring pair is selected, the ports appear highlighted in the Chassis and Tree View

Creating Port Mirroring Pairs

To create a new Port Mirroring pair, click Wizard. The Port Mirroring Wizard starts.

Editing Port Mirroring Pairs

To edit an existing Port Mirroring pair:

1. Select a pair by clicking on the row representing the Port Mirroring pair.
2. Click Wizard. The Port Mirroring Wizard starts.

When editing a Port Mirroring Pairs, the dialog boxes display the current Port Mirroring configuration parameters. To keep the values currently displayed in one of the dialog boxes, click **Next**. If you have changed some of the Port Mirroring parameters, and you want to keep the rest of the Port Mirroring configuration, click **Finish**. The device is updated with the new Port Mirroring configuration.

The Port Mirroring Wizard

This section provides detailed information on each of the Port Mirroring Wizard's screens. To continue to the next screen, click **Next**. To return to an earlier screen, click **Back**. To exit the Port Mirroring Wizard without making any changes, click **Cancel**.

The Port Mirroring Wizard consists of the following screens:

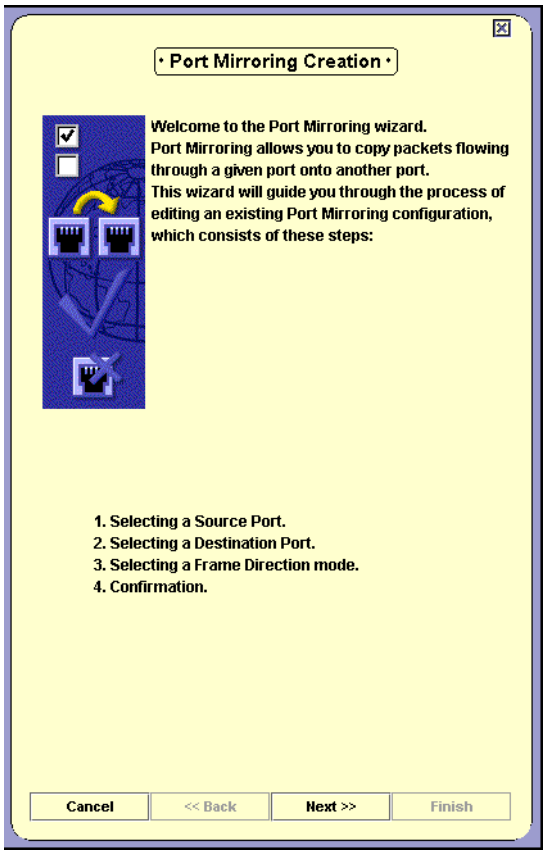
- Welcome Screen
- Source Port Selection Screen
- Destination Port Selection Screen
- Frames Direction Selection Screen
- Confirmation Screen

When you have finished selecting the traffic to be copied, click Next. The Port Mirroring Wizard continues with the When you have finished selecting the traffic to be copied, click Next. The Port Mirroring Wizard continues with the screen.Confirmation Screen screen.Confirmation Screen

Welcome Screen

The Port Mirroring Wizard provides a simple, step-by-step method for defining a Port Mirroring pair.

Figure 7-2. Port Mirroring Wizard - Welcome

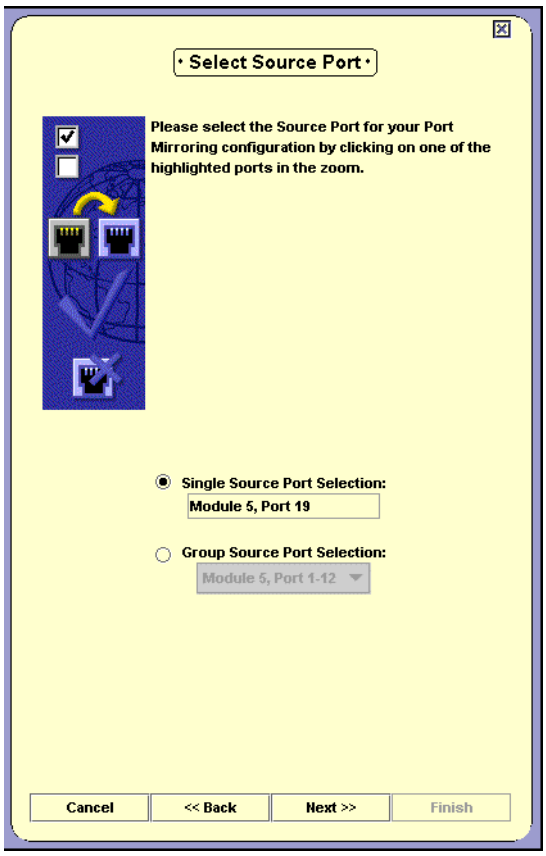


To continue, click **Next**. The Port Mirroring Wizard continues with the **Source Port Selection Screen** screen.

Source Port Selection Screen

The Source Port Selection screen of the Port Mirroring Wizard helps you select a source port for the Port Mirroring pair. Ports which can be selected as sources appear in white in the Chassis View.

Figure 7-3. Port Mirroring Wizard - Source Port Selection Screen



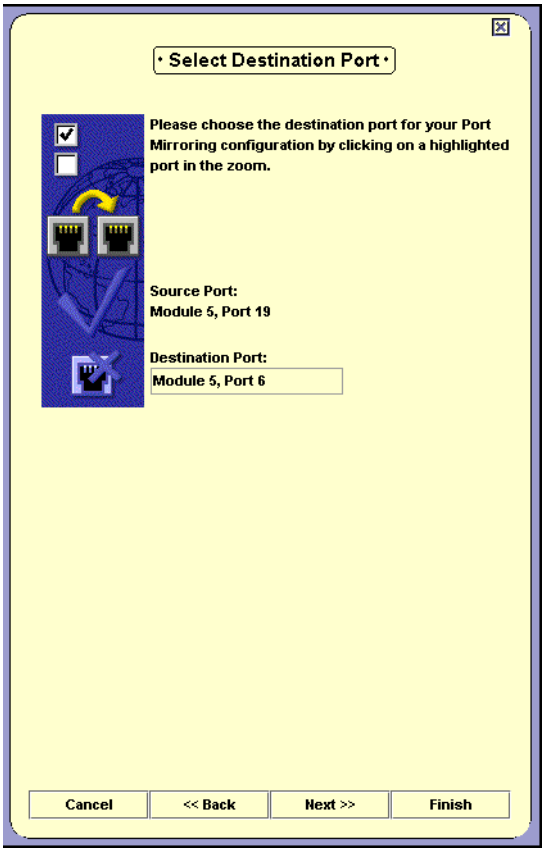
To select a source for the Port Mirroring pair, select either a highlighted port in the Chassis View or a group of ports from the Group Source Port Selection pull-down list. The selected port or group appears blue in the Chassis View and Tree View.

When you have selected the source for the Port Mirroring, click **Next**. The Port Mirroring Wizard continues with the **Destination Port Selection Screen** screen.

Destination Port Selection Screen

The Destination Port Selection screen of the Port Mirroring Wizard helps you select a destination port or LAG for the Port Mirroring pair. Ports and LAGs which can be selected as destinations appear white in the Chassis View.

Figure 7-4. Port Mirroring Wizard - Destination Port Selection Screen



To select a destination for the Port Mirroring pair, select a port in the Chassis View. The selected port appears cyan in the Chassis View and Tree View and is listed in the Destination Port field in the wizard.

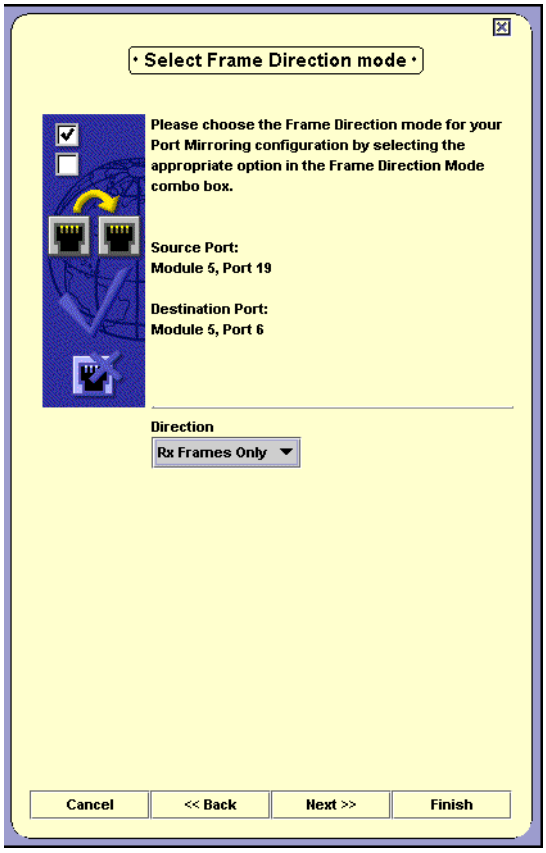
When you have finished selecting the destination for the Port Mirroring pair, click **Next**. The Port Mirroring Wizard continues with the **Frames Direction Selection Screen** screen.

Frames Direction Selection Screen

The Frames Direction Selection screen of the Port Mirroring Wizard enables you to select the traffic to be copied to the destination port. You can configure the destination port to receive all traffic going through the source port, or only the traffic received by the source port.

If you selected a group of ports for the source port, the destination port can receive only the traffic received by the source port.

Figure 7-5. Port Mirroring Wizard - Frames Direction Selection Screen



To configure which frames are copied to the destination port, select an option from the Frames Direction Mode pull-down list box. Possible options are:

- **All Frames** - All traffic going through the source port is copied to the destination port.
- **Rx Frames** - Traffic received by the source port is copied to the destination port.

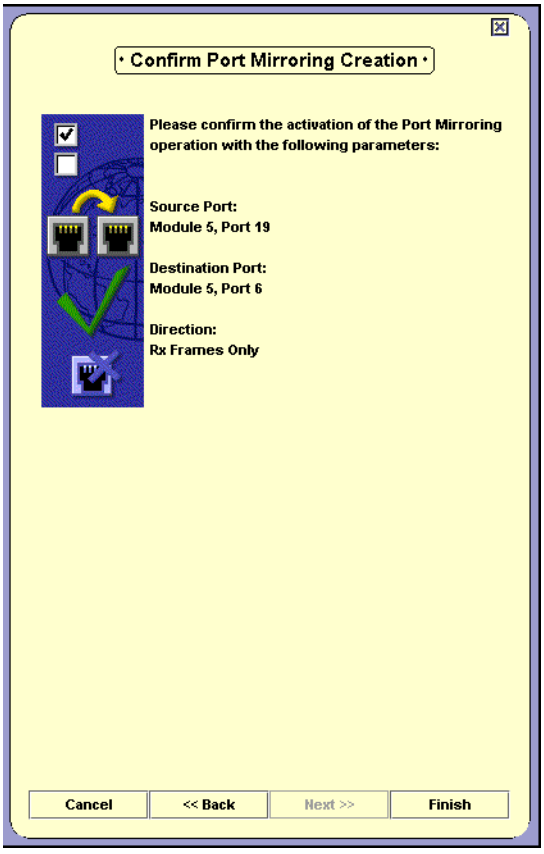
- **Tx Frames** - Traffic transmitted by the source port is copied to the destination port.

When you have finished selecting the traffic to be copied, click **Next**. The Port Mirroring Wizard continues with the **Confirmation Screen** screen.

Confirmation Screen

The Port Mirroring Wizard displays a summary of the Port Mirroring information entered using the previous screens. The Port Mirroring configuration has not yet been uploaded to the device.

Figure 7-6. Port Mirroring Wizard - Confirmation Screen



To make any changes to the summary information:

1. Click **Back** until you reach the screen you want.
2. Change the Port Mirroring parameters.

3. Click **Next** until you reach the Confirmation screen.

To upload the Port Mirroring configuration to the device, click **Finish**. The Port Mirroring configuration is uploaded to the device.

Deleting Port Mirroring Pairs

To delete an existing Port Mirroring pair:

1. Select a Port Mirroring group by clicking on the row in the Port Mirroring Table representing the group.
2. Click Delete.
3. The group is marked with the ✕ symbol.
4. Click Apply to update the device.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 18.

For more information on tables, refer to "Managing Tables" on page 14.

8 Trap Managers Configuration

This chapter provides the information and instructions for configuring trap managers for the Avaya P580/P882 Device. It includes the following topics:

- **Trap Manager Overview** - An overview on Traps and Managers.
- **Viewing the Trap Managers Table** - Instructions on accessing the Trap Managers Table, and a description of the Traps tab in the Trap Managers Table.
- **Configuring Trap Managers** - Instructions on configuring Trap Manager Parameters and their reporting statuses.
- **Editing the Trap Managers Table** - Instructions on how to edit the Trap Managers dialog box.

Trap Manager Overview

In the event of a fault or an unusual occurrence, the Avaya P580/P882 can send traps to one or more Network Management Stations (NMS). To enable this feature, you must configure the Avaya P580/P882 with a list of the managers' workstations. Traps are then sent to the stations listed in the Managers table.

*** Note:** Up to five managers can be assigned per device. However, it is recommended to keep the list limited to actual and relevant managers so as not to place undue stress on the network.

Using the Trap Managers dialog box, you can also configure which traps are sent to the managers. The Traps tab of the Trap Managers dialog box lists specific traps. Checking the checkbox in a trap column enables the managers to receive the checked trap. Managers only receive the traps which are checked.

Viewing the Trap Managers Table

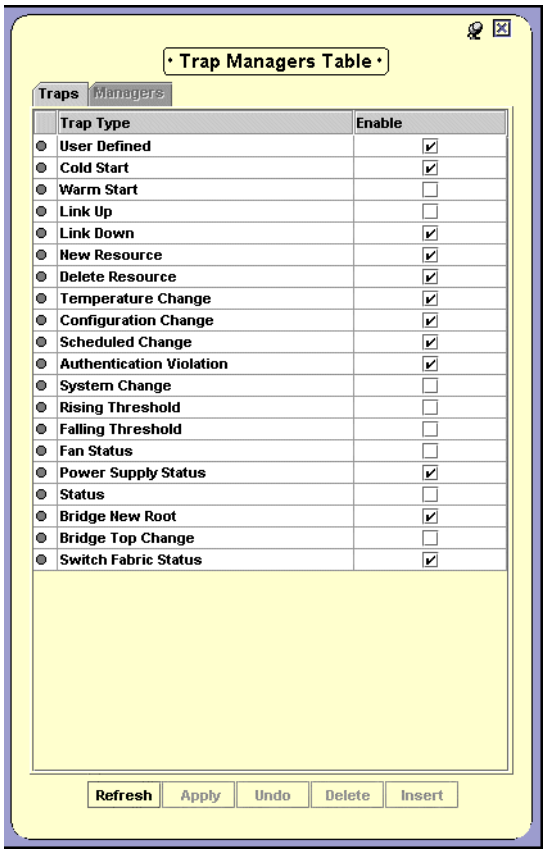
To view the Trap Managers table:

Click  .

Or

Select **Actions > Trap Managers**. The Trap Managers dialog box opens to the Traps tab.

Figure 8-1. Trap Managers Dialog Box - Traps Tab



The Traps tab is used to select the traps you want reported to the designated trap managers.

The following table provides a list of the traps in the Trap table and their descriptions.

Table 8-1. Traps Table Fields

Name	Description
User Defined	A user defined trap.
Cold Start	The device was physically reset.
Warm Start	The device was reset via the CLI, web site, or Device Manager.
Link Up	The link between a port and the device becomes connected.
Link Down	The link between a port and device was disconnected.
New Resource	A system resource was added to the device.
Deleted Resource	A system resource was removed from the device.
Temperature Change	The device temperature status changed. Temperature status changes could precede a switch shutdown and are often critical.
Configuration Change	The device's configuration changed.
Schedule Change	A scheduled task took place.
Authentication Violation	The device detected an authentication failure.
System Change	A system event occurred.
Rising Threshold	The upper threshold for the counter was exceeded.
Falling Threshold	The lower threshold for the counter was passed.
Fan Status	The fan status changed.
Power Supply Status	The power status changed.
Status	A change in a port's status.
Bridge New Root	The bridge topology changed.
Bridge Top Change	The bridge topology changed.

Table 8-1. Traps Table Fields (Continued)

Name	Description
Switch Fabric Status	There was a failure in the switch fabric. These are critical failures and should be monitored closely.

Check the traps you want reported to trap managers. Uncheck the traps you do not want reported to the trap managers.

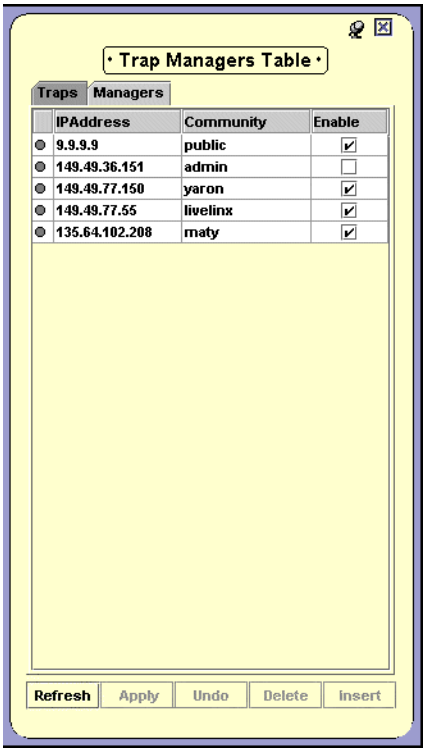
For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 15.

Configuring Trap Managers

*** Note:** The Trap Managers tab is only available if you accessed the device as an administrator. For more information on admission levels, refer to "Admission Level" on page 4

The Trap Managers tab is used to configure the IP addresses and communities of the trap managers and their trap reporting statuses for device wide traps.

Figure 8-2. Trap Managers Dialog Box - Trap Managers Tab



The following table lists the fields in the Trap Managers tab and their descriptions.

Table 8-2. Trap Manager Table Fields

Field	Description
IPAddress	The IP address of the trap manager.
Community	The write community of the trap manager.
Enabled	The state of trap reporting for the trap manager. Possible states are: • **Checked** - The trap manager receives traps from the device. • **Unchecked** - The trap manager does not receive traps from the device.

Editing the Trap Managers Table

You can add and remove managers from the Trap Managers table, and you can edit the trap reporting status of specific managers.

Adding and Removing Managers

To add managers to the table:

1. Click Insert.
2. Enter the IP address and write community of the designated management station.
3. Repeat the procedure for each manager.

To remove managers from the table:

1. Click the row with the manager's IP address.
2. Click Delete.
3. Repeat the procedure for each manager.

Editing Trap Reporting Statuses

To edit the trap reporting status of a manager, check or uncheck the checkbox next to the manager's IP address.

*** Note:** If the checkbox is not checked, no traps will be reported to the selected manager.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 15.

For more information on tables, refer to "Managing Tables" on page 14.

9 Switch Connected Addresses

This chapter provides the information and instructions for viewing stations connected to the device. It includes the following topics:

- **Switch Connected Addresses Overview** - An overview of the Switch Connected Addresses feature.
- **Viewing the Switch Connected Addresses Window** - Instructions on accessing the Switch Connected for Device window, and a description of the Switch Connected for Device window.

Switch Connected Addresses Overview

The Switch Connected Addresses feature allows you to see which devices are connected to the ports on the Avaya P580/P882 Device. Keeping track of this network information can increase efficiency and security, and assist in troubleshooting network problems.

Viewing the Switch Connected Addresses Window

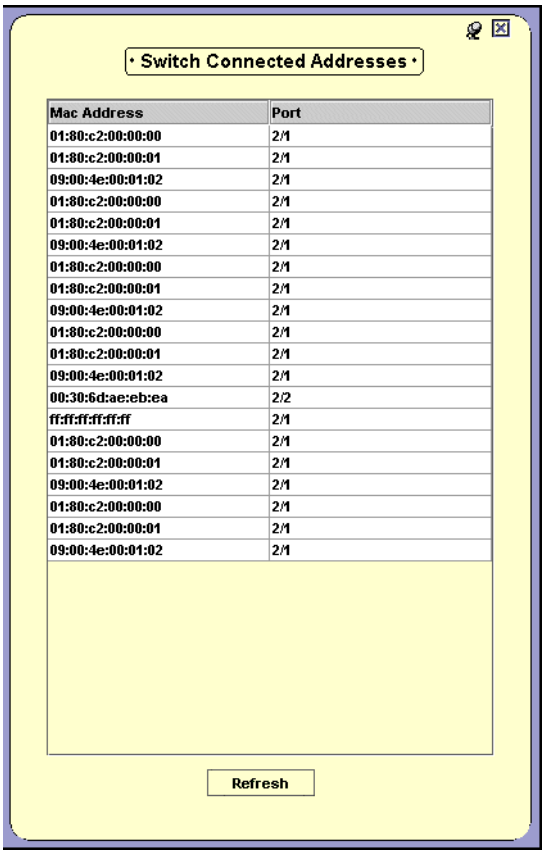
The Switch Connected Addresses window provides a list of MAC addresses along with the ports to which they are attached. To view the list of connected stations:

Click  .

Or

Select **Actions > Switch Connected Addresses**. The Switch Connected Addresses window opens.

Figure 9-1. Switch Connected Addresses Window



All the connections to the Avaya P580/P882 are listed with their respective ports in the Switch Connected Addresses window. The rows of the Switch Connected Addresses window comprise the following information:

- **Mac Address** - The MAC addresses of the stations connected to the switch.
- **Port** - The number of the module and port in the switch.

Sorting the List of Stations

To sort the list of stations, click on a column heading to sort by that column. To change the order of the sort (e.g. from ascending to descending), click again on the column heading of the field by which the list is sorted.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 15.

10 Port Security

This chapter provides the information and instructions you need to use the Port Security feature. It includes the following topics:

- **Overview of Port Security** - An overview of port security.
- **Viewing the Port Security Window** - Instructions on accessing the Port Security window, and a description of the Port Security window.
- **Configuring Port Security** - Instructions on configuring port security.
- **Updating the Device** - Instructions on updating the device with Port Security changes.

Overview of Port Security

Port Security enables you to prevent unlearned devices from sending information through selected ports. Avaya P580/P882 ports maintain a list of the MAC addresses of devices that are linked to them. This list is called the Content Address Memory (CAM). Before enabling security on a port, allow the port to learn the MAC addresses of the devices which you want to use the port. Once Port Security is enabled on the port, it rejects all traffic from devices not listed in the CAM.

Viewing the Port Security Window

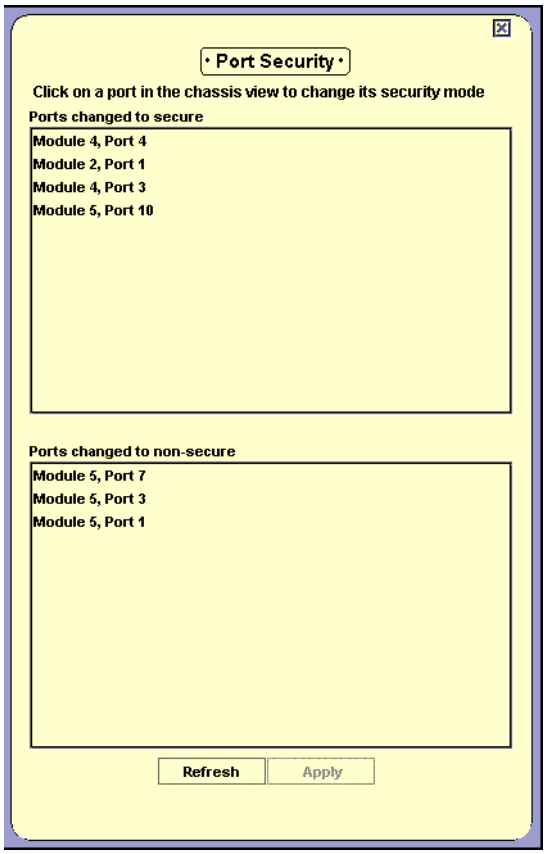
To view the Port Security window:

Click  .

Or

Select **Actions > Port Security**. The Port Security window opens.

Figure 10-1. Port Security Window



The Port Security window shows the state of Port Security on the device. In the Tree View and Chassis View, ports which are configured with Port Security appear with the security symbol.

Configuring Port Security

To toggle the state of port security activation on a port, click the port's symbol in the Tree View or Chassis View.

- If port security was not active on the port, the port is highlighted with the security symbol, and the port's module and port number appear in the Ports changed to secure list.
- If port security was active on the port, the port's security symbol disappears, and the port's module and port number appear in the Ports changed to non-secure from list.

Updating the Device

To update the device with all Port Security changes, click Apply. The device is updated with all of the new information.

To discard all Port Security changes, click Refresh. All Port Security changes are discarded.

For more information on the user interface, refer to "Using Dialog Boxes and Tables" on page 15.

11 Routing Manager

This chapter provides an introduction to the Avaya P580/P882 Routing Manager. It includes the following sections:

- **The User Interface** - An introduction to the Avaya P580/P882 Routing Manager user interface.
- **Modifying Tables** - Instructions on how to add, delete, and modify rows in Avaya P580/P882 Routing Manager tables.
- **Using Avaya P580/P882 Routing Manager Help** - An explanation of the options for accessing on-line help in the Avaya P580/P882 Routing Manager.

The User Interface

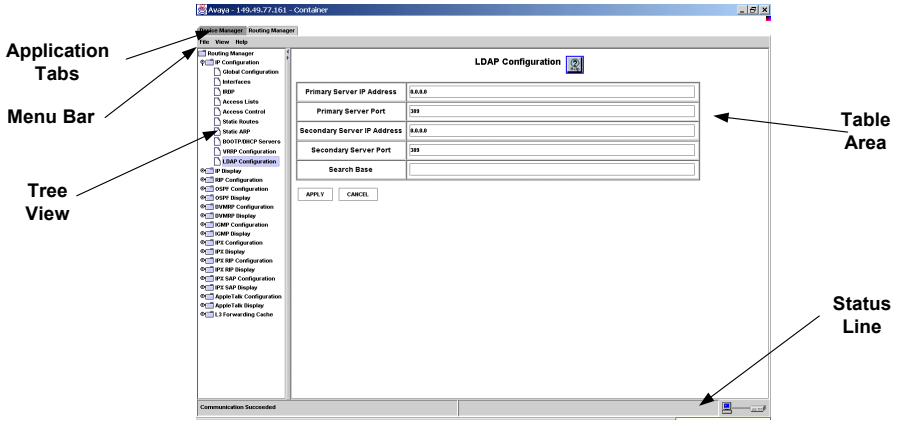
The user interface consists of the following elements:

- **Menu Bar** - Menus for accessing Avaya P580/P882 Routing Manager options. For more information on menus, refer to Appendix A, Menus.
- **Tree View** - A resizeable window containing the functions and configuration windows of Avaya P580/P882 Routing Manager.
- **Table Area** - A resizeable window where all tables are displayed.

For information on other parts of the user interface, refer to “The User Interface” on page 6.

The figure below shows the user interface, with its various parts labeled.

Figure 11-1. The Avaya P580/P882 Routing Manager User Interface



To resize the main areas of the user interface, the Tree View and the Table Area, use the splitter bar and its arrows.

Tree View

The Tree View shows the Routing Manager functions and the applicable configuration windows for each item in the folder.

The highest level of the Tree View shows the routing function. Each function contains a number of folders. The folders show the configuration windows applicable to the modules.

To expand the view of a contracted element in the tree or to contract the view of an expanded element in the tree:

Double-click the element.

Or

Click the handle next to the element you want to expand or contract.

Table Area

The right side of the application window is the Table Area. This area can be resized by dragging the vertical splitter bar with the mouse. All tables and forms appear in the Table Area. Table columns can be resized by dragging the dividers in the table header.

Modifying Tables

Avaya P580/P882 Routing Manager enables you to modify the information in many of its tables. This section provides information on how to add, modify, and delete rows in Avaya P580/P882 Routing Manager tables.

Adding Table Rows

You can add rows to some tables in Avaya P580/P882 Routing Manager by creating a new entity of the type that is described in the table. For example, to add a row to one of the Interfaces tables, create a new interface.

To add a table row:

1. Click **CREATE** at the bottom of the table. A dialog box opens in the Table Area.
2. Enter the requested information in the dialog box. The fields in the dialog box are the same as those in the table.
3. Click **CREATE** at the bottom of the dialog box. The entity is created, and a new row appears in the table.

Modifying Table Rows

You can modify the rows in some tables in Avaya P580/P882 Routing Manager. To modify a table row:

1. Check the Select checkbox in the row you want to modify.

*** Note:** Some tables do not have a Select checkbox.

2. Modify the parameters in the row.
3. Click **APPLY** at the bottom of the table. The row is modified.

Deleting Table Rows

You can delete rows in some tables in Avaya P580/P882 Routing Manager. To delete a table row:

1. Check the Select checkbox in the row you want to modify.
2. Click **DELETE** at the bottom of the table. The row is deleted.

Using Avaya P580/P882 Routing Manager Help

This section explains how to use the on-line help in the Avaya P580/P882 Routing Manager.

Opening the Help to the Contents Page

To open the help to the contents page, select **Help > Content**. The on-line help opens to the contents page.

Use the Table of Contents, Index, or Search tabs to find information.

Opening the Help to a Topic of Interest

To open the help directly to a topic of interest, click **Help**. The on-line help opens to a topic explaining the option currently selected in the Tree View.

12 IP Routing

This chapter provides instructions for all IP routing functions using the Avaya P580/P882 Manager. It includes the following sections:

IP Configuration

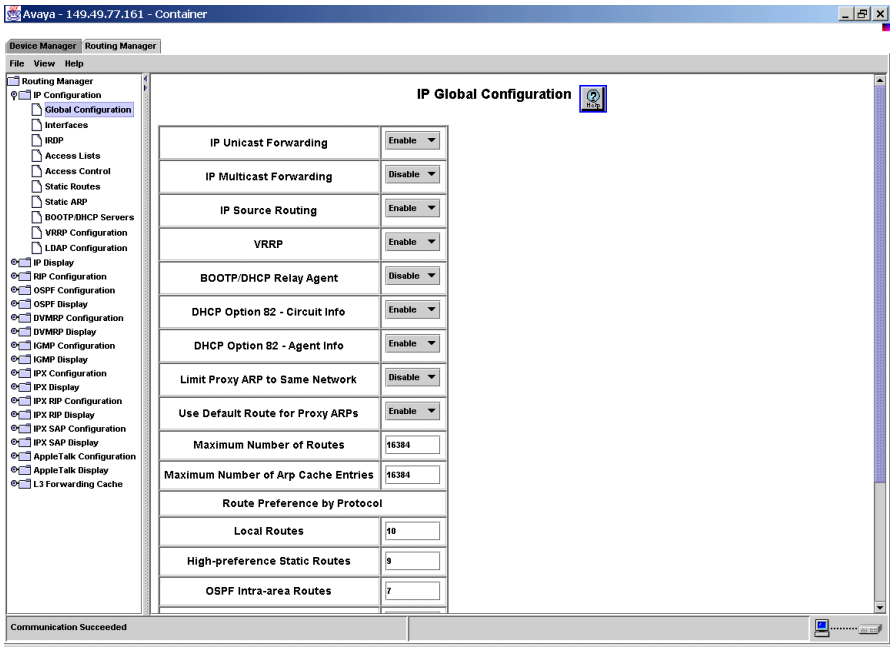
The IP Configuration folder provides access to the following windows:

- **Global Configuration**
- **Interfaces**
- **IRDP**
- **Access Lists**
- **Access Control**
- **Static Routes**
- **Static ARP**
- **BOOTP/DHCP Servers**
- **VRRP Configuration**
- **LDAP Configuration**

Global Configuration

To display and update the IP global configuration, select **IP Configuration > Global Configuration**. The IP Global Configuration window opens.

Figure 12-1. IP Global Configuration Window



The following parameters are displayed:

Table 12-1. Global Configuration Parameters

Field	Description
IP Unicast Forwarding	Determines how unicast packets are treated. Possible values are: • **Enable** - Unicast packets are forwarded. • **Disable** - Unicast packets are not forwarded.
IP Multicast Forwarding	Determines the status of IP multicasting. This affects all IP RIP interfaces set up to use multicast protocols. • **Enable** • **Disable**

Table 12-1. Global Configuration Parameters (Continued)

IP Source Routing	The state of global strict and loose source routing. Possible values are: • **Enable** • **Disable**
VRRP	The state of VRRP. Possible values are: • **Enable** • **Disable**
BOOTP/DHCP Relay Agent	Accepts client requests for an IP address and forwards them to a server. This agent also relays responses from the server to the client.
DHCP Option 82 - Circuit Info	The slot and physical port number from which the DHCP request was received.
DHCP Option 82 - Agent Info	The IP address and, if available, the system name of the switch.
Limit Proxy ARP to Same Network	Determines the router's response to ARP requests. Possible values are: • **Enable** - The router responds to ARP requests if the source and destination IP address are in the same network, but different subnets. • **Disable** - The router only responds to ARP requests if the source and destination address are in different networks.
Use Default Route for PRoxy ARPs	Determines the usage of the default route for Proxy ARPs. For example, if you have a default route configured to reach the 0.0.0.0 IP address, then any ARP request that does not match any of the other routes in your IP routing table will automatically go to this default route. • **Enable** • **Disable**
Maximum Number of Routes	The maximum number of routes that can be added to the routing table. The default maximum number of routes is 16384. *** Note:** These routes refer only to IP Unicast entries.

Table 12-1. Global Configuration Parameters (Continued)

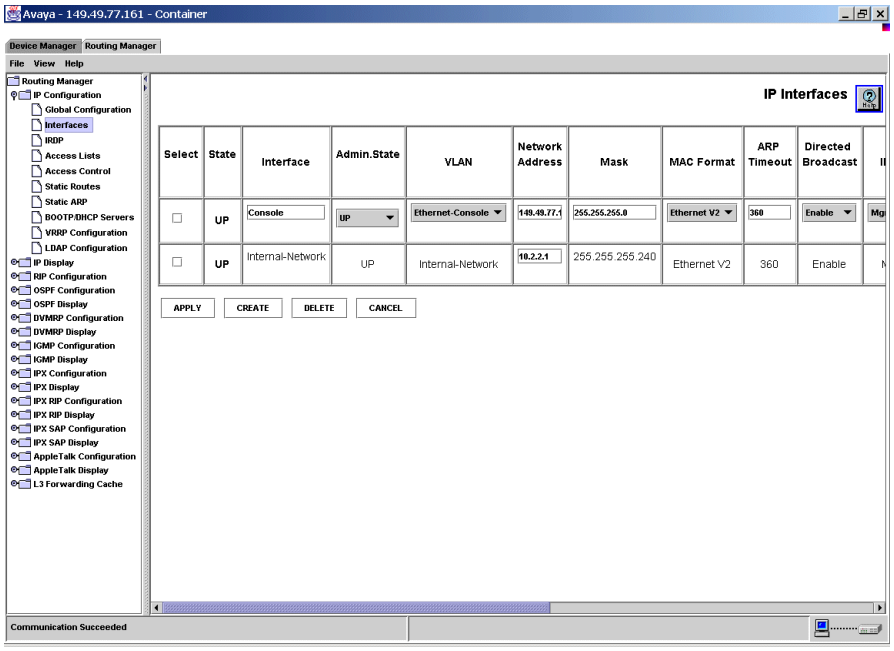
Maximum Number of ARP Cache Entries	The maximum number of ARP cache entries. This refers to the space available in the IP address table. A large number of entries will cause the table to be relearned more frequently and make address space usage more efficient. The default maximum number of entries is 16384.
Local Routes	A preference value for local routes.
High-preference Static Routes	A preference value for high-level static routes.
OSPF Intra-area Routes	Determines the OSPF intra-area route. A lower number indicates a lower preference for the path.
OSPF Inter-area Routes	Specify inter-area paths to destinations in other OSPF areas. These are discovered through the examination of received summary Link State Advertisements (LSA). Enter a number to specify your path cost. A lower number indicates a lower preference for the path.
OSPF External Routes	Specify Autonomous System (AS) external paths to destinations external to the AS. Enter a number to specify your path cost (preference). A lower number indicates a lower preference for the path.
RIP Routes	Specify RIP to use the hop count as a metric. Hence, to specify a preference for a RIP route, you need to enter a lower number (path cost).
Low-preference Static Routes	Determine a preference value for low-level static routes.

You can modify the IP Global Configuration parameters. For information, refer to "Modifying Tables" on page 85.

Interfaces

To display and update IP interfaces, select **IP Configuration > IP Interfaces**. The IP Interfaces window opens.

Figure 12-2. IP Interfaces WIndow



The following parameters are displayed:

Table 12-2. IP Interfaces Parameters

Field	Description
Select	Select the interface to be configured.
State	The state of the interface. Possible states are: • **Up** • **Down**
Interface	The name assigned to the selected IP interface.
Admin State	Determine the administrative state of the interface. Possible values are: • **UP** - The interface is active. • **DOWN** - The interface is inactive.

Table 12-2. IP Interfaces Parameters (Continued)

Field	Description
VLAN	Determine the type of VLAN. Possible values are: • **Default** - Selects the default VLAN. • **Discard** - Discards the selected VLAN. • **Ethernet-Console** - Selects the Ethernet Console port as the VLAN. • **Serial Console** - Selects the Serial Console port as the VLAN. *** Note:** The way you configure a VLAN to a port determines the IP Routing option that you select for the interface. Use the following options to configure the appropriate interface: • **Mgmt Only** - Create an IP interface for an Ethernet-Console VLAN. • **Mgmt Only** - Create an IP interface for a serial-console VLAN. • **Routing Mgmt** - Create an IP interface for an inbound VLAN.
Network Address	The network IP address for the selected interface.
Mask	The subnet mask for the interface.
MAC Format	Enter the MAC address format for the interface. Possible values are: • **Ethernet V2x** • **SNAP** (Simple Network Access Protocol)

Table 12-2. IP Interfaces Parameters (Continued)

Field	Description
IP Routing	The state of IP routing on the interface. Possible values include: • **Routing/Mgmt** - Enables you to manage the switch, from the Command Line Interface (CLI) or the Web Agent, and configure IP routing for the switch. • **Mgmt Only** - Enables you to manage the switch, however, IP routing is disabled. • **Default** - Enables you to configure IP routing for the switch, however, you cannot manage the switch. *** Note:** When the interface has a VLAN identified as Serial-Console, the only valid IP routing option is Mgmt Only.
RIP	The of RIP on a given interface. Possible values are: • **Enable** - RIP is enabled. • **Disable** - RIP is disabled. This is the default value.
OSPF	The state of OSPF on a given interface. Possible values are: • **Enable** - OSPF is enabled. • **Disable** - OSPF is disabled. This is the default value.
Multicast Protocol	Specify the multicast protocol for the interface. Possible values include: • **None** • **DVMRP** • **IGMP**
Proxy ARP	The state of Proxy ARP on a given interface. Possible values are: • **Enable** - Proxy ARP is enabled. • **Disable** - Proxy ARP is disabled. This is the default value.

Table 12-2. IP Interfaces Parameters (Continued)

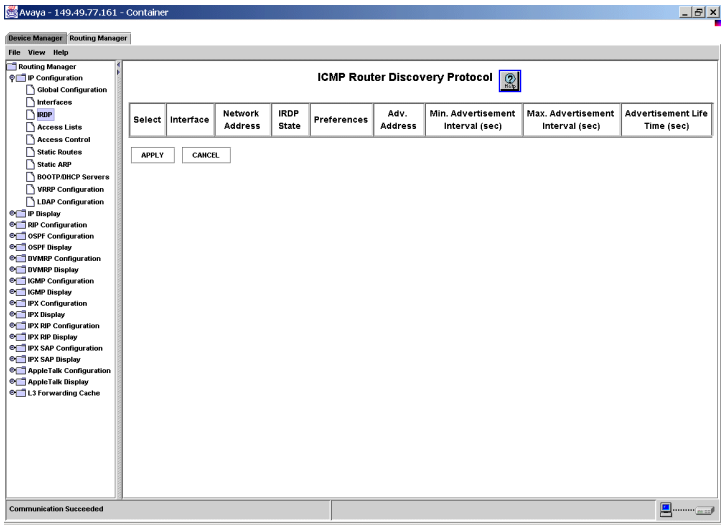
Field	Description
ICMP Redirect	The state of ICMP Redirect on a given interface. Possible values are: • **Enable** - ICMP Redirect is enabled. This is the default value. • **Disable** - ICMP Redirect is disabled.
NetBIOS UDP Rebroadcast	Configure your switch for Inter-VLAN forwarding of NetBIOS broadcasts. NetBIOS parameters include: • **Inbound** - Allow the receipt of NetBIOS replies. • **Outbound** - Allow the transmission of NetBIOS broadcasts. • **Both** - Allow the interface to both receive NetBIOS replies and send NetBIOS broadcasts. • **Disable** - Disallow both the receipt of NetBIOS replies and the transmission of NetBIOS broadcasts.
VRRP	The state of VRRP on a given interface. Possible values are: • **Enable** - VRRP is enabled. • **Disable** - VRRP is disabled. This is the default value.
Boot/DHCP Relay Gateway	The state of Boot/DHCP on a given interface. Possible values are: • **Enable** - Boot/DHCP is enabled. • **Disable** - Boot/DHCP is disabled. This is the default value.

You can add, modify, or delete IP Interfaces. For information, refer to "Modifying Tables" on page 85.

IRDP

To display and update the ICMP Router Discovery Protocol (IRDP) configuration, select **IP Configuration > IRDP**. The ICMP Router Discovery Protocol window opens.

Figure 12-3. ICMP Router Discovery Protocol Window



The following parameters are displayed:

Table 12-3. IRDP Parameters

Field	Description
Select	Select the interface to be configured.
Interface	The name of the interface.
Network Address	The IP address of the interface.
IRDP State	The state of IRDP on the selected interface. Possible values are: • **Enabled** - IRDP is enabled. This is the default. • **Disabled** - IRDP is disabled.
Preferences	The preference of the address as a default router address, relative to other router addresses on the same subnet. The minimum setting (80000000 hex) is used to indicate that the address should not be used by neighboring hosts as a default router address, even though it may be advertised. The default setting is 0.

Table 12-3. IRDP Parameters (Continued)

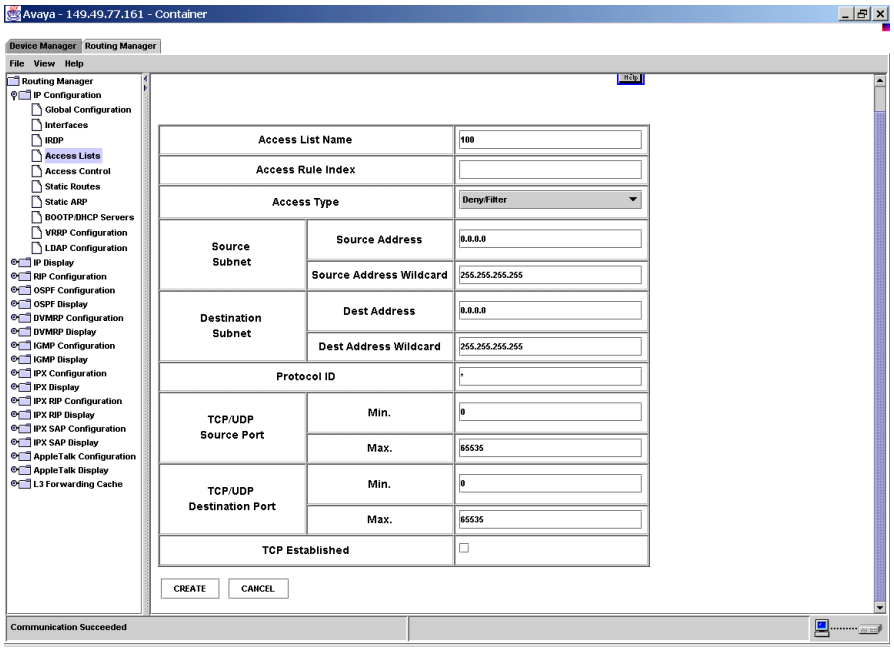
Field	Description
Adv. Address	The IP destination address used for multicast router advertisements sent from the interface. Possible options include: • **Multicast** - Listening hosts support IP multicast. The default setting is 224.0.0.1. • **Broadcast** - Listening hosts support IP unicast. The default setting is 255.255.255.255.
Min. Advertisement Interval (Sec.)	The minimum time, in seconds, that is allowed between sending unsolicited multicast router advertisements from the interface. This setting must be no less than three seconds and no greater than the Max. Advertisement Interval. The default setting is 450 seconds, 0.75 times the maximum interval.
Max. Advertisement Interval (sec.)	The maximum time, in seconds, allowed between sending multicast router advertisements from the interface. This setting must be no less than four seconds and no greater than 1800 seconds. The default setting is 600 seconds.
Advertisement Life Time (sec.)	The time, in seconds, of the life of a router advertisement that is sent from the interface. This setting must be no less than the maximum advertisement interval and no greater than 9000 seconds. The default setting is 1800 seconds, three times the maximum advertisement interval.
Cost	The metric between this router and the destination. *** Note:** The metric you enter overrides routing protocol metrics.

You can modify ICMP Router Discovery parameters. For information, refer to "Modifying Tables" on page 85.

Access Lists

To display and update the IP access lists, select **IP Configuration > Access Lists**. The IP Access List window opens.

Figure 12-4. IP Access List Window



The following parameters are displayed:

Table 12-4. IP Access Lists Parameters

Field	Description
Access List Name	Displays the name and type of the access list for the newly created access rule. Valid name values are 1-99 for standard access rules, and 100-199 for extended access rules.
Index	Displays the sequence number for each new rule you create.

Table 12-4. IP Access Lists Parameters (Continued)

Field	Description
Access Type	Displays the method of handling incoming datagrams based on the IP access type. Possible values are: • **Deny/Filter** - Allows you to filter out traffic based on the specified configuration. • **Permit/Fwd Pri8 (high)** - **Permit/Fwd Pri1 (low)** - Allows you to prioritize traffic based on the specified configuration. • **Permit/Fwd with no change in priority** - Allows you to forward traffic with no change in priority.
Source Address	The IP address of a host or switch that is denied or granted access to the switch.
Source Wildcard	The range of IP addresses of hosts and switches that are denied or granted access to data from the switch. Enter 1's in the bit positions you want ignored.
Dest Address	Displays the IP address of a host or switch that is denied or granted access to the switch.
Dest Wildcard	Displays a range of IP addresses of hosts and switches that are denied or granted access to the switch. Enter 1's in the bit positions you want ignored.
Protocol ID	Displays the protocol ID to be filtered.
TCP/UDP Source Port Min	Displays the minimum source port used to pass between two hosts or switches using the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP) to which this rule applies.
TCP/UDP Source Port Max	Displays the maximum source port used to pass between two hosts or switches using the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP) to which this rule applies.
TCP/UDP Dest Port Min	Displays the minimum destination port used to pass between two hosts or switches using the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP) to which this rule applies.

Table 12-4. IP Access Lists Parameters (Continued)

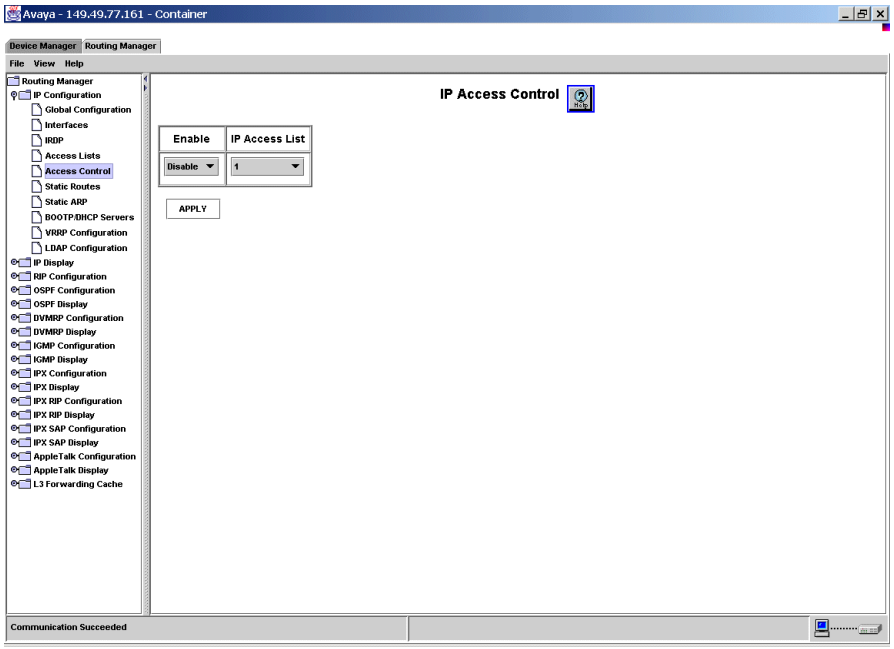
Field	Description
TCP/UDP Dest Port Max	Displays the maximum destination port used to pass between two hosts or switches using the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP) to which this rule applies.
TCP Established	Displays whether the option to run an informational logging message to the console about the packet is enabled or disabled. This option is valid for TCP only.

You can add, modify, or delete IP Access List parameters. For information, refer to "Modifying Tables" on page 85.

Access Control

To select the IP access list to use, select **IP Configuration > Access Control**. The IP Access Control window opens.

Figure 12-5. IP Access Control Window



The following parameter is displayed:

Table 12-5. Access Control Parameters

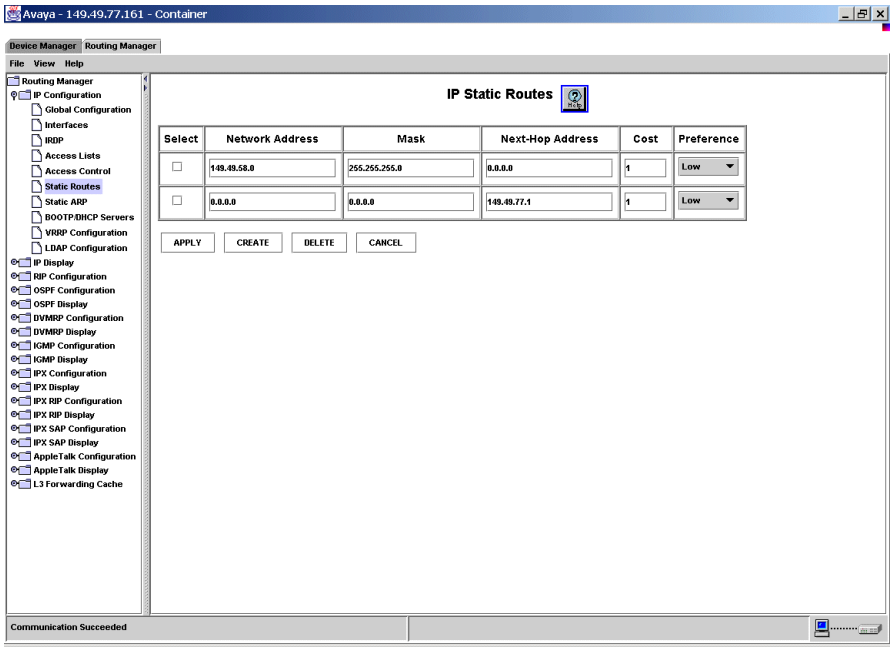
Field	Description
Enable	The state of inbound traffic filtering. Possible values are: • **Enable** • **Disable**
IP Access List	Select the IP access list to be used for filtering if IP Access Control is enabled.

You can modify IP Access Control parameters. For information, refer to "Modifying Tables" on page 85.

Static Routes

To display and update IP static routes, select **IP Configuration > Static Routes**. The IP Static Routes window opens.

Figure 12-6. IP Static Routes Window



The following parameters are displayed:

Table 12-6. Static Routes Parameters

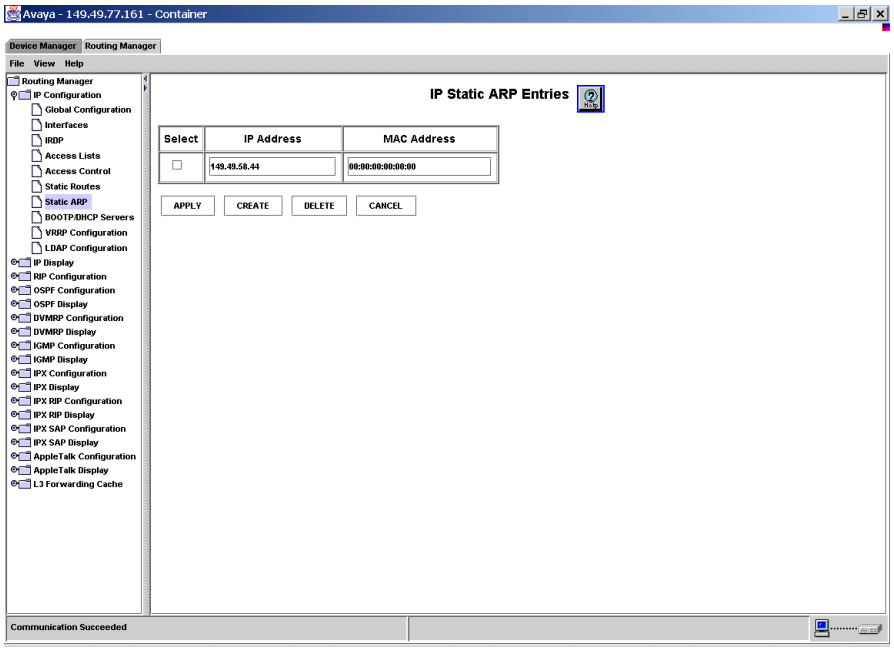
Field	Description
Select	The IP static route to be deleted or modified.
Network Address	The IP address of the static route.
Mask	The subnet mask of the static route.
Next-Hop Address	Displays the IP address of the next destination to which the packet is routed.
Cost	Number of hops to the destination network, or the cost of the route for static routes.
Preference	The routing preference. Possible values are: • **Low** • **High**

You can add, modify, or delete IP Static Routes. For information, refer to "Modifying Tables" on page 85.

Static ARP

To display and update IP static ARP entries, select **IP Configuration > Static ARP**. The IP Static ARP Entries window opens.

Figure 12-7. IP Static ARP Entries Window



The following parameters are displayed:

Table 12-7. IP Static ARP Parameters

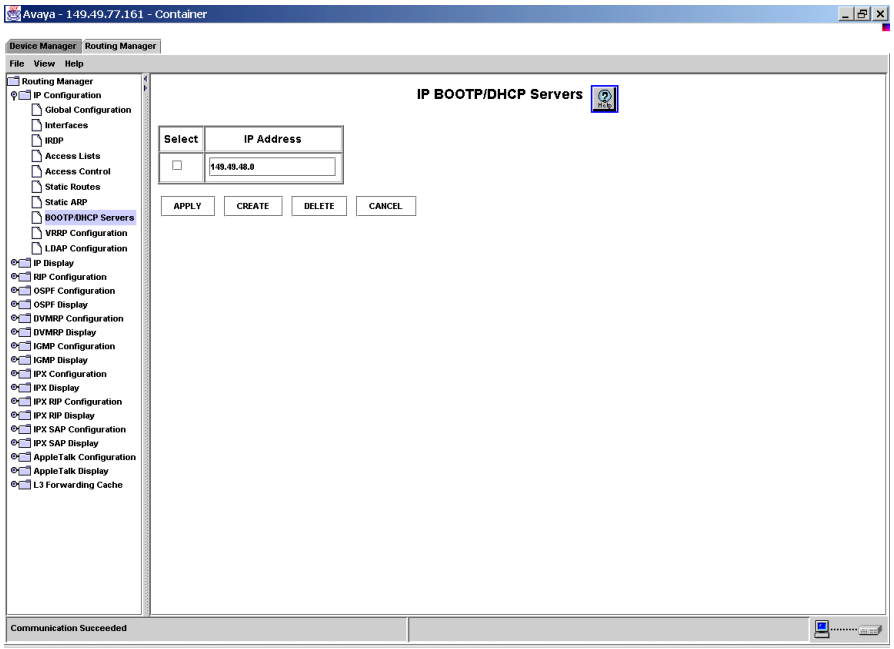
Field	Description
IP Address	The IP address to associate with the static ARP entry.
MAC Address	The MAC address of a node to which you want to create a static ARP entry.

You can add, modify, or delete IP Static ARP Entries. For information, refer to "Modifying Tables" on page 85.

BOOTP/DHCP Servers

To display and update IP BOOTP/DHCP server information, select **IP Configuration > BOOTP/DHCP Servers**. The IP BOOTP/DHCP Servers window opens.

Figure 12-8. IP BOOTP/DHCP Servers Window



The following parameters are displayed:

Table 12-8. IP BOOTP/DHCP Servers Parameter

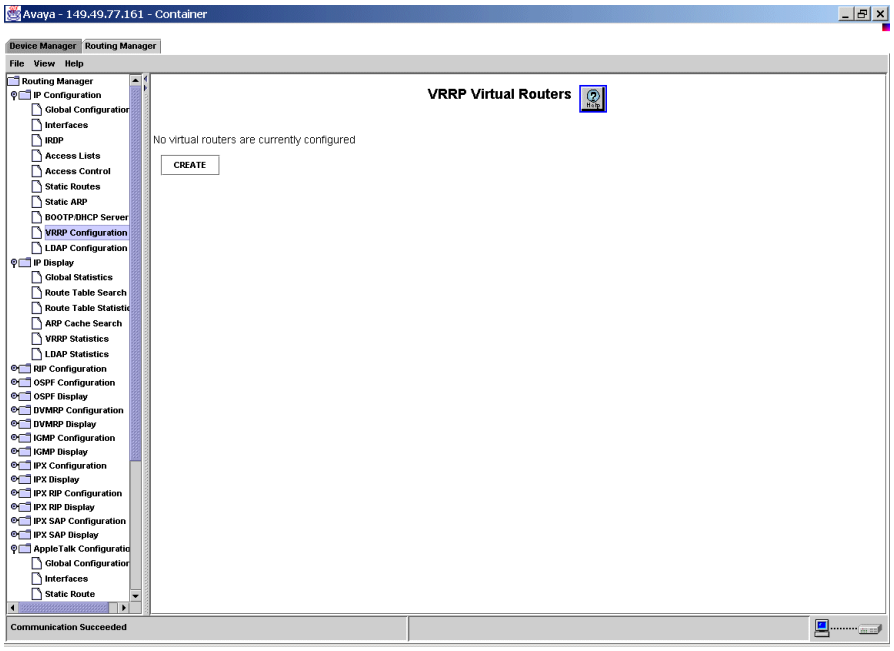
Field	Description
Select	The BOOTP/DHCP server to be deleted or modified.
IP Address	Displays the IP address of the BOOTP/DHCP server.

You can add, modify, or delete IP BOOTP/DHCP Server parameters. For information, refer to "Modifying Tables" on page 85.

VRRP Configuration

To display and update IP VRRP configuration, select **IP Configuration > VRRP Configuration**. The IP VRRP Virtual Routers window opens.

Figure 12-9. VRRP Virtual Routers Window



The following parameter is displayed:

Table 12-9. VRRP Virtual Routers Parameter

Field	Description
Interface	Displays the number associated with the selected interface.
VR ID	Displays the reporting virtual router's identification.
IP Address	Displays the virtual router's IP address. Opens the VRRP Virtual IP Address(es) dialog box for creating new VRRP IP addresses.
Priority	Displays the sending VRRP router's priority.
Advertisement Timer	Displays the number of seconds that a Master virtual router advertises itself.
Auth Key	Enter the VRRP authentication key for the interface. The default is LUCENT.

Table 12-9. VRRP Virtual Routers Parameter (Continued)

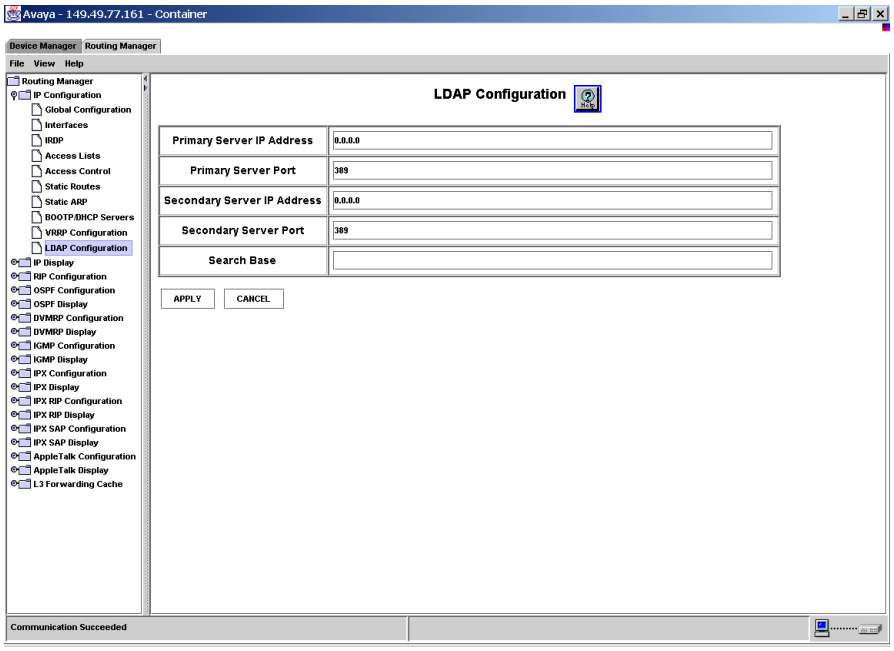
Field	Description
Addr Owner Override	The state of the address owner override. Possible values are: • **Enable** • **Disable**

You can add, modify, or delete VRRP Virtual Routers. For information, refer to "Modifying Tables" on page 85.

LDAP Configuration

To display and update IP LDAP configuration, select **IP Configuration > LDAP Configuration**. The IP LDAP window opens.

Figure 12-10. LDAP Configuration Window



The following parameters are displayed:

Table 12-10. LDAP Configuration Parameters

Field	Description
Primary Server IP Address	The IP address of your primary LDAP server for the access control list domain. This address is used first when connecting to and downloading access lists from an LDAP server. The default value of 0.0.0.0 indicates to the client that there is no primary LDAP server.
Primary Server Port	The port number of the primary LDAP server for the access control list domain. The port number is used in conjunction with the primary server IP address. The default port is 389.

Table 12-10. LDAP Configuration Parameters (Continued)

Field	Description
Secondary Server IP Address	The backup LDAP server's IP address for the access control list domain. This address is used as a backup when connecting to and downloading access lists from an LDAP server. If the LDAP client is unsuccessful in connecting to or downloading access lists from the primary server, the secondary server IP address is used. If the primary server IP address has a value of 0.0.0.0, the secondary server IP address is used. The default value is 0.0.0.0. *** Note:** Setting the IP address of the secondary server to 0.0.0.0 indicates to the LDAP client that there is no secondary server.
Secondary Server Port	The backup LDAP server IP address for the access control list domain. This address is used as a backup when connecting to and downloading access lists from an LDAP server. If the LDAP client is unsuccessful in connecting to or downloading access lists from the primary server, the secondary server IP address is used.
Search Base	Enter the search criteria that will be sent to the LDAP server. The default value is "**ou=Devices, ou=AvayaRules, o=Lucent**".

You can modify LDAP Configuration parameters. For information, refer to "Modifying Tables" on page 85.

IP Display

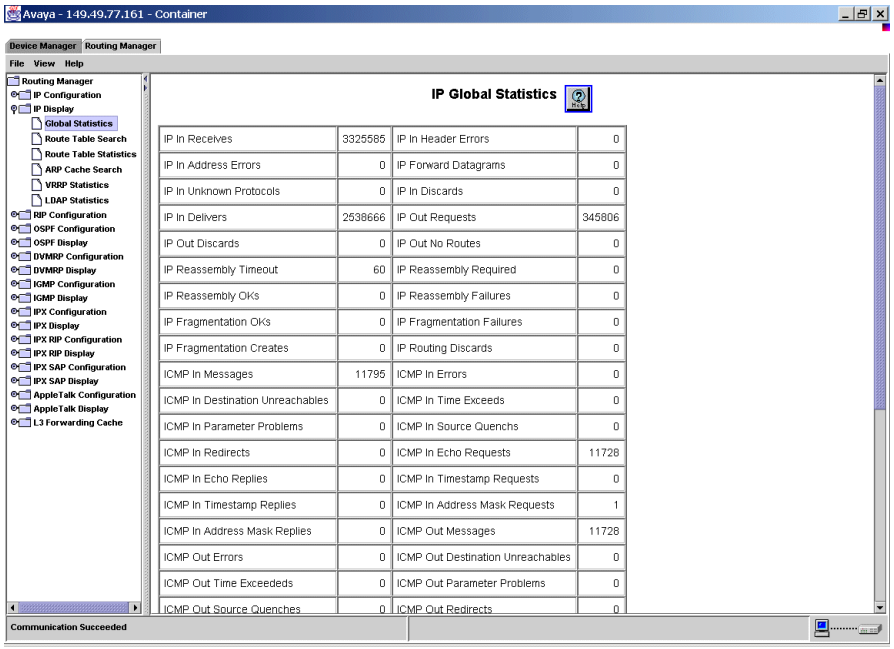
The IP Display folder provides access to the following windows:

- **Global Statistics**
- **Route Table Search**
- **Route Table Statistics**
- **ARP Cache Search**
- **VRRP Statistics**
- **LDAP Statistics**

Global Statistics

To display IP global statistics, select **IP Display > Global Statistics**. The IP Global Statistics window opens.

Figure 12-11. IP Global Statistics Window



The following statistics are displayed:

Table 12-11. IP Global Statistics Parameters

Field	Description
IP In Receives	The number of IP packets received.
IP In Header Errors	The number of IP packets received with header errors.
IP In Address Errors	The number of IP packets received with address errors.
IP Forward Datagrams	The number of IP datagrams received

You can refresh or clear the statistics available in the IP Global Statistics windows.

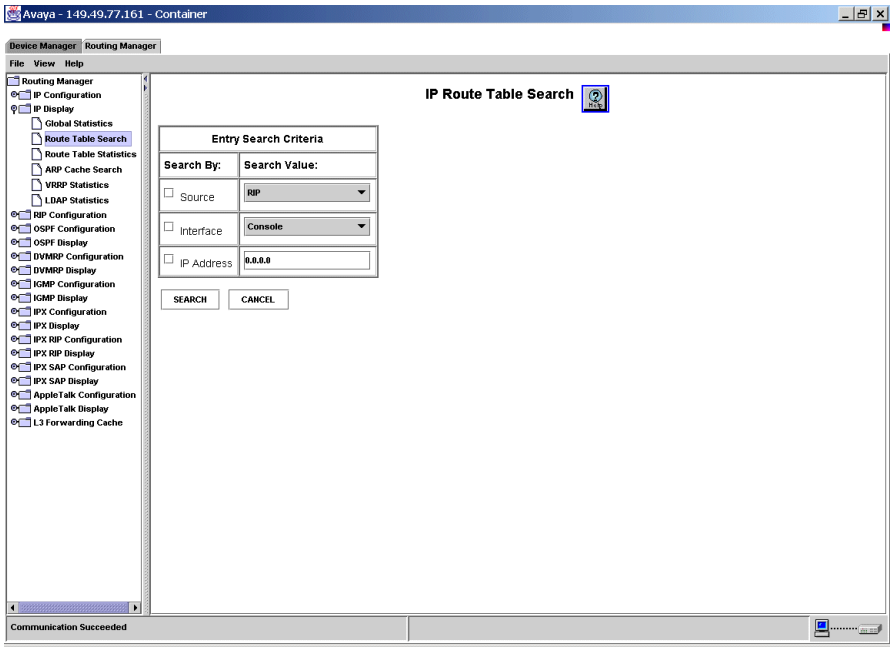
To refresh the statistics, click **REFRESH**. The statistics are refreshed.

To clear the statistics, click **CLEAR**. The statistics are cleared.

Route Table Search

To display and configure IP route table search criteria, select **IP Display > Route Table Search**. The IP Route Table Search window opens.

Figure 12-12. IP Route Table Search Window



The following parameters are displayed:

Table 12-12. IP Route Table Search Parameters

Field	Description
Source	Search your IP routing table using one of the following parameters: • **RIP** • **OSPFStatic** • **Local**
Interface	Perform a search using the interface you selected. The system default entries are: • **Default** • **Discard** • **Ethernet Console** • **Configured Interface**
IP Address	Search according to a specific IP address.

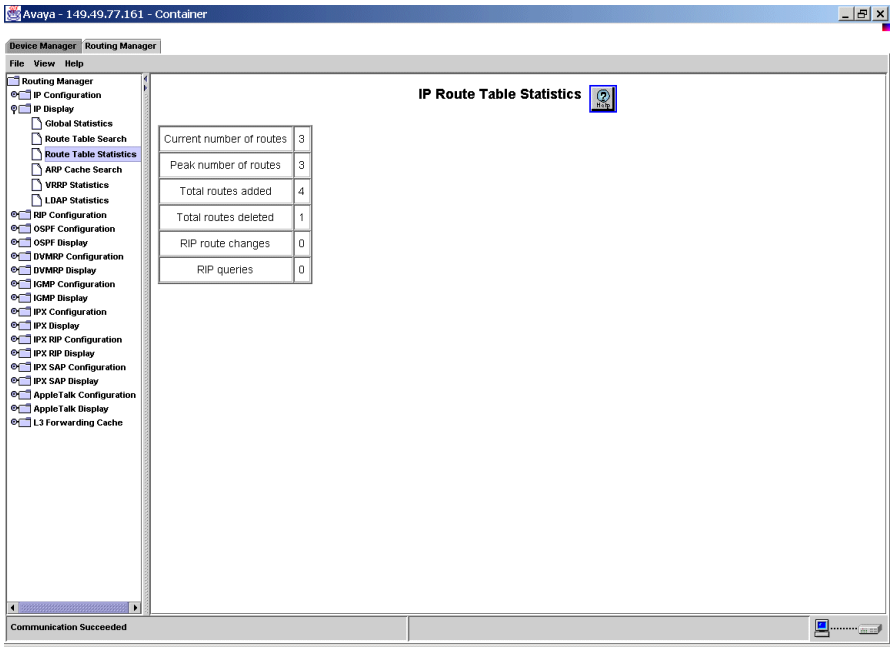
To search the routing table:

1. Enter the criteria by which you want to search.
2. Ensure that the Search by checkbox next to the criteria is checked.
3. Click **SEARCH**. A window opens in the Table Area with the results of the search.

Route Table Statistics

To display IP route table statistics, select **IP Display > Route Table Statistics**. The IP Route Table Statistics window opens.

Figure 12-13. IP Route Table Statistics Window



The following parameters are displayed:

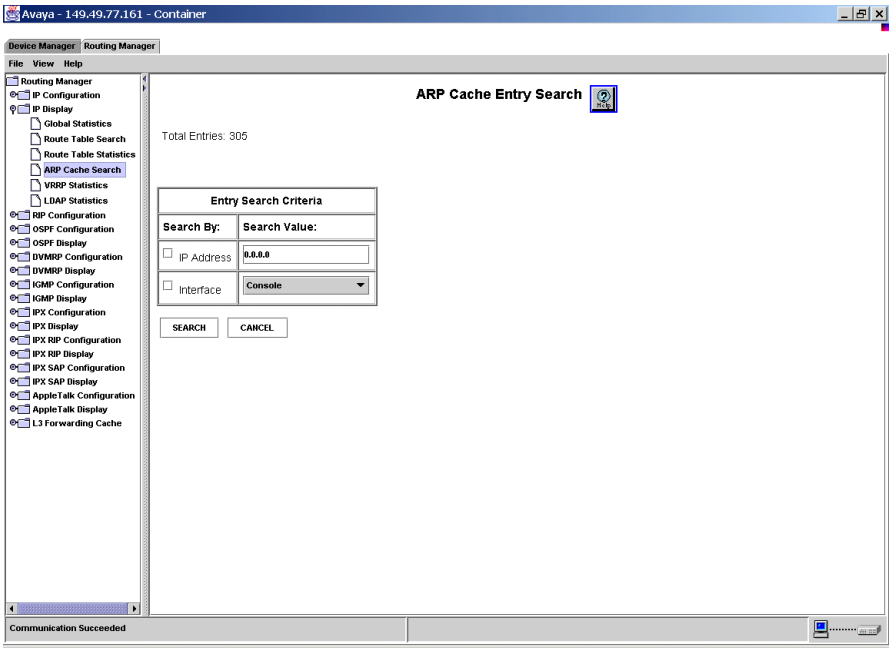
Table 12-13. Route Table Statistics Parameters

Field	Description
Current Number of routes	Displays the total number of active routes.
Peak number of routes	Displays the peak number of routes.
Total routes added	Displays the total number of routes added.
Total routes deleted	Displays the total number of routes deleted.
RIP route changes	Displays the number of changes to the route database made by RIP.
RIP queries	Displays the number of RIP queries sent to the network.

ARP Cache Search

To display and configure ARP cache entry search criteria, select **IP Display > ARP Cache Search**. The ARP Cache Entry Search window opens.

Figure 12-14. ARP Cache Entry Search Window



The following parameters are displayed:

Table 12-14. ARP Cache Entry Search Parameters

Field	Description
IP Address	Provide a specific IP address.
Interface	The selected interface. System entries include all interfaces that you previously configured.

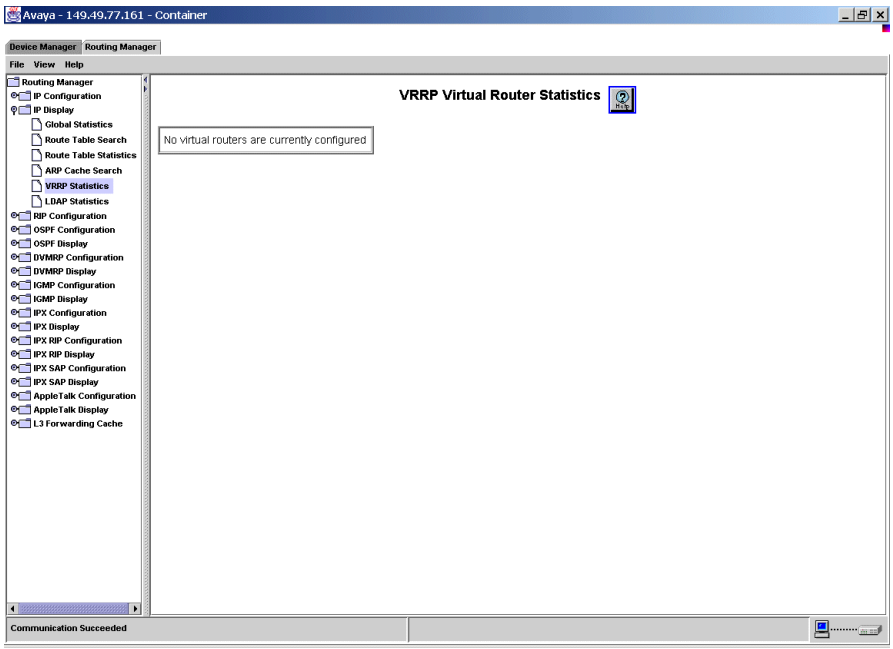
To search the ARP cache:

1. Enter the criteria by which you want to search.
2. Ensure that the Search by checkbox next to the criteria is checked.
3. Click **SEARCH**. A window opens in the Table Area with the results of the search.

VRRP Statistics

To display VRRP statistics, select **IP Display > VRRP Statistics**. The VRRP Virtual Router Statistics window opens.

Figure 12-15. VRRP Virtual Router Statistics Window



The following parameters are displayed:

Table 12-15. VRRP Statistics Parameters

Field	Description
Interface	The IP interface name corresponding to the selected VRRP virtual router.
VR - ID	Displays the virtual router's identification. The ID range is between 1through 255 (decimal).
IP Address	The IP address that corresponds with the selected VRRP virtual router.

Table 12-15. VRRP Statistics Parameters (Continued)

Field	Description
State	The state of the virtual router.Possible values include: • **Inactive** - Disables the VRRP virtual router. • **Initialize** - Initializes the VRRP Virtual Router. • **Backup** - Defines the VRRP Virtual Router as a backup router to the master. • **Master** - The VRRP Virtual Router functions as the forwarding router.
Time of State Change	The last state of transition. This value is in an HH:MM:SS format.
Times this VR Became Master	The number of instances that the virtual router became the Master.
Advertisements Received	Number of advertisements received that matched the VRRP Virtual Router configuration.
Advertisements Sent	Number of advertisements sent by the VRRP Virtual Router.

You can refresh or clear the statistics available in the VRRP Virtual Router Statistics windows.

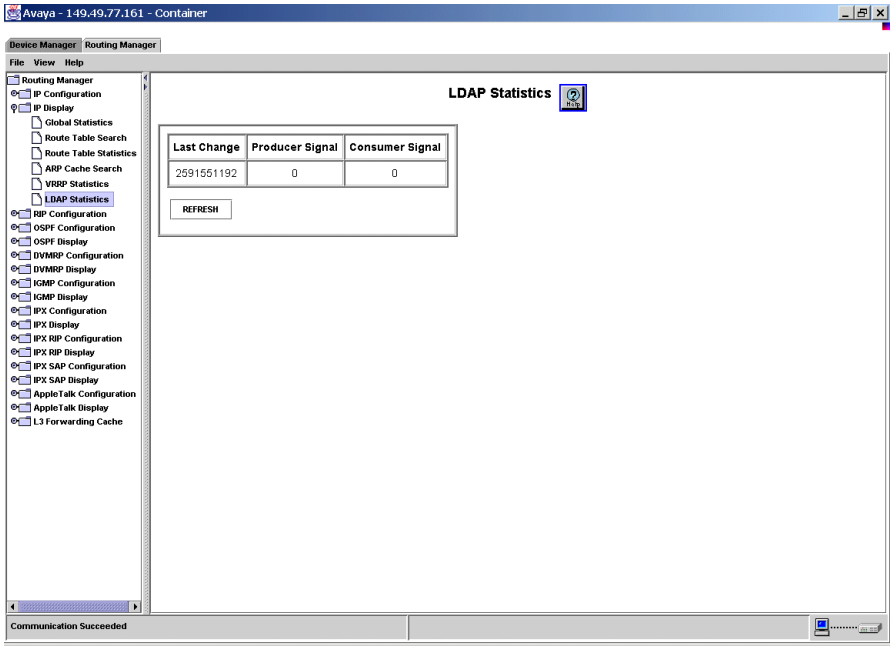
To refresh the statistics, click **REFRESH**. The statistics are refreshed.

To clear the statistics, click **CLEAR**. The statistics are cleared.

LDAP Statistics

To display LDAP statistics, select **IP Display > LDAP Statistics**. The LDAP Statistics window opens.

Figure 12-16. LDAP Statistics Window



The following parameters are displayed:

Table 12-16. LDAP Statistics Parameters

Field	Description
Last Change	The IP address of your primary LDAP server for the access control list domain. This address is used first when connecting to and downloading access lists from an LDAP server. The default value of 0.0.0.0 indicates to the client that there is no primary LDAP server.
Producer Signal	The sequence number that, when modified, triggers the LDAP client to download the latest policy from the LDAP server. If this value is a non-zero value, the LDAP client will compare it to the producer signal on the LDAP server. No comparison is made if the value is zero.
Consumer Signal	Indicates the success of the LDAP client's downloading a policy. If the consumer signal matches the producer signal, then the last time the LDAP client attempted to download a policy, the download was successful. If the consumer signal is -1, then either the LDAP client had a problem processing the access lists or the consumer signal set on the LDAP client did not match the signal configured on the LDAP server. If the consumer signal is not -1 and does not match the producer signal, then the LDAP client was unable to connect to the LDAP server(s).

You can refresh the statistics available in the LDAP Statistics windows. To refresh the statistics, click **REFRESH**. The statistics are refreshed.

RIP Configuration

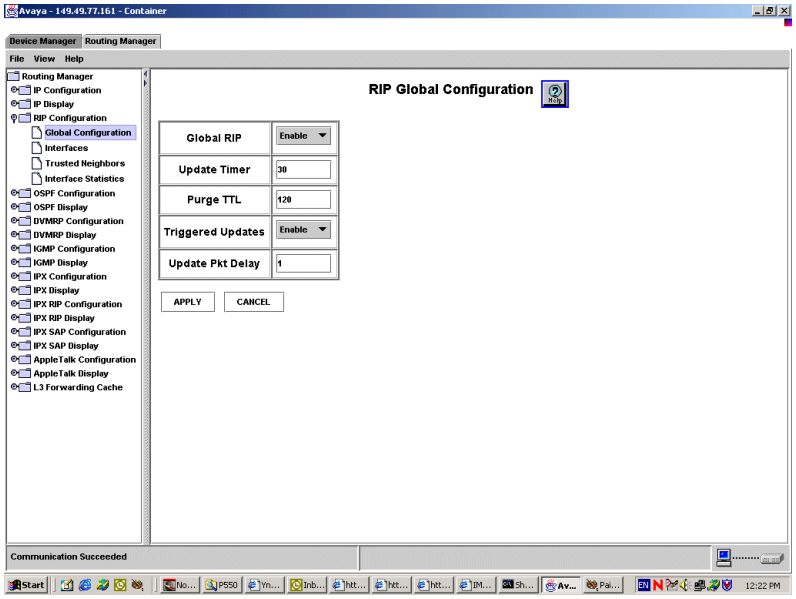
The RIP Configuration folder provides access to the following windows:

- Global Configuration
- Interfaces
- Trusted Neighbors
- Interface Statistics

Global Configuration

To display and update the RIP global configuration, select **RIP Configuration > Global Configuration**. The RIP Global Configuration window opens.

Figure 12-17. RIP Global Configuration Window



The following parameters are displayed:

Table 12-17. Global Configuration Parameters

Field	Description
Global RIP	Enable or disable global RIP.
Update Timer	The value (in seconds) that represents the time between RIP updates on all interfaces.
Purge TTL	The global TTL (in seconds) that the RIP update persists.
Triggered Updates	The state of RIP updates to be immediately transmitted to the network in response to changes in the network topology. Possible values are: • **Enabled** • **Disabled**

Table 12-17. Global Configuration Parameters (Continued)

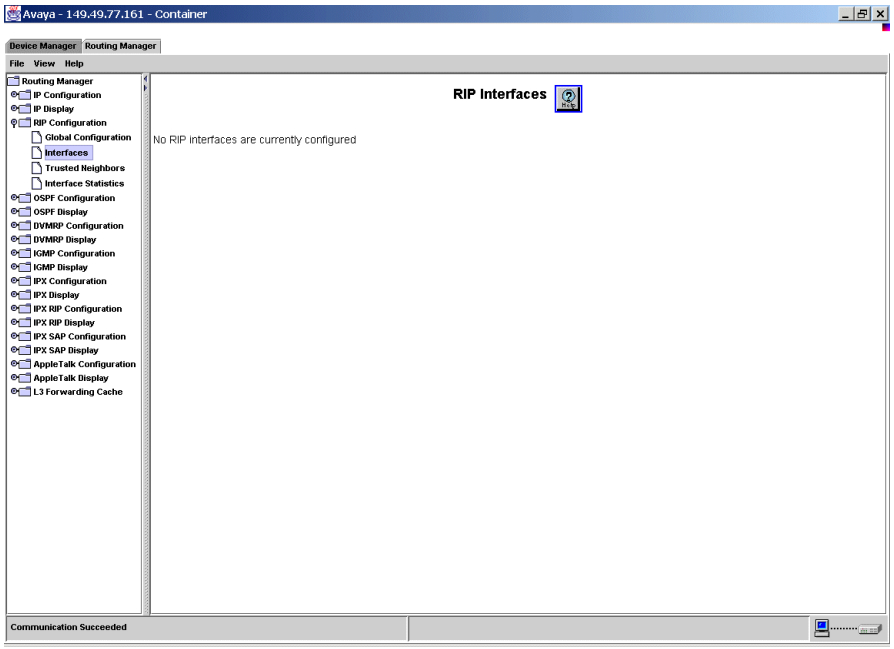
Field	Description
Update Packet Delay	Specify the value (in seconds) that represents the time delay between successive RIP update packets to the neighbor, when the update requires multiple packets.

You can modify the RIP Global Configuration parameters. For information, refer to "Modifying Tables" on page 85.

Interfaces

To display RIP interfaces, select **RIP Configuration > Interfaces**. The RIP Interfaces window opens.

Figure 12-18. RIP Interfaces Window



The following parameters are displayed:

Table 12-18. RIP Interfaces Parameters

Field	Description
Select	Select the RIP interface to modify.
Interface	Displays an interface from the list of interfaces that you previously configured.
Network Address	Displays the IP address to be associated with the displayed interface.
Mode	Specify the RIP State. Possible values are: • **Talk only** - send RIP information to the network • **Listen only** - receive RIP information from the network • **Talk/Listen** - both send and receive RIP information from the network

Table 12-18. RIP Interfaces Parameters (Continued)

Field	Description
Send Version	The version of RIP you want to use to send packets across your interface. Possible values include: • **V1x** • **V2x** • **V1/V2**
Receive Version	Specify the version of RIP you want to use to receive packets across your interface. Possible values include: • **V1x** • **2x** • **V1/V2**
Split Horizon	Specify that the IP routes learned from an immediate neighbor are not advertised back to the neighbor from which the routes were learned.Possible values are • **Split Horizon** - Routes are advertised. • **Split Horizon with Poison Reverse** - Routes are advertised with an infinite metric (16).
Default Route	Specify the mode for the default route. Different states include: • **Disable** - Disables the default route. • **Talk Only** - Send RIP information to the network. • **Listen Only** - Receive RIP information from the network. • **Talk/Listen** - Both send and receive RIP information from the network.
Auth Type	The type of authentication available for use on a give RIP interface. Authentication types include: • **None** - No authentication available • **Simple** - Uses a clear-text-password for validation. • **MD5** - Uses a stronger encryption technique for passwords.

Table 12-18. RIP Interfaces Parameters (Continued)

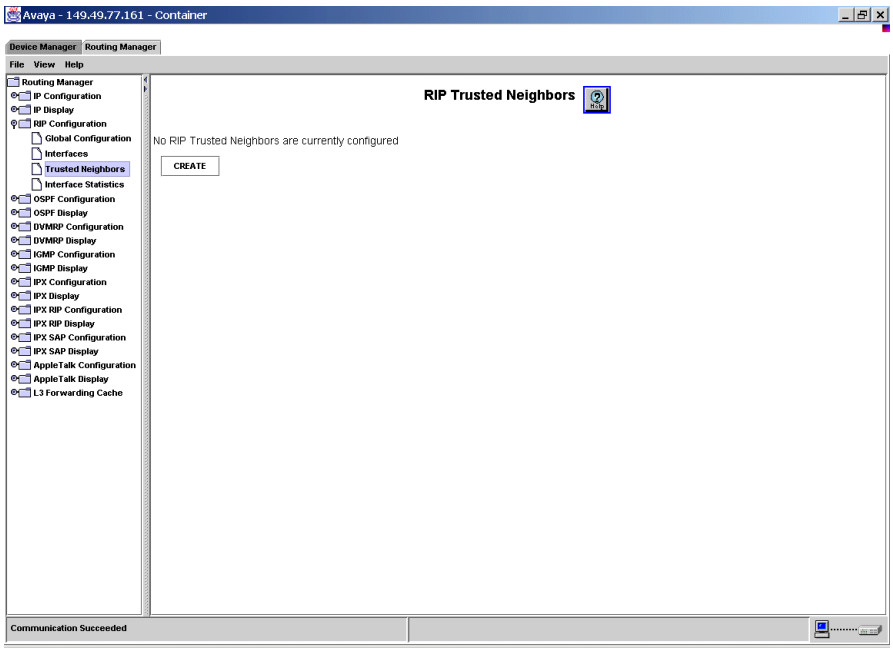
Field	Description
Auth Key	The value for the authorization key.

You can add, modify, or delete RIP Interfaces. For information, refer to "Modifying Tables" on page 85.

Trusted Neighbors

To display and update RIP Trusted Neighbors, select **RIP Configuration > Trusted Neighbors**. The RIP Trusted Neighbors window opens.

Figure 12-19. Trusted Neighbors Window



The following parameters are displayed:

Table 12-19. Trusted Neighbors Parameters

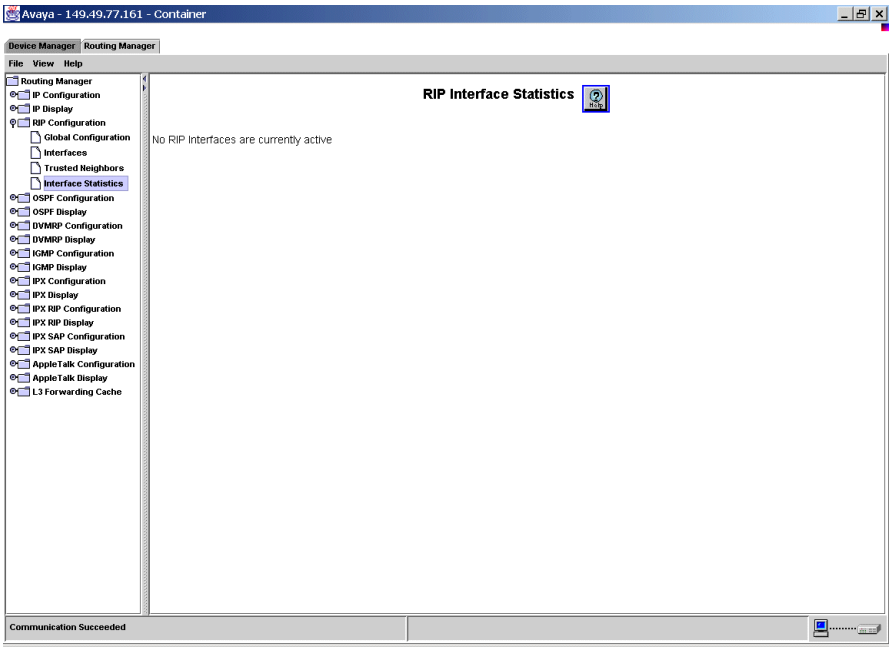
Field	Description
Select	The RIP trusted neighbor to be configured.
Neighbor IP Address	The RIP neighbor from which routing information is learned.

You can add, modify, or delete RIP Trusted Neighbor parameters. For information, refer to "Modifying Tables" on page 85.

Interface Statistics

To display RIP interface statistics, select **RIP Configuration > Interface Statistics**. The RIP Interface Statistics window opens.

Figure 12-20. Interface Statistics Window



The following parameters are displayed:

Table 12-20. Interface Statistics Parameters

Field	Description
Interface	The physical or virtual interface associated with the IP address specified.
State	The current status of the RIP route.Possible values are: • **Up** - Indicates that the interface is active and RIP can transmit and receive updates. • **Down** - Indicates the interface is disabled and can not transmit or receive updates.
IP Address	The IP address associated with the interface. For example, if you configure your switch for an out-of-band connection, the IP address is associated with the Ethernet Console port interface (if RIP is enabled on that interface).

Table 12-20. Interface Statistics Parameters (Continued)

Field	Description
Triggered Updates Sent	The number of RIP triggered updates sent.
Non-triggered Updates Sent	The number of RIP non-triggered updates sent.
Updates Received	The number of RIP updates received based on route changes in the IP routing table.
Bad Packets Received	The number of bad packets received on this interface.
Bad Routes Received	The number of bad routes received on this interface.

You can refresh or clear the statistics available in the RIP Interface Statistics windows.

To refresh the statistics, click **REFRESH**. The statistics are refreshed.

To clear the statistics, click **CLEAR**. The statistics are cleared.

OSPF Configuration

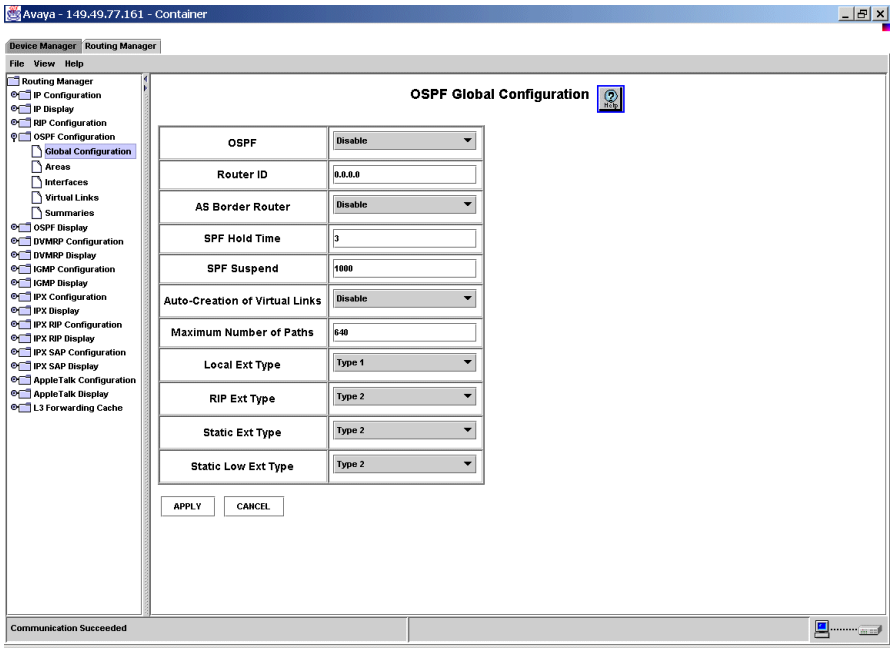
The OSPF Configuration folder provides access to the following windows:

- **Global Configuration**
- **Areas**
- **Interface**
- **Virtual Links**
- **Summaries**

Global Configuration

To display and update the OSPF global configuration, select **OSPF Configuration > Global Configuration**. The OSPF Global Configuration window opens.

Figure 12-21. OSPF Global Configuration Window



The following parameters are displayed:

Table 12-21. Global Configuration Parameters

Field	Description
OSPF	The state of OSPF. Possible values are: • **Enable** • **Disable**
Router ID	The Router ID on the switch. The router ID is a 32-bit number assigned to each switch running the OSPF protocol. This number uniquely identifies the switch within an Autonomous System. If 0.0.0.0 is used, the switch will use one of the active IP addresses of an interface.

Table 12-21. Global Configuration Parameters (Continued)

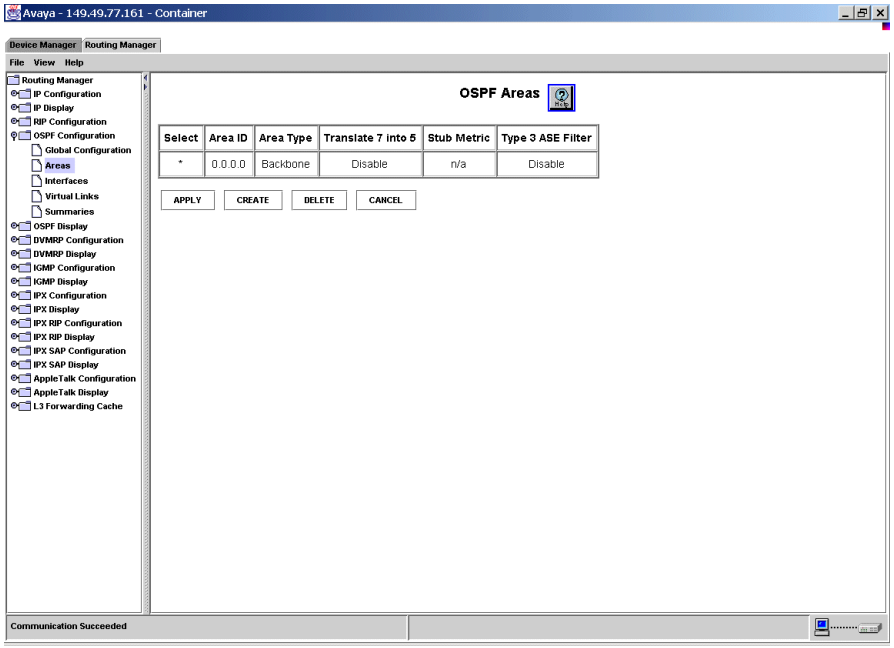
Field	Description
AS Border Route	The state of the switch. Possible values are: • **Enable** - The switch operates as an autonomous system border router (ASBR). • **Disable** - The switch does not operate as an autonomous system border router (ASBR).
SPF Hold Time	The minimum number of seconds between SPF runs.
SPF Suspend	The number of nodes to process SPF functions before suspending.
Auto-Creation of Virtual Links	Select to enable or disable automatic creation of virtual circuits based on network topology.
Maximum Number of Paths	The maximum number of paths used when running SPF.
Local Ext Type	The manner in which imported local routes are advertised in OSPF. Possible values are: • **Type 1** - Internal metrics. • **Type 2** - External metrics.
RIP Ext Type	The manner in which imported RIP routes are advertised in OSPF. Possible values are: • **Type 1** - Internal metrics. • **Type 2** - External metrics.
Static Ext Type	The manner in which imported high preference routes are advertised in OSPF. Possible values are: • **Type 1** - Internal metrics. • **Type 2** - External metrics.
Static Low Ext Type	The manner in which imported low preference routes are advertised in OSPF. Possible values are: • **Type 1** - Internal metrics. • **Type 2** - External metrics.

You can modify OSPF Global parameters. For information, refer to "Modifying Tables" on page 85.

Areas

To display and configure OSPF areas, select **OSPF Configuration > Areas**. The OSPF Areas window opens.

Figure 12-22. OSPF Areas Window



The following parameters are displayed:

Table 12-22. Areas Parameters

Field	Description
Select	The OSPF area to be configured.
Area ID	The IP address for the area. This must be a unique ID.
Area Type	The type of OSPF area. Possible values are: • **Non-Stub** - non-edge device/router. • **Stub** - An edge device/router that does not leak external advertisements. • **Not-so-stubby** - A stub area where the device/router can leak some external advertisements.

Table 12-22. Areas Parameters (Continued)

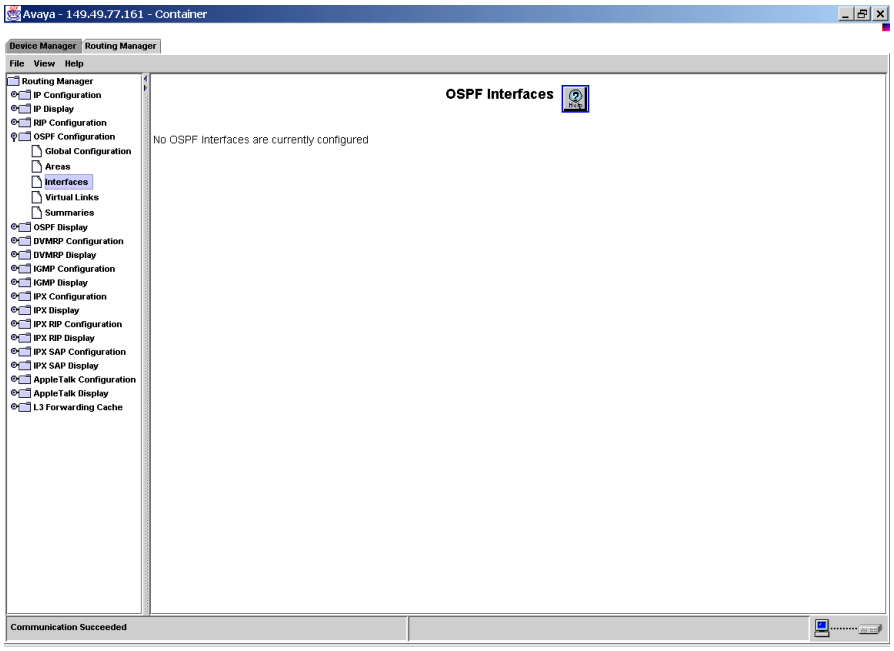
Field	Description
Translate 7 into 5	The status of the translation of the NSSA ASE Type 7 into an AS External LSA Type 5. Possible values are: • **Enable** • **Disable**
Stub Metric	The stub area default summary cost metric. The default is 1.
Type 3 ASE Filter	The status of the Type 3 summary LSA filter status for Stub and NSSA only. Possible values are: • **Enable** • **Disable**

You can add, modify, or delete OSPF Area parameters. For information, refer to "Modifying Tables" on page 85.

Interface

To display OSPF interfaces, select **OSPF Configuration > Interfaces**. The OSPF Interfaces window opens.

Figure 12-23. OSPF Interface Window



The following parameters are displayed:

Table 12-23. OSPF Interface Parameters

Field	Description
Select	The OSPF interface to be modified.
Interface	The IP interface on which OSPF is enabled.
IP Address	The IP address associated with the OSPF interface.
Area	The area ID to be configured for this interface.
DR Priority	The decimal value for this interface for the DR priority function.
Transit Delay	The estimated number of seconds it takes to transmit a link state update packet over this interface.

Table 12-23. OSPF Interface Parameters (Continued)

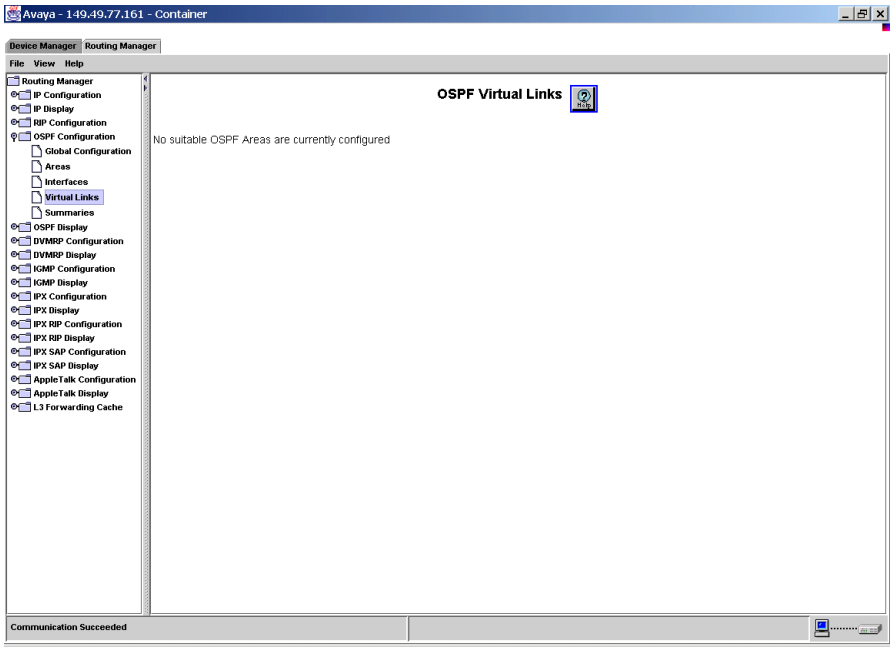
Field	Description
Retransmit Interval	The number of seconds between link-state advertisement retransmissions, for adjacencies belonging to this interface. This value is also used when retransmitting database description and link-state request packets.
Hello Interval	The length of time (in seconds) between the Hello packets the router sends on the interface. This value must be the same for all routers attached to a common network.
Dead Interval	The length of time (in seconds) that a router's Hello packets are not received before it's neighbors declare the router down. This value should be a multiple of the Hello interval.
Poll Interval	The larger time interval (in seconds) between Hello packets sent to an inactive non-broadcast multi-access neighbor.
Cost	The cost metric associated with this interface.
Authentication	The type of authentication available for use on a given OSPF interface. Possible values are: • **None** - No authentication available. • **Simple Password** - Uses a clear-text password for validation. • **MD5 Authentication** - Uses a stronger encryption technique for passwords.
Key	The area's authorization key value.
MD5 Key ID	The key value (in decimal).

You can add, modify, or delete OSPF Interfaces. For information, refer to "Modifying Tables" on page 85.

Virtual Links

To display and configure OSPF virtual links, select **OSPF Configuration > Virtual Links**. The OSPF Virtual Links window opens.

Figure 12-24. OSPF Virtual Links Window



The following parameters are displayed:

Table 12-24. Virtual Links Parameters

Field	Description
Select	The OSPF virtual link to be modified.
Router ID	The router ID for the far end of the virtual link.
Area	The area ID for the area through which the virtual link will travel.
Transit Delay	The estimated number of seconds it takes to transmit a link state update packet over this virtual link.
Retransmit Interval	The number of seconds between link-state advertisement retransmissions, for adjacencies belonging to this interface. This value is also used when re-transmitting database description and link-state request packets.

Table 12-24. Virtual Links Parameters (Continued)

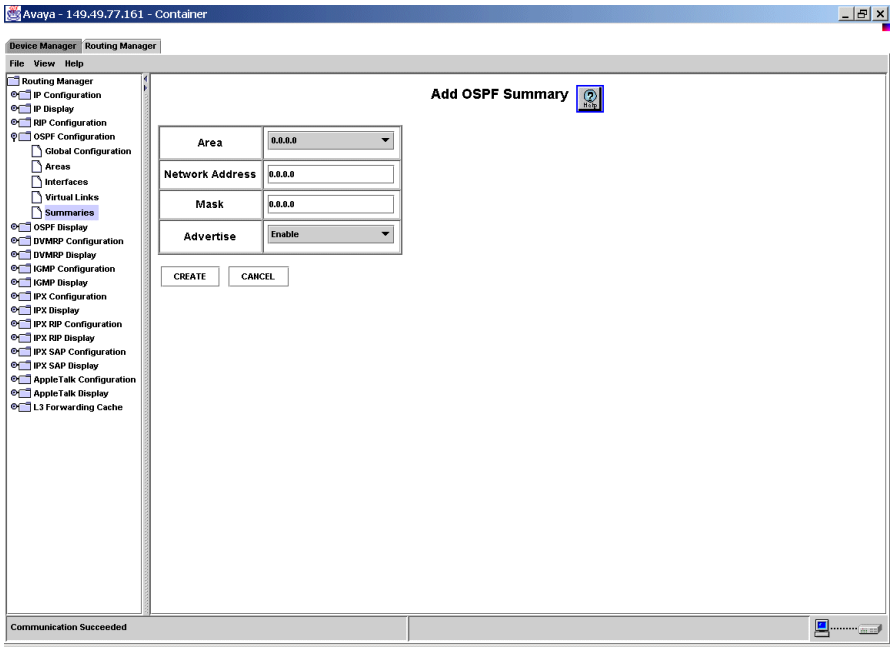
Field	Description
Hello Interval	The length of time (in seconds) between the Hello packets the router sends on the interface. This value must be the same for all routers attached to a common network.
Dead Interval	The length of time (in seconds) that a router's Hello packets have not been seen before it's neighbors declare the router down. This value should be a multiple of the Hello interval.
Authentication	The type of authentication available for use on a given OSPF interface.Possible options include: **None** - No authentication available. **Simple Password** - Uses a clear-text password for validation. **MD5 Authentication** - Uses a stronger encryption technique for passwords.
Key	The authorization key for this virtual link.
MD5 Key ID	The MD5 authentication key ID.

You can add, modify, or delete OSPF Virtual Links. For information, refer to "Modifying Tables" on page 85.

Summaries

To display and configure an OSPF Summary, select **OSPF Configuration > Summaries**. The OSPF Summaries window opens.

Figure 12-25. OSPF Summaries Window



The following parameters are displayed:

Table 12-25. OSPF Summaries Parameters

Field	Description
Area	The area ID from which the routes are aggregated (summary IP address).
Network Address	The IP address of the network to be advertised.
Mask	The subnet mask of the network to be advertised.
Advertise	The status of advertisements for this summary. Possible values are: • **Enabled** • **Suppressed** When **Suppressed**, advertisements of IP routes in this range are also suppressed.

You can add, modify, or delete OSPF Summaries. For information, refer to "Modifying Tables" on page 85.

OSPF Display

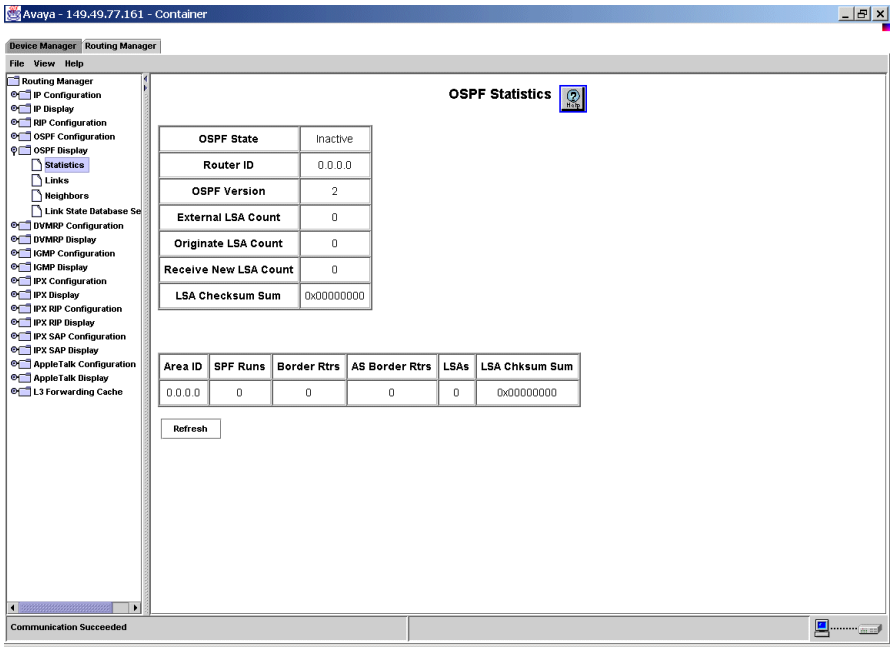
The OSPF Displaying folder provides access to the following windows:

- **Statistics**
- **Links**
- **Neighbors**
- **Link State Database Search**

Statistics

To display OSPF statistics, select **OSPF Display > Statistics**. The OSPF Statistics window opens.

Figure 12-26. OSPF Statistics Window



The following parameters are displayed:

Table 12-26. OSPF Statistics Parameters

Field	Description
OSPF State	The state of OSPF
Router ID	The router ID address for OSPF.
OSPF Version	The current version of OSPF. Avaya P550 and higher support OSPF V2.
External LSA Count	The number of external (LS type 5) link-state advertisements in the link-state database.
Originate LSA Count	The number of LSAs originated by this router.
Receive New LSA Count	The number of new LSAs received by this router.

Table 12-26. OSPF Statistics Parameters (Continued)

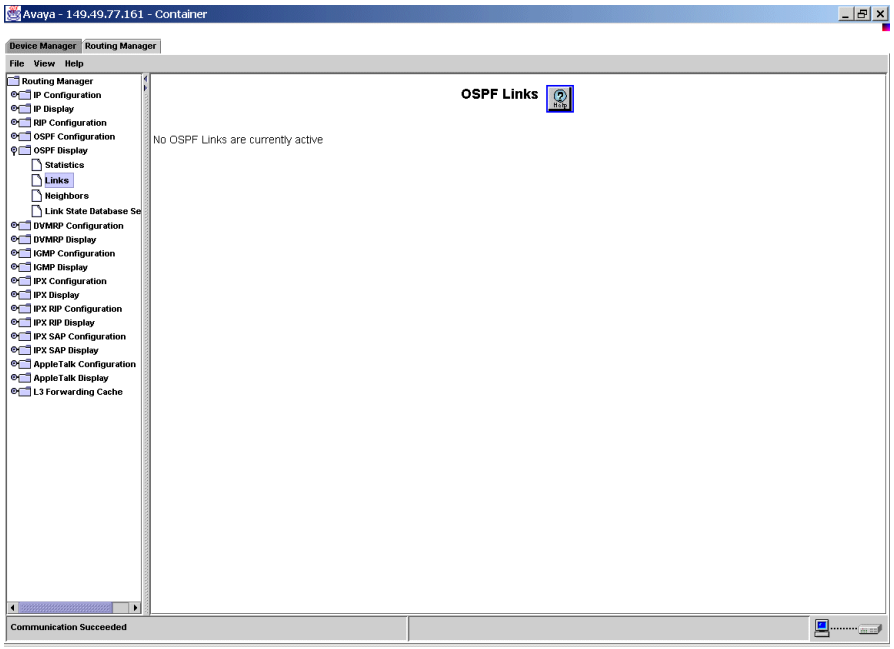
Field	Description
LSA Checksum Sum	The 32-bit unsigned sum of the LS checksums for the external link-state advertisements contained in the link-state database. This sum is used to determine if there has been a change in a router's link-state database, or to compare the link-state database of two routers.
Area ID	The OSPF area ID.
SPF Runs	The number of times that the intra-area route table has been calculated using this area's link-state database.
Border Rtrs	The total number of area border routers reachable within this area. The default is zero, and is calculated in each SPF pass.
AS Border Rtrs	The total number of Autonomous System border routers reachable within this area. The default is zero, and is calculated in each SPF pass.
LSAs	The total number of link-state advertisements in this area's link-state database, excluding AS External LSAs.
LSA Chksum Sum	A 32-bit unsigned sum of the LS checksums for the external link-state advertisements contained in the link-state database. This sum is used to determine if there has been a change in a router's link-state database, or to compare the link-state database of two routers.

You can refresh the statistics available in the OSPF Statistics windows. To refresh the statistics, click **REFRESH**. The statistics are refreshed.

Links

To display OSPF links, select **OSPF Display > Links**. The OSPF Links window opens.

Figure 12-27. OSPF Links Window



The following parameters are displayed:

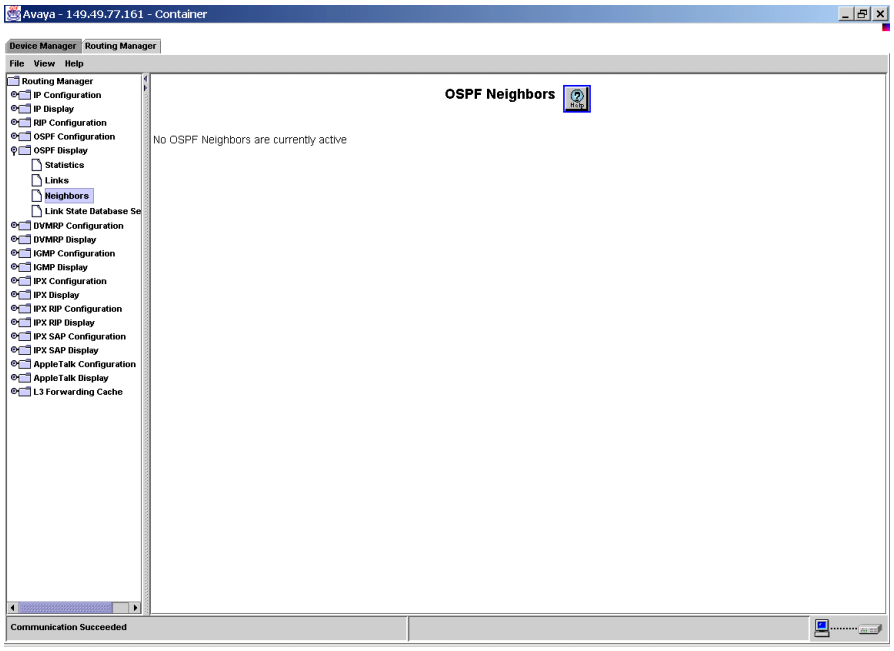
Table 12-27. OSPF Links Parameters

Field	Description
State	The status of the OSPF link.
IP Address	The IP address of the OSPF link.
Area ID	The area ID (IP address) associated with the OSPF link.
Type	The type of OSPF link.
DR Router ID	The identification of the designated router.
DR Address	The IP address of the designated router.
BDR Address	The IP address of the designated border router.

Neighbors

To display OSPF neighbors, select **OSPF Display > Neighbors**. The OSPF Neighbors window opens.

Figure 12-28. OSPF Neighbors Window



The following parameters are displayed:

Table 12-28. OSPF Neighbors Parameters

Field	Description
IP Address	The IP address (interface) associated with the OSPF neighbor.

Table 12-28. OSPF Neighbors Parameters (Continued)

Field	Description
State	The functional state of the interface.Possible values are: • **Down** - The initial state of a neighbor conversation. It indicates that no information has recently been received. • **Attempt** - Indicates that no recent information has been received from the neighbor, but that a more concerted effort should be made to contact the neighbor. • **INIT** - Indicates that the Hello packet has recently been seen from the neighbor. However, bi-directional communication has not yet been established with the neighbor. • **2-Way** - Communication between the two routers is bi-directional. • **ExStart** - The first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and upon the initial DD sequence number. Neighbor conversations in this state or greater are called adjacencies. • **Exchange** - Router is describing its entire link state database by sending Database Description packets to the neighbor. • **Loading** - Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state. • **Full** - The neighboring routers are fully adjacent. These adjacencies will now appear in router-LSAs and network-LSAs.
Router ID	The router ID of the neighbor.
Master	The state of the neighbor. Possible values are: • **Master** • **Slave**.

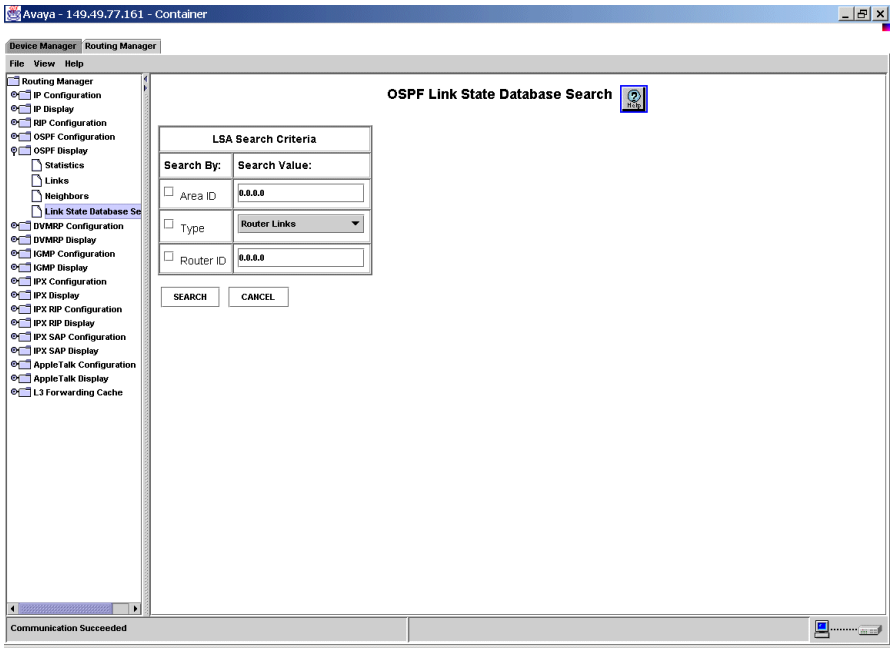
Table 12-28. OSPF Neighbors Parameters (Continued)

Field	Description
DD Number	The hexadecimal number used to sequence the collection of Database Description Packets. The initial value, indicated by the Init bit being set should be unique. The DD sequence number then increments until the complete database description has been sent.
DR Priority	The DR priority of the neighbor router.
E-Option	The method used to flood AS-external LSAs.
T-Option	Displays whether this neighbor is an ASBR.
MC-Option	Displays whether this neighbor supports MOSPF.
N-Option	Displays whether this neighbor supports the handling of Type-7 LSAs.
OPQ-Option	Displays whether this neighbor supports opaque LSAs.
DR Choice	Displays the IP address of the designated router.
BDR Choice	Displays the IP address of the designated backup router.

Link State Database Search

To display and configure OSPF link state database search criteria, select **OSPF Display > Link State Database Search**. The OSPF Link State Database Search window opens.

Figure 12-29. OSPF Link State Database Search Window



The following parameters are displayed:

Table 12-29. Link State Database Search Parameters

Field	Description
Area ID	Enter the search area IP address for all database entries in the specified area.
Type	Select the search type for all advertisement entries in the database. Possible values are: • **Router Links** - These packets describe the states of the router's links to the area and are only flooded within a particular area. • **Network Links** - These packets are generated by Designated Routers and describe the set of routers attached to a particular network. • **Summary Network** - These summaries are generated by Area Border Routers and describe inter-area routes to various networks. They can also be used for aggregating routes. • **Summary AS Border** - This describes links to Autonomous System Border Routers and are generated by Area Border Routers. • **AS External** - These packets are generated by Autonomous System Border Routers and describe routes to destinations external to the Autonomous system. They are flooded everywhere except stub areas. • **Multicast Group** - These packets are generated by multicast group. • **NSSA External** - These packets are generated by Area Border Routers and describe routes within the NSSA (Not-So-Stubby-Area).
Router ID	The router ID of the link-state database for entries originated by this router.

To search the Link State Database:

1. Enter the criteria by which you want to search.
2. Ensure that the Search by checkbox next to the criteria is checked.
3. Click **SEARCH**. A window opens in the Table Area with the results of the search.

DVMRP Configuration

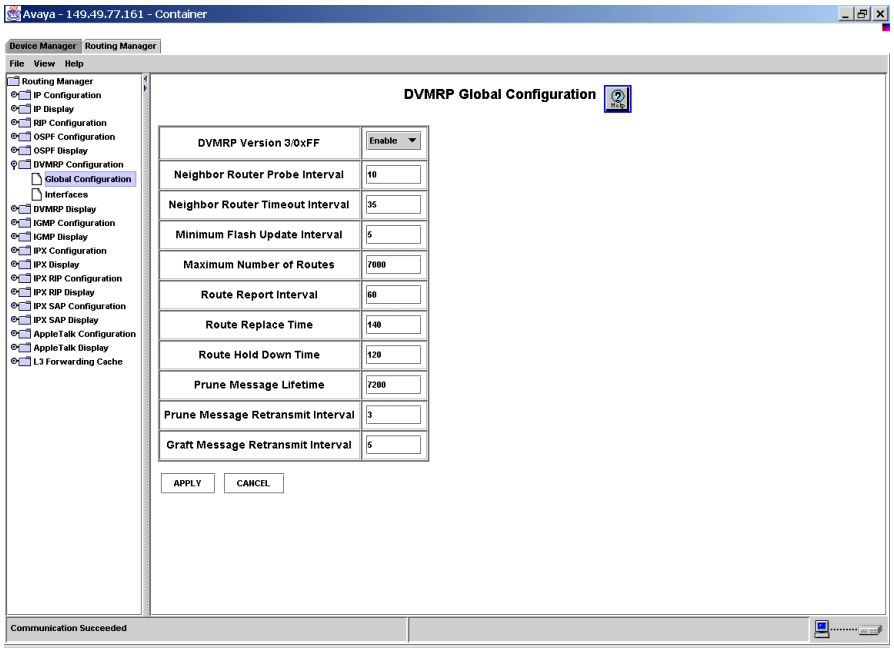
The DVMRP Configuration folder provides access to the following windows:

- **Global Configuration**
- **Interfaces**

Global Configuration

To display and update the DVMRP global configuration, select **DVMRP Configuration > Global Configuration**. The DVMRP Global Configuration window opens.

Figure 12-30. DVMRP Global Configuration Window



The following parameters are displayed:

Table 12-30. DVMRP Global Configuration Parameters

Field	Description
DVMRP Version 3/0xFF	The status of DVMRP. Possible values are: • **Enable** • **Disable**
Neighbor Router Probe Interval	The amount of time, in seconds, that the switch probes the network for available neighbor routers.
Neighbor Router Timeout Interval	The amount of time, in seconds, that a neighbor stays up without confirmation. This is used to timeout old routes.
Minimum Flash Update Interval	The amount of time, in seconds, between flash updates. This represents the minimum amount of time between advertisements of the same route.

Table 12-30. DVMRP Global Configuration Parameters (Continued)

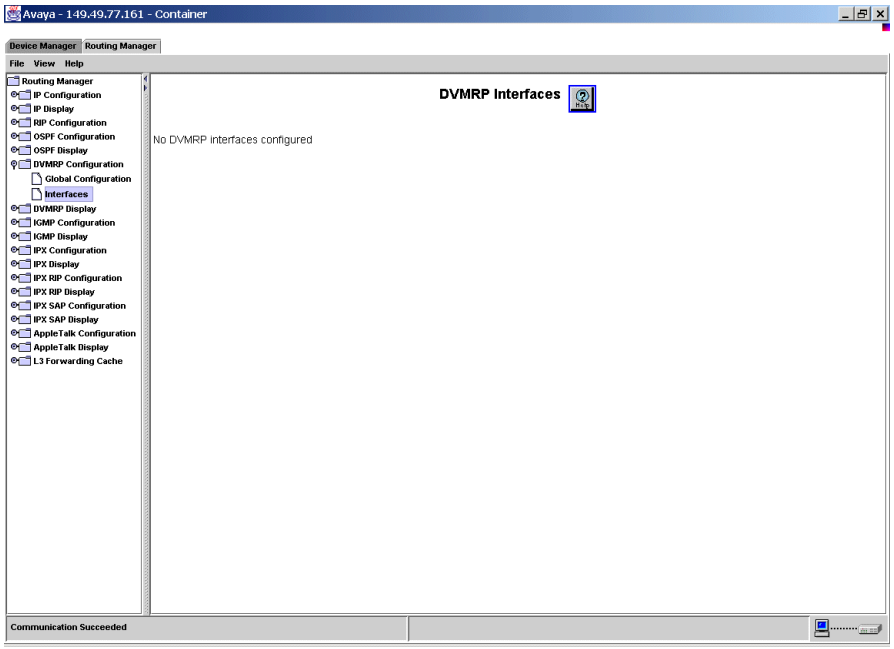
Field	Description
Maximum Number of Routes	The value for the maximum number of routes for this interface.
Router Report Interval	The amount of time, in seconds, that elapses between delivery of DVMRP routing table updates.
Router Replace Time	The amount of time, in seconds, before which a route entry is removed if it is not refreshed.
Route Hold Down Time	The amount of time, in seconds, that a switch reports unavailable routes with a metric of infinity.
Prune Message Lifetime	The amount of time, in seconds, that the transmitted prune message persists.
Prune Message Retransmit Interval	The amount of time, in seconds, between the transmission of prune messages on your network.
Graft Message Retransmit Interval	The amount of time, in seconds, between the transmitting of graft messages.

You can modify DVMRP Global parameters. For information, refer to "Modifying Tables" on page 85.

Interfaces

To display and configure DVMRP interfaces, select **DVMRP Configuration > Interfaces**. The DVMRP Interfaces window opens.

Figure 12-31. DVMRP Interfaces Window



The following parameters are displayed:

Table 12-31. DVMRP Interfaces Parameters

Field	Description
Select	The DVMRP interface to be configured.
Interface	The interface that is configured with the DVMRP multicast protocol.
IP Address	The IP address of the DVMRP interface.
IP Address Mask	The subnet mask of each interface.

Table 12-31. DVMRP Interfaces Parameters (Continued)

Field	Description
Interface Type	Select the interface type for each interface. Possible values are: • **Broadcast** - All traffic is forwarded through the routers. This is not a tunnel and does not require encapsulation. • **Non-Encapsulated Tunnel** - All multicast traffic is IPIP encapsulated, but the protocol messages are unicast. • **IPIP Tunnel** - All multicast traffic on this interface is encapsulated in IP unicast packets with the protocol set to IPIP.
Tunnel Endpoint Address	The tunnel endpoint IP address of a router. Configure this setting to represent the IP address of another router to which you want to send datagrams through a tunnel.
Interface Metric	The cost metric between a source and endpoint router.
Src Host Addr in Prune Msg	The state of host addresses in prune messages. Possible values are: • **Enable** - Send prunes with the host address. • **Disable** - Send prunes with the subnet address.
Interface Scope	The number that represents minimum TTL required for a packet to leave this interface. Possible values are: • **None** - No limits set. • **127** • **255**

You can add, modify, or delete DVMRP Interfaces. For information, refer to "Modifying Tables" on page 85.

DVMRP Display

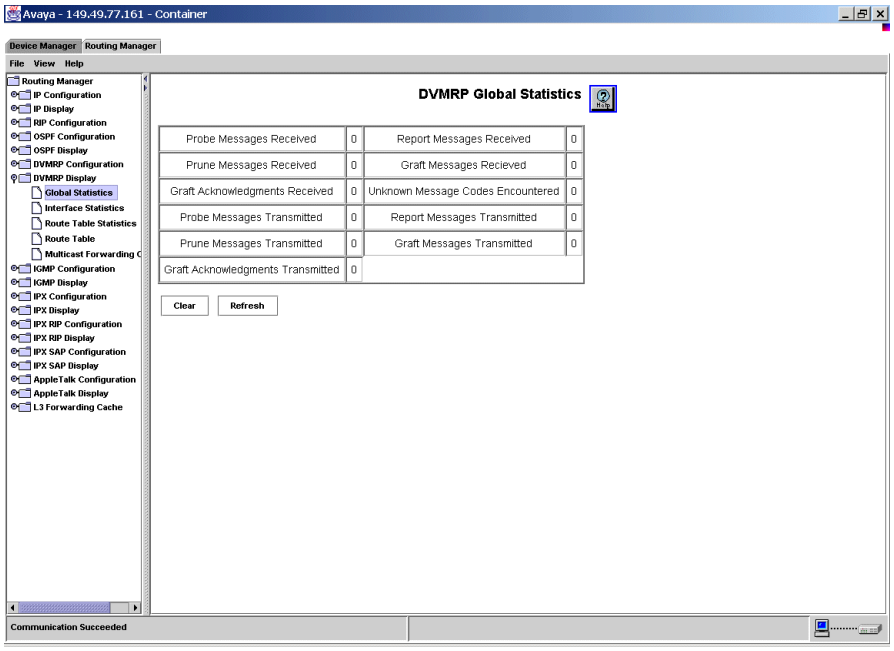
The DVMRP Display folder contains the following:

- **Global Statistics**
- **Interface Statistics**
- **Route Table Statistics**
- **Route Table**
- **Multicast Forwarding Cache**

Global Statistics

To display DVMRP global statistics, select **DVMRP Display > Global Statistics**. The DVMRP Global Statistics window opens.

Figure 12-32. DVMRP Global Statistics Window



The following parameters are displayed:

Table 12-32. DVMRP Global Statistics Parameters

Field	Description
Probe Message Received	Probe messages received on this switch. DVMRP routers exchange probes and routing updates so they each have a picture of their neighbors' capabilities and the DVMRP network topology.
Prune Messages Received	Prune messages received on this switch. This indicates the number of old branches removed from the multicast distribution tree.
Graft Acknowledgements Received	Graft acknowledgments received.
Probe Messages Transmitted	Probe messages transmitted to the network.

Table 12-32. DVMRP Global Statistics Parameters (Continued)

Field	Description
Prune Messages Transmitted	Prune messages transmitted upstream on this switch. This indicates the number of old branches removed from the multicast distribution tree.
Graft Acknowledgements Transmitted	Graft acknowledgments sent downstream from this switch. This indicates the number of new downstream branches added to the multicast distribution tree.
Report Messages Received	Report messages received on this switch.
Graft Messages Received	The number of attempts at adding a new branch to the multicast distribution tree.
Unknown Message Codes Encountered	Messages received that are not graft, report, or probe messages.
Report Messages Transmitted	Report messages transmitted to the network.
Graft Messages Transmitted	Graft messages transmitted upstream from this switch. This indicates the number of new upstream branches added to the multicast distribution tree.

You can refresh or clear the statistics available in the DVMRP Global Statistics windows.

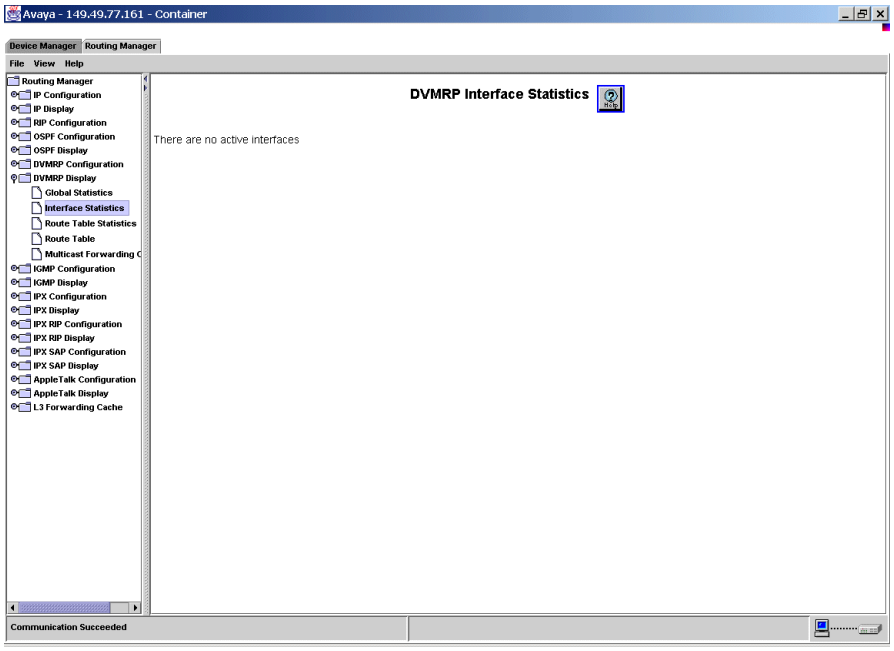
To refresh the statistics, click Refresh. The statistics are refreshed.

To clear the statistics, click Clear. The statistics are cleared.

Interface Statistics

To display DVMRP interface statistics, select **DVMRP Display > Interface Statistics**. The DVMRP Interface Statistics window opens.

Figure 12-33. DVMRP Interface Statistics Window



The following parameters are displayed:

Table 12-33. DVMRP Interface Statistics

Field	Description
DVMRP Interface	The IP interface configured with the DVMRP multicast routing protocol.
Network Address	The IP address of the interface configured with the DVMRP multicast.
Address Mask	The IP subnet mask associated with the interface.
State	The current status of the interface. Possible status indications include: • **UP** - The interface is active. • **DOWN** - The interface is inactive.

Table 12-33. DVMRP Interface Statistics (Continued)

Field	Description
Type	The type of interface configured. Possible values include: • **Broadcast** - All traffic is forwarded through the routers. This is not a tunnel and does not require encapsulation. • **IPIP Tunnel** - All multicast traffic (data and protocol messages) on this interface is encapsulated in IP unicast packets with the protocol set to IPIP (IP in IP). • **Non-Encapsulated Tunnel** - All multicast data traffic on this interface is IPIP encapsulated, but the protocol messages are simple unicast.
Metric	The interface cost.
IGMP Querier On Interface	The Router is the IGMP querier. The purpose of the IGMP querier is to periodically poll hosts on your network to trigger group membership reports.
Next Probe Message in (sec)	The amount of time, in seconds, remaining until the next probe message is sent.
Unrecognized packets received	The number of unknown DVMRP messages.
Invalid routes received	The number of invalid routes received on this interface.
Neighbor DVMRP Router(s)	The number of (neighbor) routers that are also running DVMRP. *** Note:** This number is a hypertext link that provides additional information on the DVMRP neighbor router(s).

You can refresh or clear the statistics available in the DVMRP Interface Statistics windows.

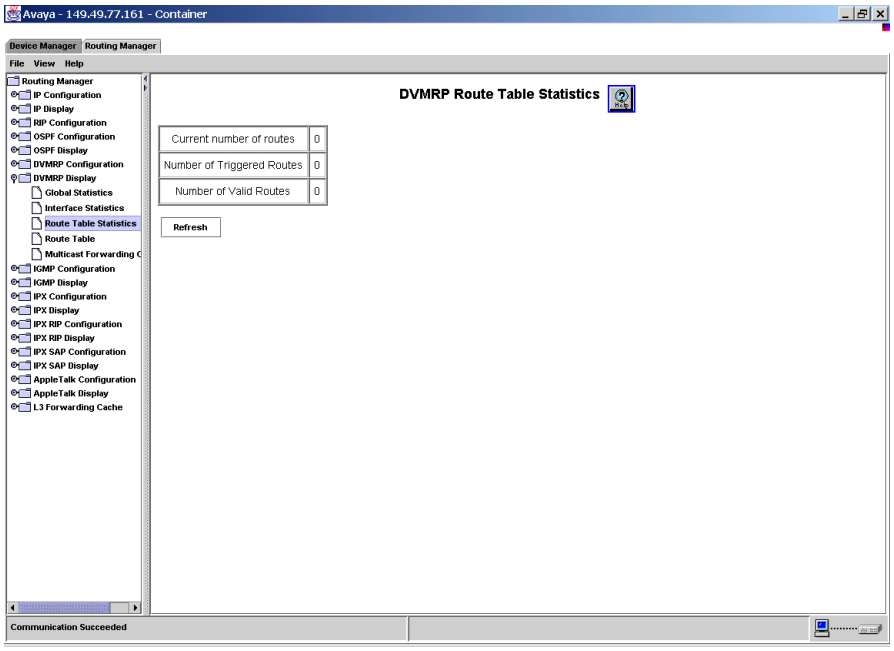
To refresh the statistics, click Refresh. The statistics are refreshed.

To clear the statistics, click Clear. The statistics are cleared.

Route Table Statistics

To display DVMRP route table statistics, select **DVMRP Display > Route Table Statistics**. The DVMRP Route Table Statistics window opens.

Figure 12-34. DVMRP Route Table Statistics Window



The following parameters are displayed:

Table 12-34. DVMRP Route Table Statistics Parameters

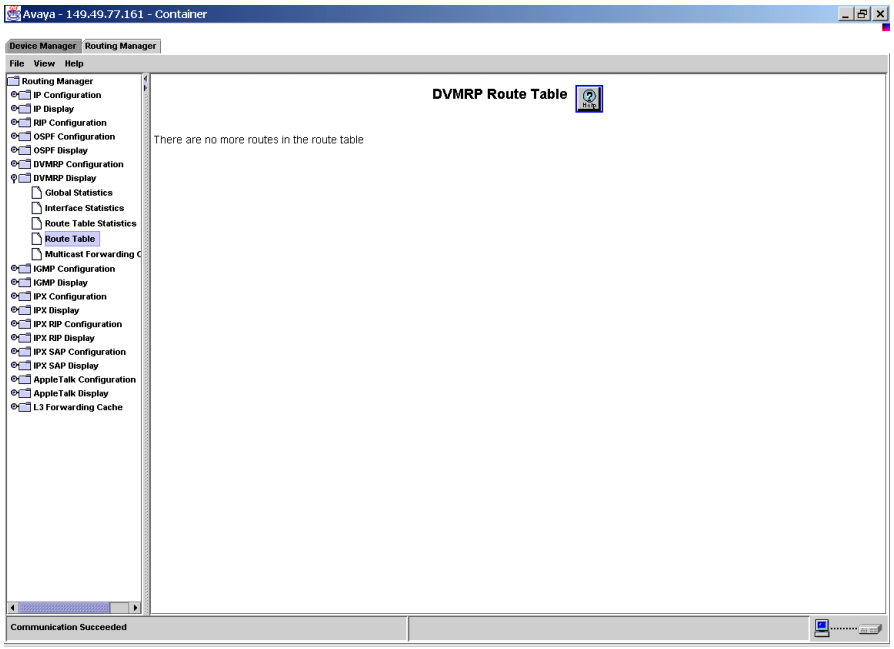
Field	Description
Current Number of Routes	The current number of DVMRP routes.
Number of Triggered Routes	The number of triggered DVMRP routes.
Number of Valid Routes	The number of valid DVMRP routes.

You can refresh the statistics available in the DVMRP Route Table Statistics windows. To refresh the statistics, click **REFRESH**. The statistics are refreshed.

Route Table

To display the DVMRP route table, select **DVMRP Display > Route Table**. The DVMRP Route Table window opens.

Figure 12-35. DVMRP Route Table Window



The following parameters are displayed:

Table 12-35. DVMRP Route Table Parameters

Field	Description
Select	Select the DVMRP route.
Source Network	The network from which the multicast flow originates.
Source Network Mask	The source network mask.
Reporting Router	The IP address of the router closest to the source network.
Reporting Router Interface	The subnet VLAN configured on the upstream neighbor DVMRP router.

Table 12-35. DVMRP Route Table Parameters (Continued)

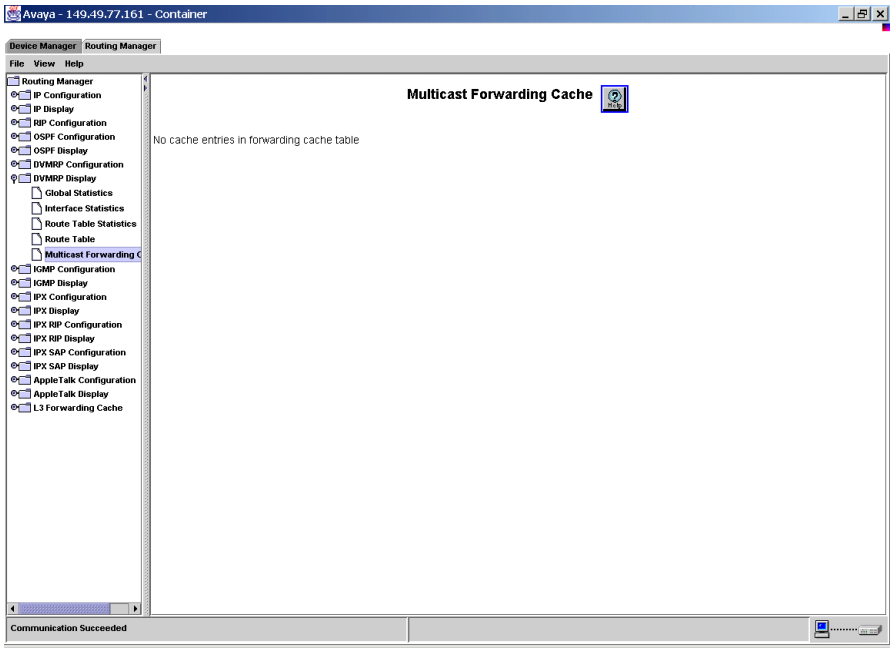
Field	Description
Route Metric	The information configured by the network administrator that is associated with the hop count or lowest cost to reach a next hop destination. In this case, the destination is a DVMRP router.
Expiration Period (sec)	The amount of time, in seconds, remaining before the source sub-network is removed from the DVMRP routing table.
Upstream Router	The IP address of the DVMRP router that is the upstream neighbor to the local router. The local DVMRP router must know which DVMRP router is its upstream neighbor to determine how packets from a given source will be transmitted to a given multicast group.
Designated Forwarder(s)	The network router that is responsible for forwarding from the source network onto the upstream interface.
Downstream Dependent Router	The number of downstream DVMRP routers that send a poison reverse message to its upstream neighbor when it is dependent on that neighbor to receive traffic from a given source network.

You can add, modify, or delete DVMRP Route Table entries. For information, refer to "Modifying Tables" on page 85.

Multicast Forwarding Cache

To display the DVMRP multicast forwarding cache, select **DVMRP Display > Multicast Forwarding Cache**. The Multicast Forwarding Cache window opens.

Figure 12-36. Multicast Forwarding Cache Window



The following parameters are displayed:

Table 12-36. Multicast Forwarding Cache Parameters

Field	Description
Select	Select the multicast forwarding cache.
Destination Group Address	The destination group address of the multicast transmission.
Source SubNetwork	The subnet from which the flow is coming.
Source Address Mask	The subnet mask associated with the DVMRP source subnetwork.
Upstream Interface	The local interface which is receiving this flow.
Invalid Flows From Upstream	The number of invalid flows received from the upstream neighbor.
Packets Forwarded through Cache Entry	The number of packets successfully forwarded in the CPU for this flow.

Table 12-36. Multicast Forwarding Cache Parameters (Continued)

Field	Description
Upstream Interface is Pruned	The router that is sending prunes to the upstream neighbor. This allows you to open the DVMRP Upstream Prune Information dialog box.
Next Pruned Downstream Interface to Timeout	The next interface that is currently pruned which will be grafted back.
Downstream Interface(s)	The number of downstream interfaces. This allows you to open the DVMRP Downstream Links dialog box.
Upstream Source(s)	The number of upstream interfaces. This allows you to open the Upstream Sources dialog box.

You can add, modify, or delete Multicast Forwarding Cache entries. For information, refer to "Modifying Tables" on page 85.

IGMP Configuration

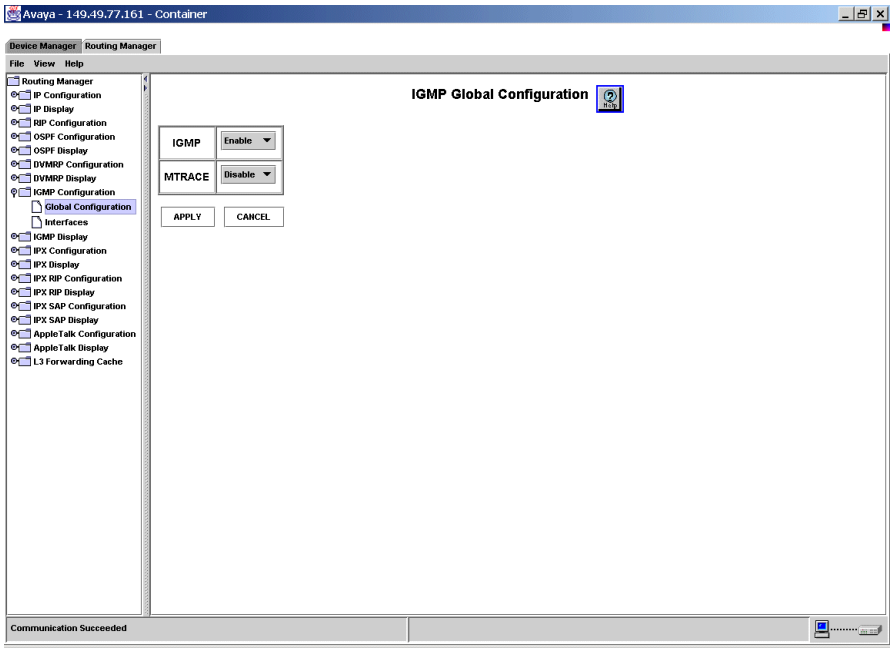
The IGMP Configuration folder includes the following:

- **Global Configuration**
- **Interfaces**

Global Configuration

To display and update the IGMP global configuration, select **IGMP Configuration > Global Configuration**. The IGMP Global Configuration window opens.

Figure 12-37. IGMP Global Configuration Window



The following parameters are displayed:

Table 12-37. IGMP Global Configuration Parameters

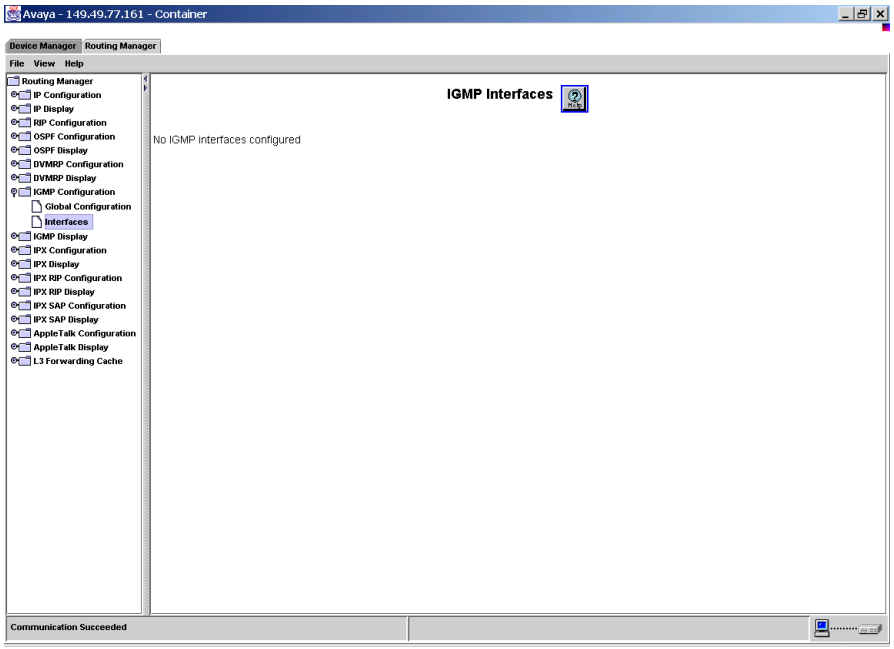
Field	Description
IGMP	The status of IGMP configuration. Possible values are: • **Enable** • **Disable**
MTRACE	The status of MTRACE support. Possible values are: • **Enable** • **Disable**

You can modify IGMP Global parameters. For information, refer to "Modifying Tables" on page 85.

Interfaces

To display and configure IGMP interfaces, select **IGMP Configuration> Interfaces**. The IGMP Interfaces window opens.

Figure 12-38. IGMP Interfaces Window



The following parameters are displayed:

Table 12-38. IGMP Interfaces Parameters

Field	Description
Select	The interface to be modified.
Interface	The IP interface that is configured with IGMP.
IP Address	Identify an IP address associated with this interface. This parameter is not configurable from the IGMP configuration dialog box.
IP Address Mask	Identify a subnet mask associated with this interface. This parameter is not configurable from the IGMP configuration dialog box.

Table 12-38. IGMP Interfaces Parameters (Continued)

Field	Description
IGMP Version	Specify the IGMP Version to associate with the IGMP interface. Possible values are: • **1.0** • **2.0**
Maximum Groups	The number of IGMP Groups that can be active on this interface. The default value is 32.
Always be a Group Membership Querier	The state of group membership. Possible values for Version 1.0 are: • **Enable** • **Disable** Possible values for Version 2.0: • **Enable** - Force this interface to send queries. • **Disable** - Obey the designated querier election.Only the designated router will query hosts on your network. This is the default.
Process Leave Packets	Terminate group memberships quickly. (IGMP Version 2.0 only). The default value is Enabled.
Query Request Interval (sec)	The time period between queries. The default value is 125 seconds.
Query Response Interval	The amount of time to wait for a response from a host after sending a query. If no response is received within this time, the host is removed from the group table. The default value is 10 seconds.
Neighbor Querier Timeout Interval	The amount of time, in seconds, this interface should wait after hearing a neighbor's query before assuming the role of querier, if not already the querier. If no query is received from a neighbor with a lower IP address in the allotted time, this interface becomes the querier. (IGMP Version 2.0 only). The default value is 255 seconds.

Table 12-38. IGMP Interfaces Parameters (Continued)

Field	Description
Robustness Variable	Perform tuning for the expected packet loss on a subnet. The greater the amount of expected packet loss in this subnet, the higher the Robustness Variable should be set. The Robustness Variable must not be set to 0 and should not be set to 1. The default value is 2.
Preference	The state of the routing preference. Possible values are: • **High** • **Low**

You can add, modify, or delete IGMP Interfaces. For information, refer to "Modifying Tables" on page 85.

IGMP Display

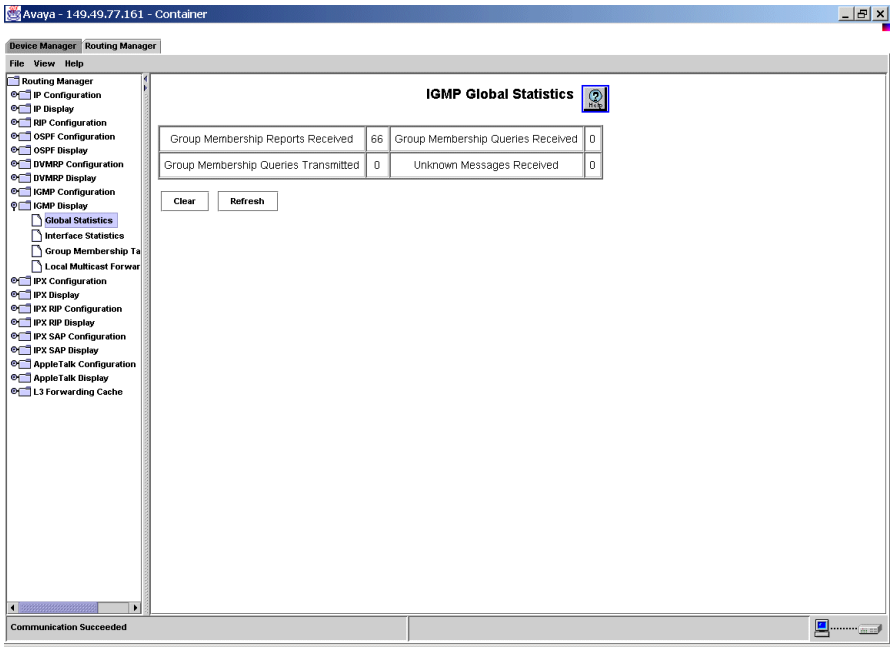
The IGMP Display folder includes the following:

- **Global Statistics**
- **Interface Statistics**
- **Group Membership Table**
- **Local Multicast Forwarding Cache**

Global Statistics

To display IGMP global statistics, select **IGMP Display > Global Statistics**. The IGMP Global Statistics window opens.

Figure 12-39. IGMP Global Statistics Window



The following parameters are displayed:

Table 12-39. IGMP Global Statistics Parameters

Field	Description
Group Membership Reports Received	The number of reports received in response to a group membership query. Hosts respond to a Query by generating Host Membership Reports reporting each host group to which they belong on the network interface from which the Query was received.
Group Membership Queries Transmitted	The number of query messages sent by all local IGMP interfaces. These messages are sent to discover which host groups have members on their attached local networks. Queries are addressed to the all-hosts group (address 224.0.0.1), and carry an IP time-to-live of 1.

Table 12-39. IGMP Global Statistics Parameters (Continued)

Field	Description
Group Membership Queries Received	The number of query messages received by all local IGMP interfaces. All hosts that receive this query transmit a group membership report reporting each host group to which they belong.
Unknown Messages Received	An IGMP message of a type other than Group Membership Query, Group Membership Report, or Leave Group.

You can refresh or clear the statistics available in the IGMP Global Statistics windows.

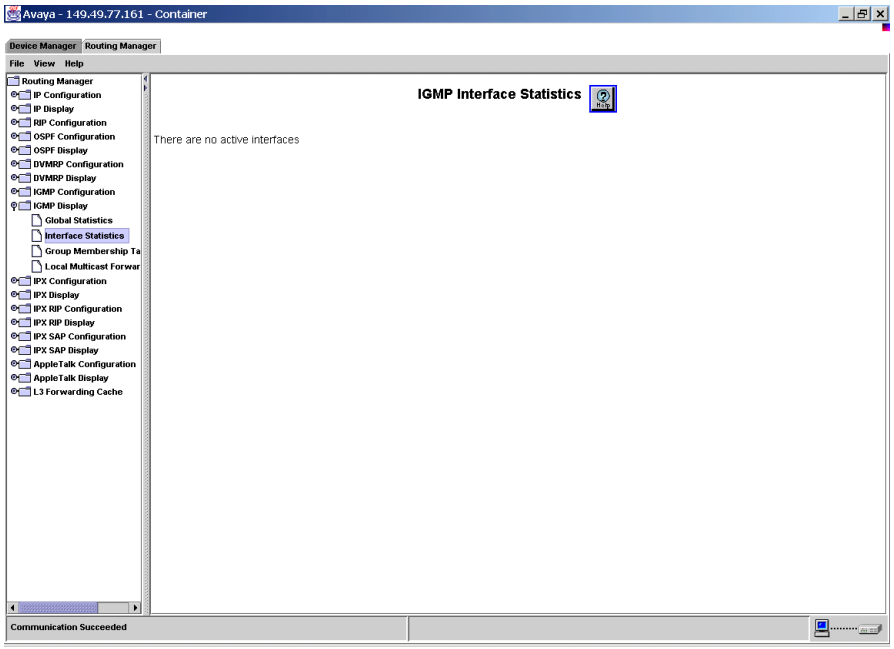
To refresh the statistics, click **REFRESH**. The statistics are refreshed.

To clear the statistics, click **CLEAR**. The statistics are cleared.

Interface Statistics

To display IGMP interface statistics, select **IGMP Display > Interface Statistics**. The IGMP Global Statistics window opens.

Figure 12-40. IGMP Interface Statistics Window



The following parameters are displayed:

Table 12-40. IGMP Interfaces Parameters

Field	Description
Interface	The IP interface that is configured with IGMP.
IP Address	The IP address associated with this interface. This parameter is not configurable from the IGMP configuration dialog box.
IP Address Mask	The subnet mask associated with this interface. This parameter is not configurable from the IGMP configuration dialog box.
IGMP Version	The IGMP Version to associate with the IGMP interface. Possible values are: • **1.0** • **2.0**
Maximum Groups	The number of IGMP Groups that can be active on this interface. The default value is 32.

Table 12-40. IGMP Interfaces Parameters (Continued)

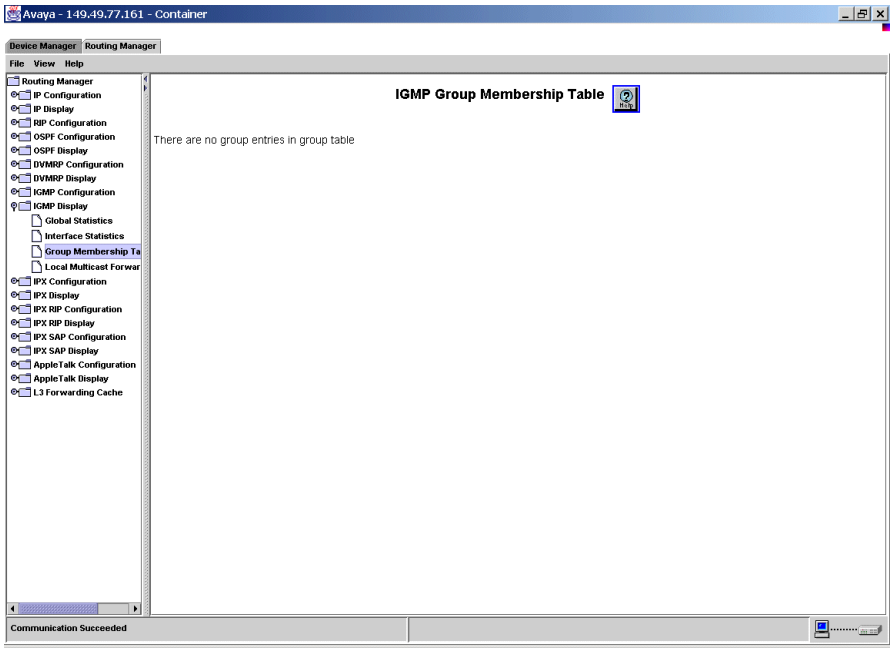
Field	Description
Process Leave Packets	Terminate group memberships quickly. (IGMP Version 2.0 only). The default value is Enabled.
Query Request Interval (sec)	The amount of time, in seconds, between queries. The default value is 125 seconds.
Query Response Interval (sec)	The amount of time, in seconds, to wait for a response from a host after sending a query. If no response is received within this time, the host is removed from the group table. The default value is 10 seconds.
Neighbor Querier Timeout Interval (sec)	The amount of time, in seconds, this interface should wait after hearing a neighbor's query before assuming the role of querier. If no query is received from a neighbor with a lower IP address in the allotted time, this interface becomes the querier. (IGMP Version 2.0 only). The default value is 255 seconds.
Robustness Variable	Perform tuning for the expected packet loss on a subnet. If a subnet is expected to have more packet loss, the Robustness Variable should be increased. The Robustness Variable must not be set to 0 and should not be set to 1. The default value is 2.
Preference	Specify a low or high routing preference.

You can refresh the statistics available in the IGMP Interface Statistics windows. To refresh the statistics, click **REFRESH**. The statistics are refreshed.

Group Membership Table

To display and update the IGMP Group Membership Table, select **IGMP Display > Group Membership Table**. The IGMP Group Membership Table window opens.

Figure 12-41. IGMP Group Membership Table Window



The following parameters are displayed:

Table 12-41. IGMP Group Membership Table Parameters

Field	Description
Select	Select the interface.
Group Member Interface	The virtual interface that is a member of the selected IGMP group.
Group Address	The group address that has members on this interface.
Group Created On	The time at which the group was created on the router.
Group Multicast Protocol	The routing protocol being used for the group. If no routing protocol is being used on the interface a group is on, this field will display IGMP.

Table 12-41. IGMP Group Membership Table Parameters (Continued)

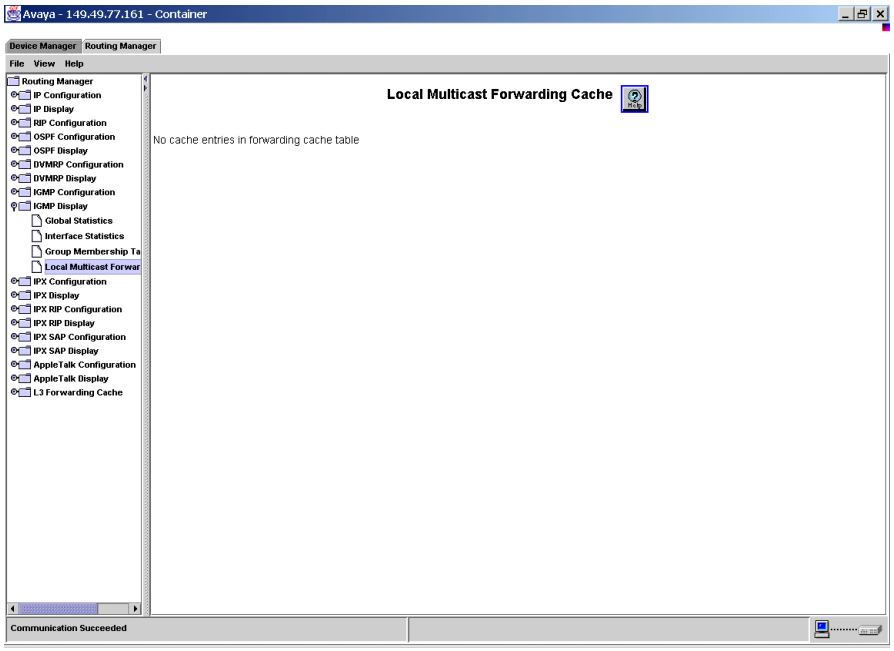
Field	Description
Group Reporter Address	The IP address of the host that sent the most recent host membership report for this group.
Entry Expiration Date	The expiration time, in seconds, of the group that is being displayed.

You can add, modify, or delete IGMP Group Membership parameters. For information, refer to "Modifying Tables" on page 85.

Local Multicast Forwarding Cache

To display the IGMP local multicast forwarding cache, select **IGMP Display > Local Multicast Forwarding Cache**. The IGMP Local Multicast Forwarding Cache window opens.

Figure 12-42. Local Multicast Forwarding Cache Window



The following parameters are displayed:

Table 12-42. Local Multicast Forwarding Cache Parameters

Field	Description
Destination Group Address	The destination group address of the multicast transmission.
Source SubNetwork	The subnet on which the IGMP interface exist.
Source Address Mask	The subnet mask associated with the IGMP source subnetwork.
Upstream Interface	The IP interface configured on the upstream interface.
Invalid Flows from Upstream	The number of invalid flows received from the upstream neighbor.
Packets Forwarded through Cache Entry	The number of packets successfully forwarded in the CPU (supervisor module).

Table 12-42. Local Multicast Forwarding Cache Parameters

Field	Description
Downstream Interface(s)	The number of downstream interfaces.
Upstream Source(s)	The number of upstream interfaces.

13 IPX Routing

This chapter provides instructions for all IPX routing functions using the Avaya P580/P882 Manager. It includes the following sections:

IPX Configuration

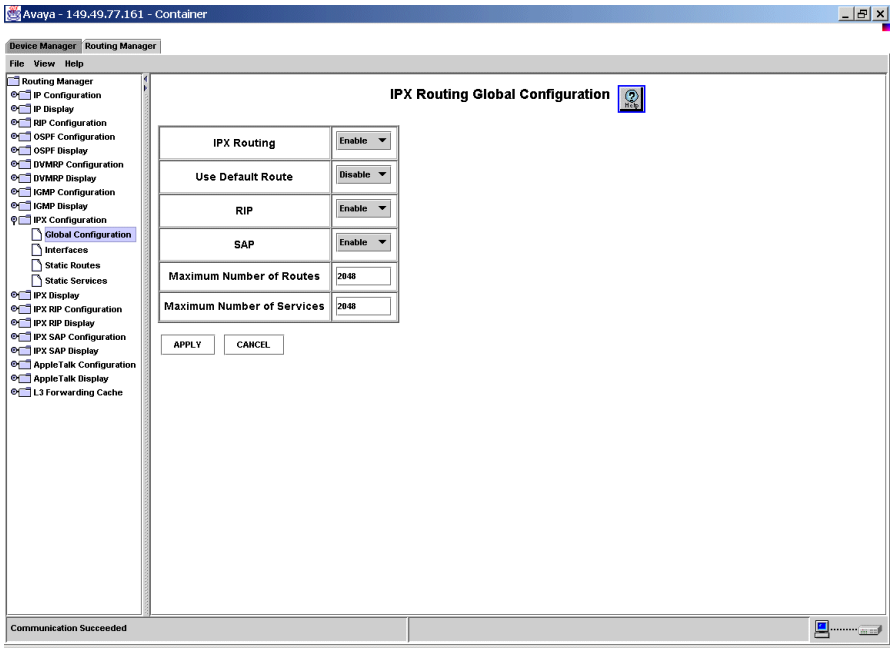
The IP Configuration folder provides access to the following windows:

- **Global Configuration**
- **Interfaces**
- **Static Routes**
- **Static Services**

Global Configuration

To display and update the IPX global configuration, select **IPX Configuration > Global Configuration**. The IPX Global Configuration window opens.

Figure 13-1. IPX Routing Global Configuration Window



The following parameters are displayed:

Table 13-1. IPX Routing Global Configuration Parameters

Field	Description
IPX Routing	The status of IPX Routing. Possible values are: • **Enable** • **Disable**
Use Default Route	The state of IPX route usage. Possible values are: • **Enable** • **Disable** The default value is **Disable**.
RIP	The status of IPX RIP. Possible values are: • **Enable** • **Disable** The default value is **Enable**.

Table 13-1. IPX Routing Global Configuration Parameters

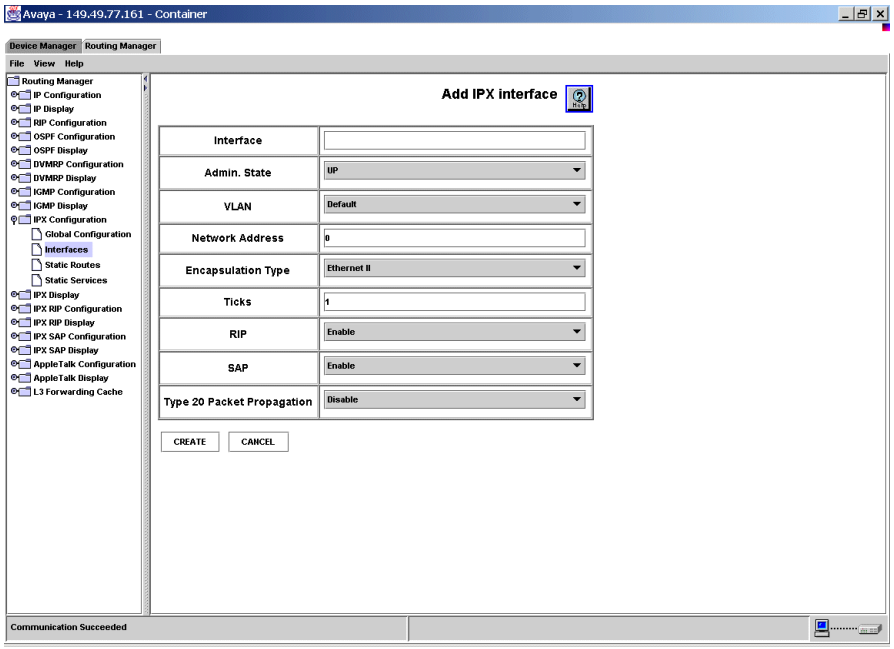
SAP	The status of IPX SAP. Possible values are: • **Enable** • **Disable** The default value is **Enable**.
Maximum Number of Routes	The maximum number of routes that can be added to the routing table. The system rounds out your entry to the nearest power of 2.
Maximum Number of Services	The maximum number of services that can be added to the routing table. The system will round out your entry to the nearest power of 2.

You can modify IPX Global parameters. For information, refer to "Modifying Tables" on page 85.

Interfaces

To display and update the IPX interfaces, select **IPX Configuration > Interfaces**. The IPX Interfaces window opens.

Figure 13-2. IPX Interfaces WIndow



The following parameters are displayed:

Table 13-2. IPX Interface Parameters

Field	Description
Interface	The name of the IPX interface.
Admin State	The current administrator status of the interface. Possible options include: • **Up** • **Down**
VLAN	The VLAN that corresponds to the IPX interface.
Network Address	Displays the address of the network on which the IPX interface resides.

Table 13-2. IPX Interface Parameters (Continued)

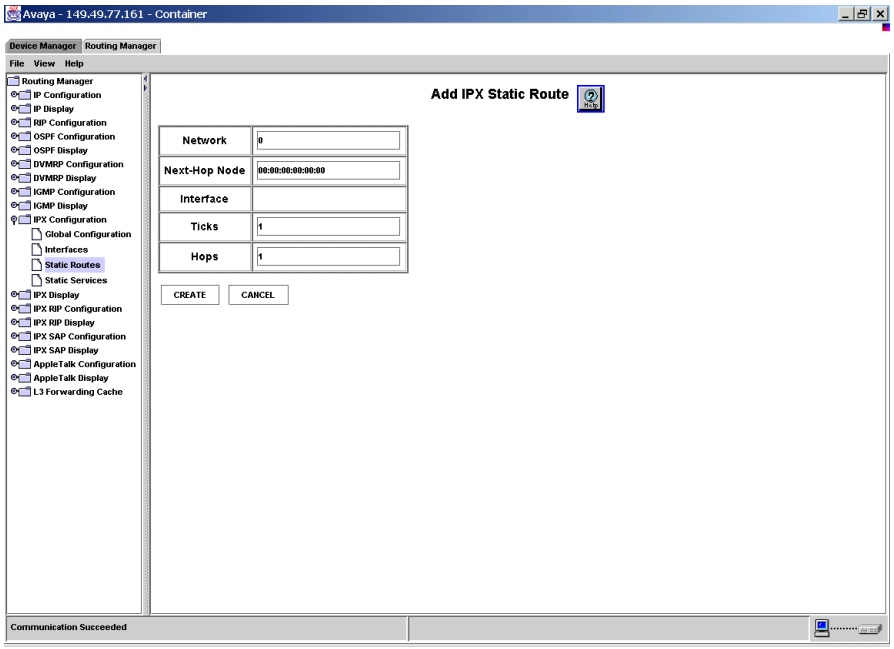
Field	Description
Encapsulation Type	The format of the MAC header on the IPX packets sent by the router on the interface. • **Ethernet II** - MTU = 1500 • **Ethernet SNAP** - MTU =1492 • **Ethernet 802.2** - MTU = 1497 • **Ethernet 802.3** - MTU = 1500
Ticks	The amount of time, in ticks, that a packet takes to reach the network number you specified. A tick is approximately 1/18th of a second.
RIP	The status of IPX RIP on the selected interface.
SAP	The status of IPX SAP on the selected interface.
Type 20 Packet Propagation	The manner in which Type 20 packets are configured on a selected interface. Possible values are: • **Disable** - Type 20 packets are neither sent nor received. • **Inbound** - Type 20 packets received. • **Outbound** - Type 20 packets sent. • **Both** - Type 20 packets sent and received.

You can add, modify, or delete IPX Interfaces. For information, refer to "Modifying Tables" on page 85.

Static Routes

To display and update IPX static routes, select **IPX Configuration > Static Routes**. The IPX Static Route window opens.

Figure 13-3. IPX Static Route Window



The following parameters are displayed:

Table 13-3. IPX Static Route Parameters

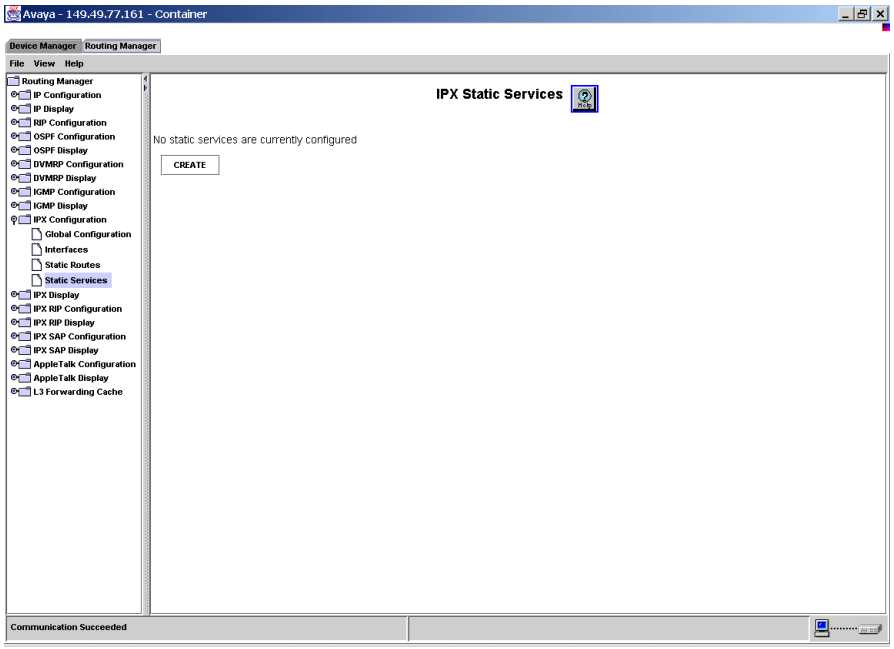
Field	Description
Network	The number of the IPX network (in hex) you want to assign to the IPX static route.
Next-Hop Node	The MAC address of the next destination to which the packet is routed. The format of the value to enter is aa:bb:cc:dd:ee:ff.
Interface	The IPX interface associated with the next hop.
Ticks	The amount of time, in ticks, that the packet takes to reach the network number you specify. A tick is approximately 1/18th of a second.
Hops	The number of routers that the packet must pass through before reaching the network number associated with the IPX network.

You can add, modify, or delete IPX Static Routes. For information, refer to "Modifying Tables" on page 85.

Static Services

To display and update IPX static services, select **IPX Configuration > Static Services**. The IPX Static Services window opens.

Figure 13-4. IPX Static Services Window



The following parameters are displayed:

Table 13-4. IPX Static Services Parameters

Field	Description
Service Name	The name of the IPX static service.
Type	The service type (in hex) that identifies the type of IPX static service the server provides. Possible options include: • **Unknown (0)** • **Print Queue (3)** • **File Server (4)** • **Job Server (5)** • **Print Server (7)** • **Archive Server (9)** • **Remote Bridge Server (24)** • **Advertising Print Server (47)**

Table 13-4. IPX Static Services Parameters (Continued)

Field	Description
Network	The network number (in hex) of the IPX static service.
Node	The node address (in hex) of the IPX static service. The format of the node value is aa:bb:cc:dd:ee:ff.
Socket	The number (in hex) associated with a running process on the end node.
Next-Hop Node	The MAC address of the next destination through which the service is reached. The format of the node value is aa:bb:cc:dd:ee:ff.
Interface	The interface that corresponds to the next-hop node.

You can add, modify, or delete IPX Static Services. For information, refer to "Modifying Tables" on page 85.

IPX Display

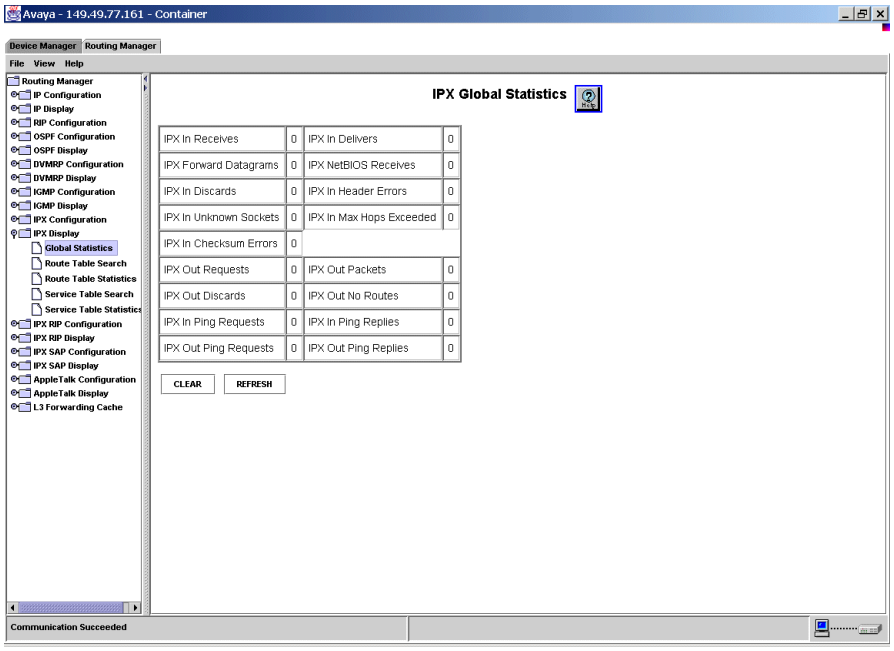
The IPX Display folder provides access to the following windows:

- **Global Statistics**
- **Route Table Search**
- **Route Table Statistics**
- **Service Table Search**
- **Service Table Statistics**

Global Statistics

To display IPX global statistics, select **IPX Display > Global Statistics**. The IPX Global Statistics window opens.

Figure 13-5. IPX Global Statistics Window



The following parameters are displayed:

Table 13-5. IPX Global Statistics Parameters

Field	Description
IPX in Receives	The total number of IPX packets received, including errors.
IPX Forward Datagrams	The number of IPX packets forwarded.
IPX In Discards	The number of IPX packets received and then discarded.
IPX In Unknown Sockets	The number of IPX packets discarded because the destination socket was not open.
IPX in Checksum Errors	The number of IPX packets received with bad checksums.
IPX Out Requests	The Number of IPX packets supplied locally for transmission, not including any packets counted in IPX Forward Datagrams.

Table 13-5. IPX Global Statistics Parameters (Continued)

Field	Description
IPX Out Discards	The number of outgoing IPX packets discarded.
IPX In Ping Requests	The number of received ping requests.
IPX Out Ping Requests	The number of transmitted ping requests.
IPX In Delivers	The total number of IPX packets delivered locally, including packets from local applications.
IPX NetBIOS Receives	The number of NetBIOS packets received.
IPX In Header Errors	The number of IPX packets discarded because of errors in the packet header. This includes packets that are less than the minimum 30 byte length.
IPX in Max Hops Exceeded	The number of IPX packets discarded because the Transport Control field is greater than or equal to 16.
IPX Out Packets	The total number of IPX packets transmitted.
IPX Out No Routes	The number of IPX packets which can not be transmitted because no routes are available.
IPX In Ping Replies	The number of received replies made to ping requests.
IPX Out Ping Replies	The number of transmitted replies made to ping requests.

You can refresh or clear the statistics available in the IPX Global Statistics windows.

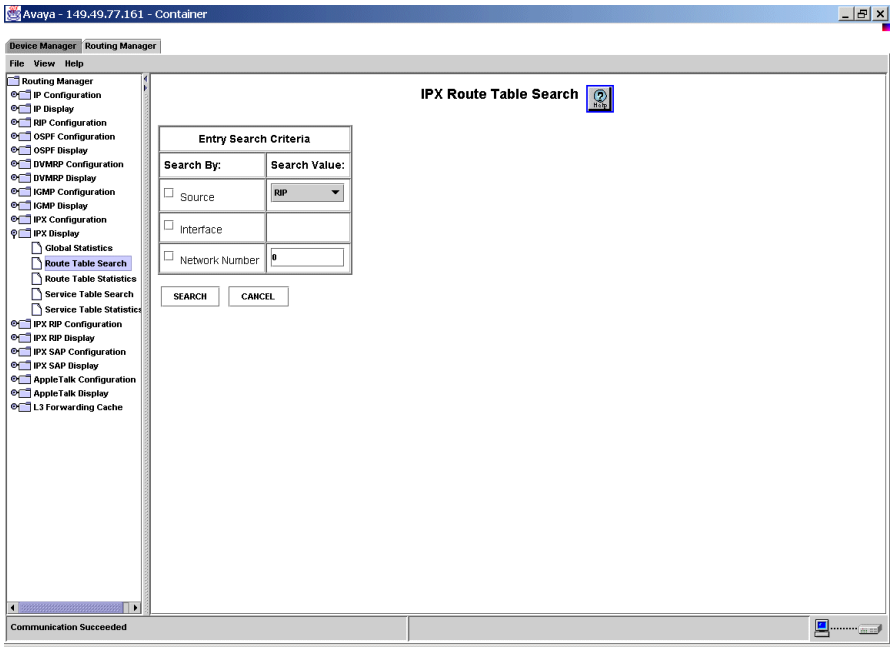
To refresh the statistics, click **REFRESH**. The statistics are refreshed.

To clear the statistics, click **CLEAR**. The statistics are cleared.

Route Table Search

To display and update IPX route table search criteria, select **IPX Display > Route Table Search**. The IPX Route Table Search window opens.

Figure 13-6. IPX Route Table Search Window



The following parameters are displayed:

Table 13-6. IPX Route Table Search Parameters

Field	Description
Source	The method by which the network is learned. • **RIP** - RIP routing updates. • **Static** - User configuration. • **Local** - Directly connected routes.
Interface	The interface associated with next hop to the IPX network.
Network Number	The network number (in hex) of the IPX network to be searched.

To search the IPX routing table:

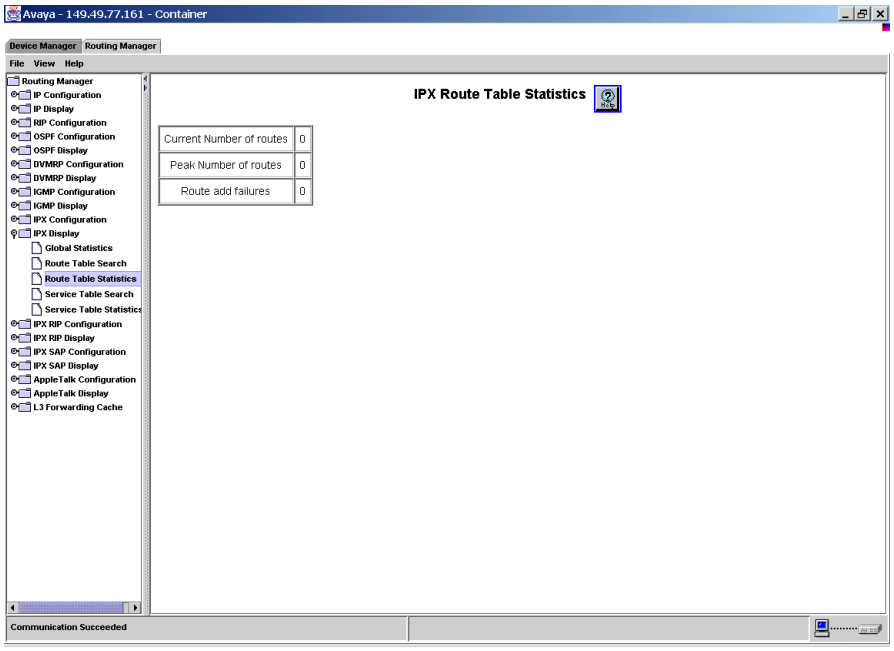
1. Enter the criteria by which you want to search.
2. Ensure that the Search by checkbox next to the criteria is checked.

3. Click **SEARCH**. A window opens in the Table Area with the results of the search.

Route Table Statistics

To display IPX route table statistics, select **IPX Display > Route Table Statistics**. The IPX Route Table Statistics window opens.

Figure 13-7. IPX Route Table Statistics Window



The following parameters are displayed:

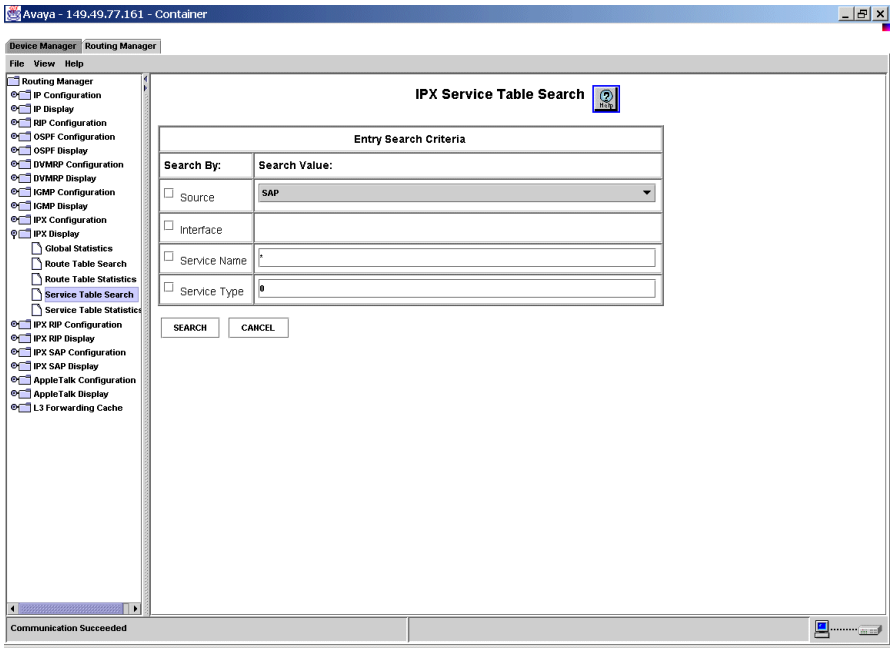
Table 13-7. IPX Route Table Statistics Parameters

Field	Description
Current Number of Routers	The current number of IPX routes.
Peak Number of Routes	The peak number of routes.
Route add failures	The number of route add failures.

Service Table Search

To display and configure IPX service table search criteria, select **IPX Display > Service Table Search**. The IPX Service Table Search window opens.

Figure 13-8. IPX Service Table Search Window



The following parameters are displayed:

Table 13-8. IPX Service Table Search Parameters

Search By	Search Value
Source	The parameter to search the IPX service table. • **SAP** - Services learned via the SAP protocol. • **Static** - User configuration. • **Local** - Local services.
Interface	The interface associated with the next hop to the service.
Service Name	The search value to perform a search based on a specified service name. Use an asterisk (*) as a wildcard.
Service Type	A value based on the specified service type.

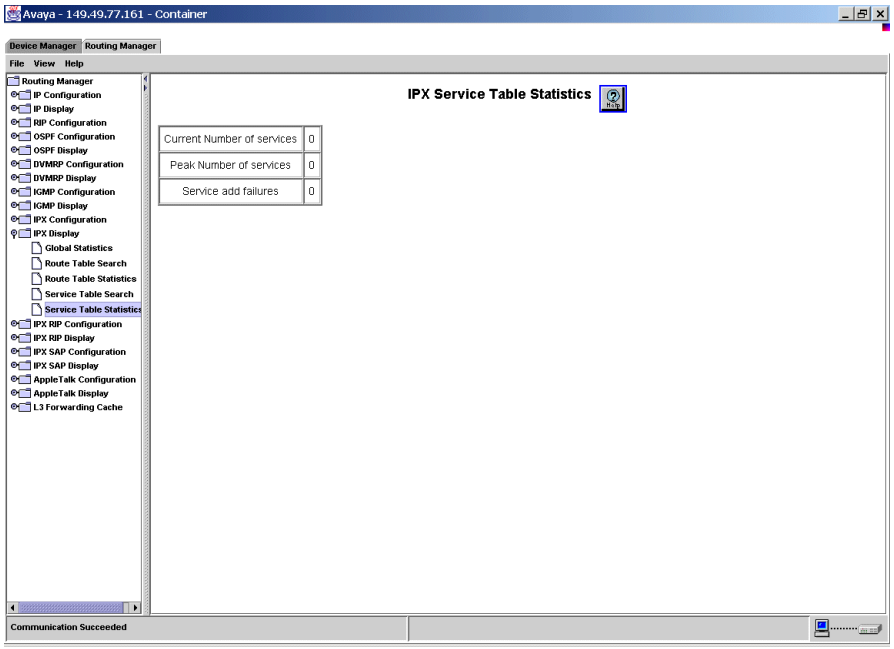
To search for IPX Services:

1. Enter the criteria by which you want to search.
2. Ensure that the Search by checkbox next to the criteria is checked.
3. Click **SEARCH**. A window opens in the Table Area with the results of the search.

Service Table Statistics

To display IPX service table statistics, select **IPX Display > Service Table Statistics**. The IPX Service Table Statistics window opens.

Figure 13-9. IPX Service Table Statistics Window



The following parameters are displayed:

Table 13-9. IPX Service Table Statistics Parameters

Field	Description
Current Number of Services	The current number of IPX services.
Peak Number of Services	The peak number of services.
Service add failures	The number of service add failures.

IPX RIP Configuration

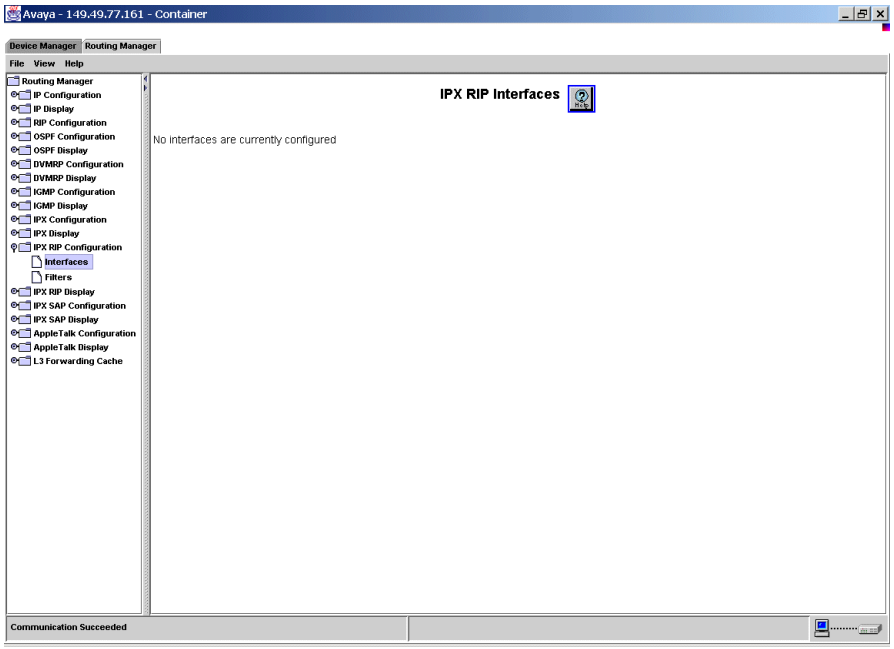
The IPX RIP Configuration folder provides access to the following windows:

- **Interfaces**
- **Filters**

Interfaces

To display and update IPX RIP interfaces, select **IPX RIP Configuration > Interfaces**. The IPX RIP Interfaces window opens.

Figure 13-10. IPX RIP Interfaces Window



The following parameters are displayed:

Table 13-10. IPX RIP Interfaces Parameters

Field	Description
Interface	The IPX interface associated with the RIP interface.
Network Number	The number of the IPX network associated with the interface.
Use Interpacket Gap	The status of RIP updates sent out over an interface. • **Enabled** - IPX RIP provides update packets. • **Disabled** - IPX RIP periodic update packets have no interpacket gap.

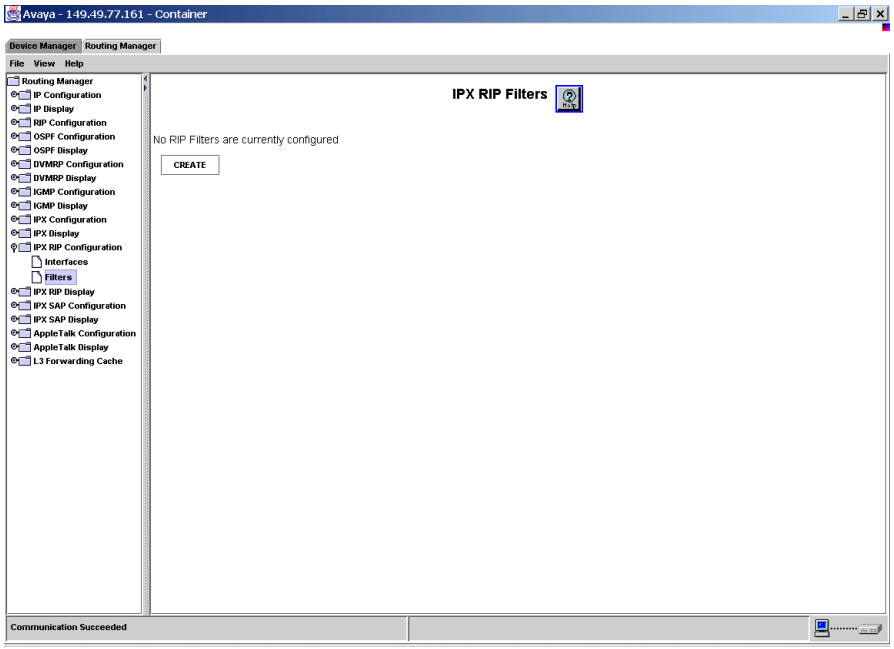
Table 13-10. IPX RIP Interfaces Parameters (Continued)

Field	Description
Use Max Packet Size	The size of the RIP packets sent out an interface. • **Enabled** - RIP packets can contain the maximum allowed by the MTU of the RIP interface. • **Disabled** - RIP packets are limited to 50 network entries.
Periodic Update Interval	The interval, in seconds, at which periodic RIP updates are sent out an interface.
Aging Interval Multiplier	The length of time that information from received RIP updates are kept as a multiplier of the Periodic Update Interval.
Triggered Updates	The status of RIP updates to be immediately transmitted to the network in response to changes in the network topology. Possible values are: • **Enable** • **Disable**
Advertise Default Route Only	The state of advertising the default network exclusively Possible values are: • **Enable** • **Disable**
Mode	The mode for the RIP interface. Possible options include: • **Talk/Listen** - Send and receive advertisements. • **Talk Only** - Send advertisements. • **Listen Only** - Receive advertisements.

Filters

To display the IPX RIP filters, select **IPX RIP Configuration > Filters**. The IPX RIP Filters window opens.

Figure 13-11. IPX RIP Filters Window



The following parameters are displayed:

Table 13-11. IPX RIP Filter Parameters

Field	Description
Interface	The interface to which this filter will be applied to RIP packets sent and/or received on the interface.
Precedence	The filter precedence, where zero is equal to most important. All filters on the same interface must be assigned a unique filter precedence. *** Note:** All RIP filters on the same interface must be assigned a unique precedence value.
Start Network	The first IPX network number in the range.
End Network	The last IPX network number in the range.

Table 13-11. IPX RIP Filter Parameters (Continued)

Field	Description
Direction	The direction of the filter. Possible values are: • **Inbound** - Apply the filter only to RIP packets received on the interface. • **Outbound** - Apply the filter only to RIP packets sent on the interface. • **Both** - Apply the filter to RIP packets both sent and received on the interface.
Filter/Suppress	The status of the filter on the interface. Possible values are: • **Enabled** • **Disabled**
Ticks	The amount of time, in ticks, that the packet takes to reach the specified network number.
Hops	The number of routers that the packet must pass through before reaching the network number associated with the IPX interface. Entering 0 ensures that there is no override in the transmission of data on the network.

You can add, modify, or delete IPX RIP Filters. For information, refer to "Modifying Tables" on page 85.

IPX RIP Display

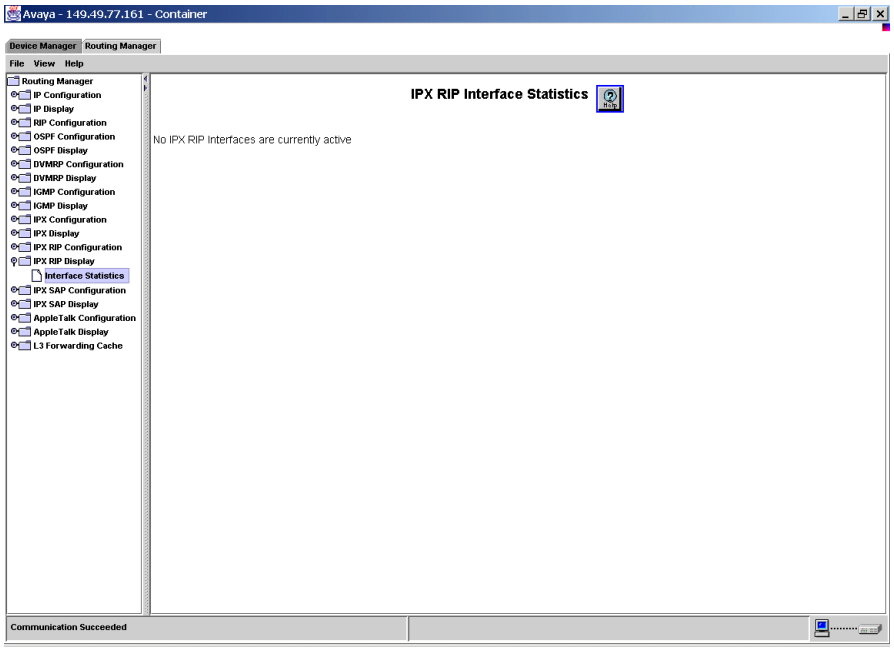
The IPX RIP Display folder provides access to the following window:

- **Interface Statistics**

Interface Statistics

To display IPX RIP interface statistics, select **IPX RIP Display > Interface Statistics**. The IPX RIP Interface Statistics window opens.

Figure 13-12. IPX RIP Interface Statistics Window



The following parameters are displayed:

Table 13-12. IPX RIP Interface Statistics Parameters

Field	Description
Interface	The interface associated with this RIP interface.
State	The current state of the RIP interface.
Network Number	The network number of the IPX network associated with the interface.
Trigger Updates Sent	The number of triggered updates sent from the RIP interface.
Non-triggered Updates Sent	The number of non-triggered updates sent from the RIP interface.
Updates Received	The number of updates received by the RIP interface. Updates may be received periodically even if no changes have occurred.
Requests Received	The number of requests for updates received by the RIP interface.

Table 13-12. IPX RIP Interface Statistics Parameters (Continued)

Field	Description
Bad Packets Received	The number of bad packets received by the RIP interface.

You can refresh or clear the statistics available in the IPX RIP Interface Statistics windows. To refresh the statistics, click **REFRESH**. The statistics are refreshed.

IPX SAP Configuration

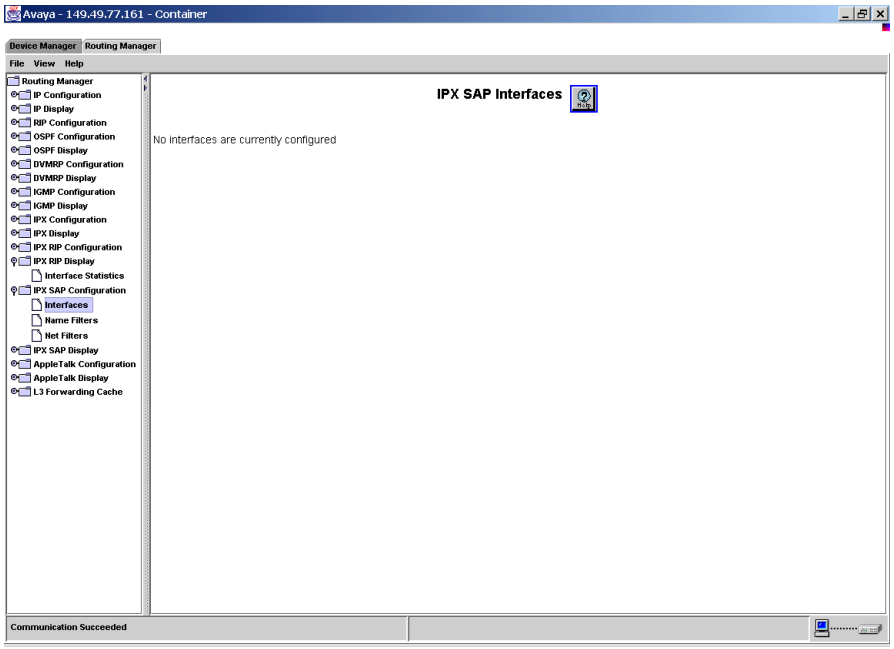
The IPX SAP Configuration folder provides access to the following windows:

- **Interfaces**
- **Name Filters**
- **Net Filters**

Interfaces

To display and update IPX SAP interfaces, select **IPX SAP Configuration > Interfaces**. The IPX SAP Interfaces window opens.

Figure 13-13. IPX SAP Interfaces Window



The following parameters are displayed:

Table 13-13. IPX SAP Interfaces Parameters

Field	Description
Interface	The IPX interface associated with the SAP interface.
Network Number	The number of the IPX network associated with the interface.
Use Interpacket Gap	The status of SAP updates sent out over an interface. • Enabled - IPX SAP provides update packets. • Disabled - IPX SAP periodic update packets have no interpacket gap.

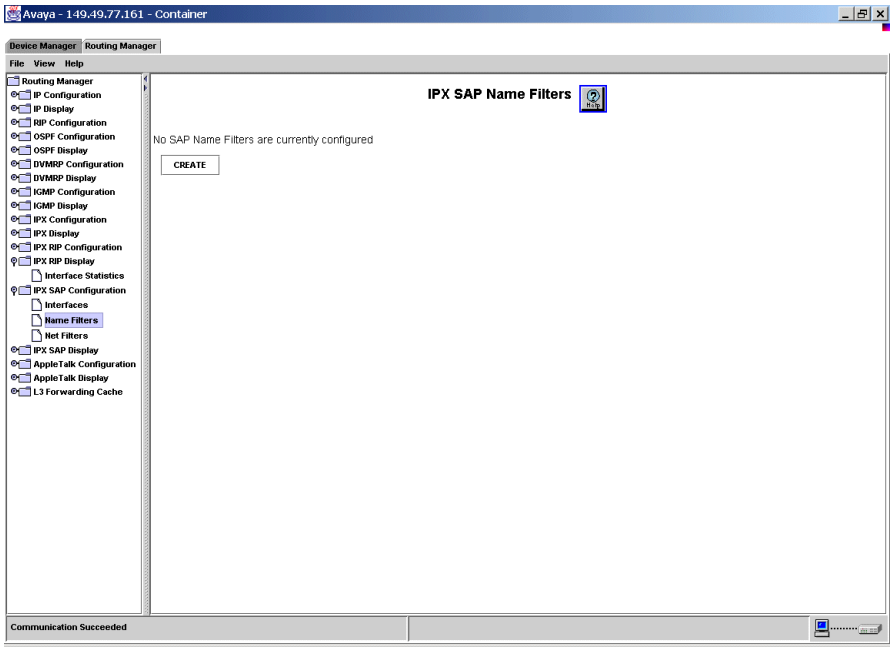
Table 13-13. IPX SAP Interfaces Parameters (Continued)

Field	Description
Use Max Packet Size	The size of the SAP packets sent out an interface. • Enabled - SAP packets can contain the maximum allowed by the MTU of the RIP interface. • Disabled - SAP packets are limited to 50 network entries.
Periodic Update Interval	The interval, in seconds, at which periodic SAP updates are sent out an interface.
Aging Interval Multiplier	The length of time that information from received SAP updates are kept as a multiplier of the Periodic Update Interval.
Triggered Updates	The status of SAP updates to be immediately transmitted to the network in response to changes in the network topology. Possible values are: • Enable • Disable
Get Nearest Server Reply	The status of server reactions to Get Nearest Server requests received on the interface. Possible values are: • Enable • Disable
Get Nearest Server Reply Delay	The delay, in msecs, to wait before responding to a Get Nearest Service request received on the interface.
Mode	The mode for the SAP interface.Possible options include: • Talk/Listen - Send and receive advertisements. • Talk Only - Send advertisements. • Listen Only - Receive advertisements.

Name Filters

To display and update IPX SAP name filters, select **IPX SAP Configuration > Name Filters**. The IPX SAP Name Filters window opens.

Figure 13-14. IPX SAP Name Filter Window



The following parameters are displayed:

Table 13-14. IPX SAP Name Filter Parameters

Field	Description
Precedence	The filter precedence with 0 equal to most important. *** Note:** All SAP filters on the same interface, must be assigned a unique filter precedence.
Name	The service name. A single asterisk may be present as the last character, which will match all remaining characters of a service name.

Table 13-14. IPX SAP Name Filter Parameters (Continued)

Field	Description
Type	The type (in hex) of service the server provides. Possible values are: • **Unknown (0)** • **Print Queue (3)** • **File Server (4)** • **Job Server (5)** • **Print Server (7)** • **Archive Server (9)** • **Remote Bridge Server (24)** • **Advertising Print Server (47)** • **NetWare Directory Services [NDS] (278)** • **fff** - all service type values.
Direction	The direction of the filter. Possible options include: • **Inbound** - Apply the filter only to SAP packets received on the interface. • **Outbound** - Apply the filter only to SAP packets sent on the interface. • **Both** - Apply the filter to SAP packets both sent and received on the interface.
Filter/Suppress	The status IPX networks within the specified range in the filter to be filtered (inbound) or suppressed (outbound). Possible values are: • **Filtered** - Apply the filter only to SAP packets received (inbound direction) on the interface. • **Suppressed** - Apply the filter only to SAP packets sent (outbound direction) on the interface. • **Enable** - Enable the filtering and suppression of traffic. • **Disable** - Disable the filtering and suppression of traffic.

Table 13-14. IPX SAP Name Filter Parameters (Continued)

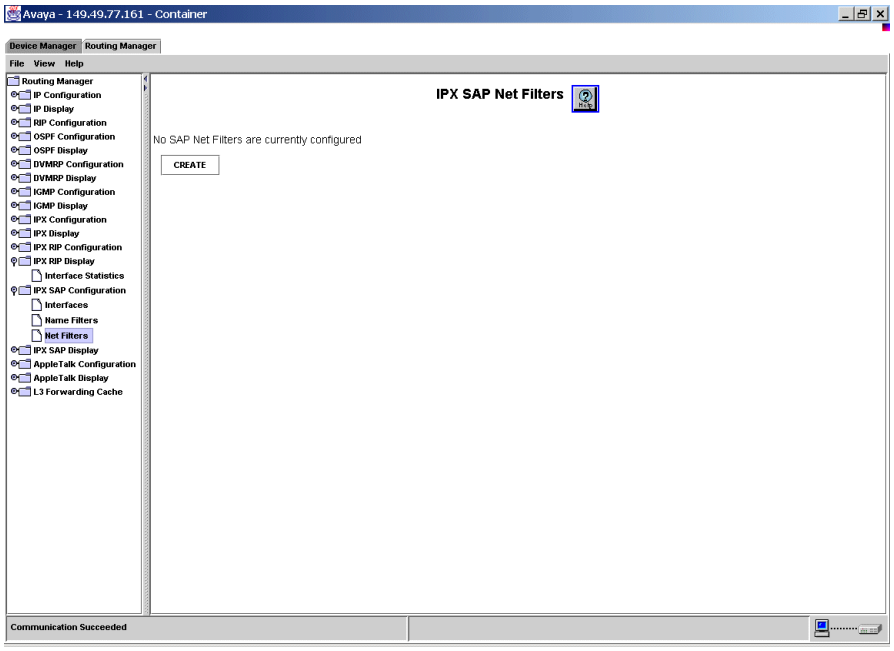
Field	Description
Hops	The number of routers that the packet must pass through before reaching the services matched by the filter. This entry is used to override the value in the SAP packet.Entering 0 ensures that there is no override in the transmission of data on the network.

You can add, modify, or delete IPX SAP Name Filters. For information, refer to "Modifying Tables" on page 85.

Net Filters

To display and update IPX SAP net filters, select **IPX SAP Configuration > Net Filters**. The IPX SAP Net Filters window opens.

Figure 13-15. IPX SAP Net Filter Window



The following parameters are displayed:

Table 13-15. IPX SAP Net Filter Parameters

Field	Description
Interface	The interface to which this filter will be applied to SAP packets sent and/or received on the interface.
Precedence	The filter precedence where zero is equal to most important. All filters on the same interface must be assigned an unique filter precedence.
Net	The network on which the server resides. A network number of ffffffff represents all networks.

Table 13-15. IPX SAP Net Filter Parameters (Continued)

Field	Description
Type	The type (in hex) of service the server provides. Possible values are: • **Unknown (0)** • **Print Queue (3)** • **File Server (4)** • **Job Server (5)** • **Print Server (7)** • **Archive Server (9)** • **Remote Bridge Server (24)** • **Advertising Print Server (47)** • **NetWare Directory Services [NDS] (278)**

You can add, modify, or delete IPX SAP Net Filters. For information, refer to "Modifying Tables" on page 85.

IPX SAP Display

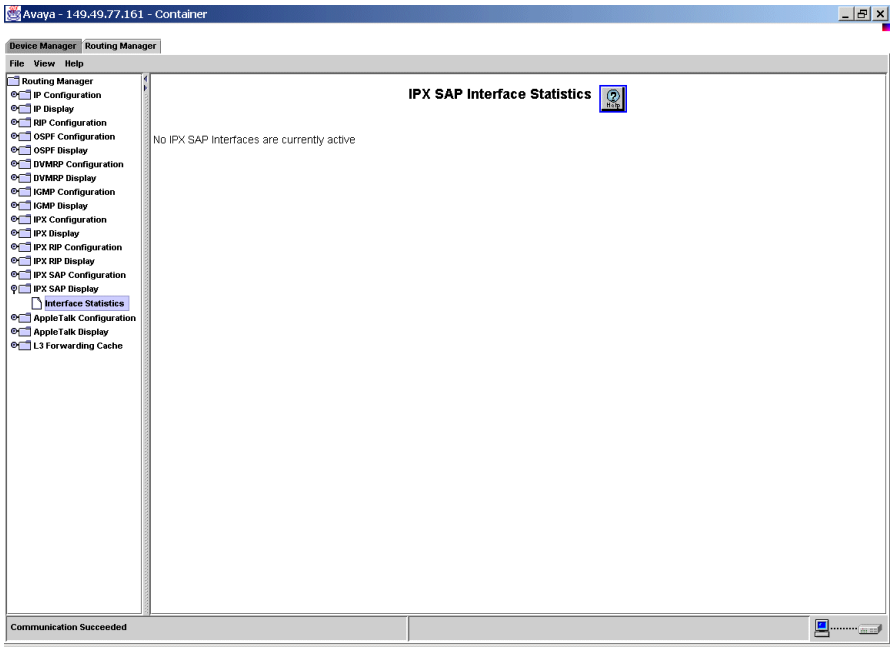
The IPX SAP Display folder provides access to the following window:

- **Interface Statistics**

Interface Statistics

To display IPX SAP interface statistics, select **IPX SAP Display > Interface Statistics**. The IPX SAP Interface Statistics window opens.

Figure 13-16. IPX SAP Interface Statistics Window



The following parameters are displayed:

Table 13-16. IPX SAP Interface Statistics Parameters

Field	Description
Interface	The interface associated with this SAP interface.
State	The current state of the SAP interface.
Network Number	The network number of the IPX network associated with the interface.
Trigger Updates Sent	The number of triggered updates sent from the SAP interface.
Non-Triggered Updates Sent	The number of non-triggered updates sent from the SAP interface.
GNS Responses Sent	The number of GNS responses sent from the SAP interface.
Updates Received	The number of updates received on the SAP interface.

Table 13-16. IPX SAP Interface Statistics Parameters (Continued)

Field	Description
Requests Received	The number of requests received on the SAP interface.
GNS Requests Received	The number of requests received on the SAP interface.
Bad Packets Received	The number of bad packets received on the SAP interface.

You can refresh or clear the statistics available in the IPX SAP Interface Statistics windows. To refresh the statistics, click **REFRESH**. The statistics are refreshed.

14 AppleTalk Routing

This chapter provides instructions for all AppleTalk routing functions using the Avaya P580/P882 Manager. It includes the following sections:

AppleTalk Configuration

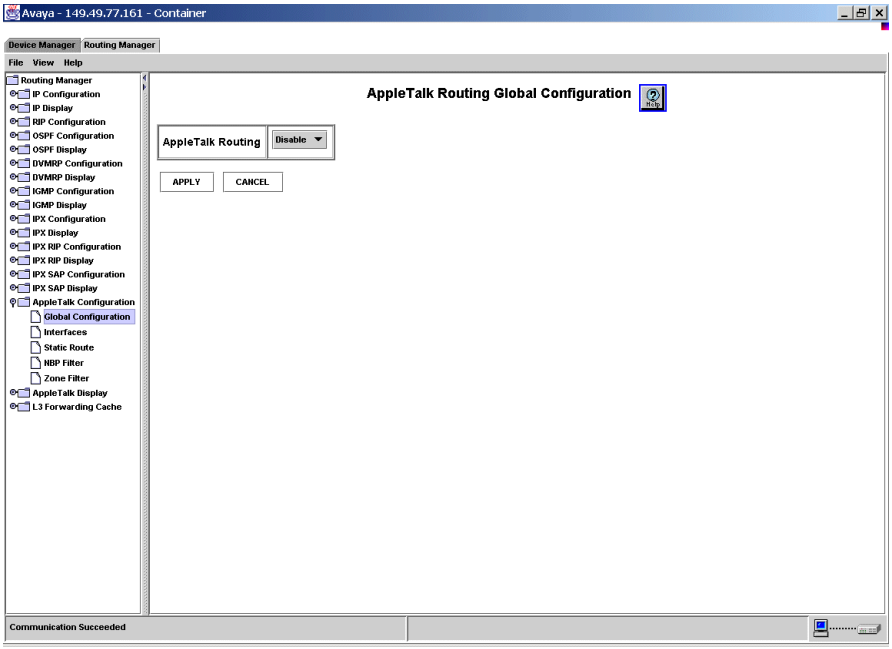
The AppleTalk Configuration folder provides access to the following windows:

- **Global Configuration**
- **Interfaces**
- **Static Route**
- **NBP Filter**
- **Zone Filter**

Global Configuration

To display and update the AppleTalk global configuration, select **AppleTalk Configuration > Global Configuration**. The AppleTalk Routing Global Configuration window opens.

Figure 14-1. Global Configuration Window



The following parameter is displayed:

Table 14-1. AppleTalk Routing Global Configuration Parameter

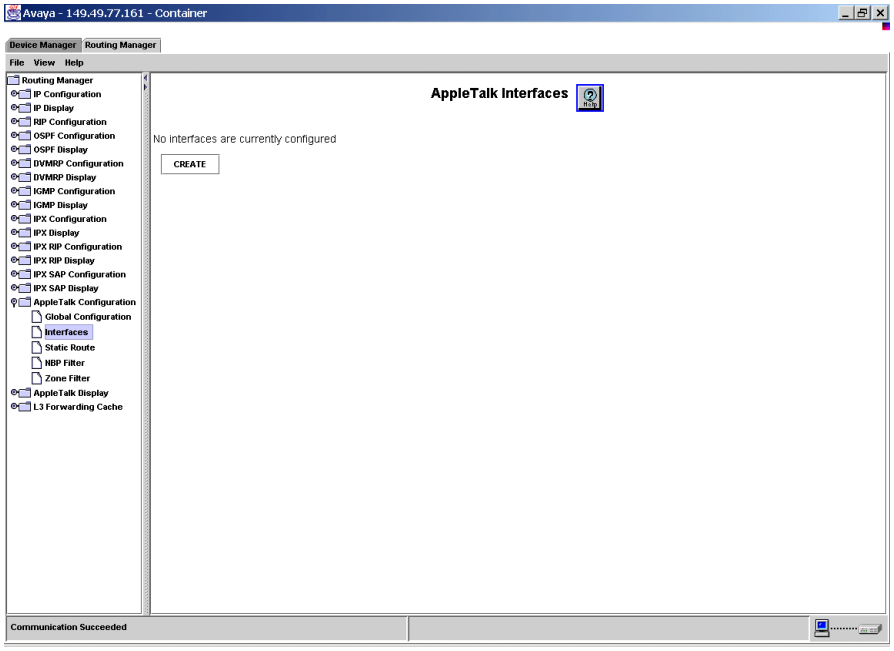
Field	Description
AppleTalk Routing	The state of AppleTalk Routing. Possible values are: • **Enable** - AppleTalk Routing is enabled. This is the default. • **Disable** - AppleTalk Routing is disabled.

You can modify the Appletalk Routing Global Configuration parameter. For information, refer to "Modifying Tables" on page 85.

Interfaces

To display and configure AppleTalk interfaces, select **AppleTalk Configuration > Interfaces**. The AppleTalk Interfaces window opens.

Figure 14-2. AppleTalk Interfaces Window



The following parameters are displayed:

Table 14-2. AppleTalk Interfaces Parameter

Field	Description
Interface	The interface associated with AppleTalk.
VLAN	The VLAN to be associated with the interface. Possible options include: • **Default** • **Discard**
Metric	The metric associated with the AppleTalk interface.
Encapsulation Type	The format of the MAC header on the AppleTalk packets sent by the router on the interface. Possible options include: • **Ethernet II** - MTU = 1500 • **Ethernet SNAP** - MTU =1492

Table 14-2. AppleTalk Interfaces Parameter (Continued)

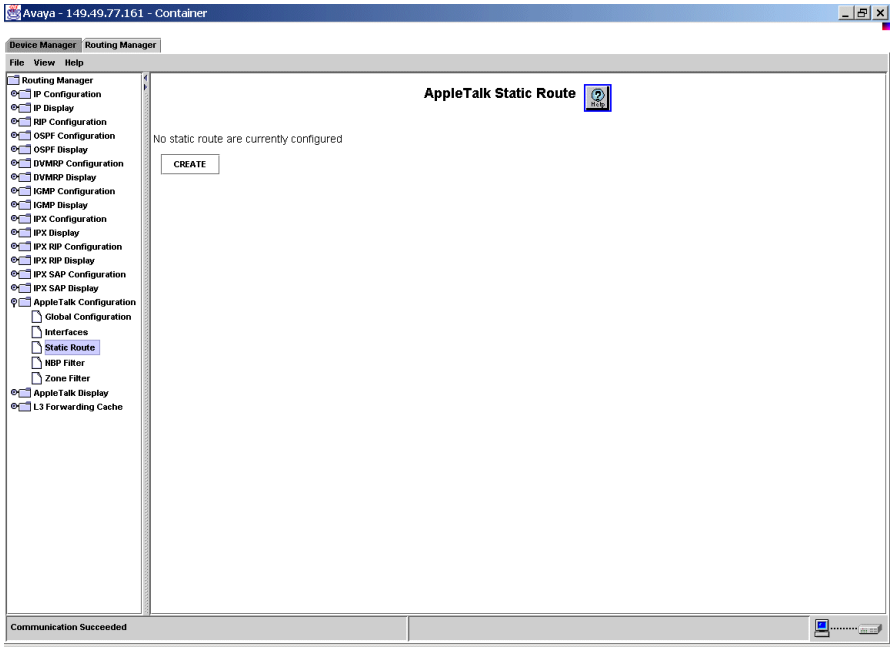
Field	Description
Network Range End	The ending network number. The network number specifies the range of AppleTalk network numbers for extended networks. Each number in the range must be an integer between 0 and 65279. *** Note:** If the Network Range Start value equals zero, the Network Range End value must also equal zero.
Network Number	The interface network number. This number specifies the network number the interface is using. *** Note:** This value must be within the Network Range or be equal to zero.
Node	The interface node identification number. The value for this field must be between 0 and 253.
Admin State	The status of administrator state. The administrator state determines if the interface is operational from a management point of view. Possible values are: • **Enable** • **Disable**
Zone	The default AppleTalk zone to be used by this interface. Zone names may be up to 32 characters in length.

You can add, modify, or delete AppleTalk Interfaces. For information, refer to "Modifying Tables" on page 85.

Static Route

To display and update the AppleTalk Static Routes, select **AppleTalk Configuration > Static Routes**. The AppleTalk Static Route window opens.

Figure 14-3. AppleTalk Static Route Window



The following parameters are displayed:

Table 14-3. AppleTalk Static Route Parameters

Field	Description
Network Range Start	The starting network number. The network number specifies the range of AppleTalk network numbers for extended networks. The numbers range between 1 through 65279. *** Note:** The Network Range Start value must be less than or equal to the Network Range End value.
Network Range End	The ending network number.
Network Number	The interface network number. This number specifies the network number of the next hop router for the network range.
Node	The interface node identification number. This number must be between 1 and 253.

Table 14-3. AppleTalk Static Route Parameters (Continued)

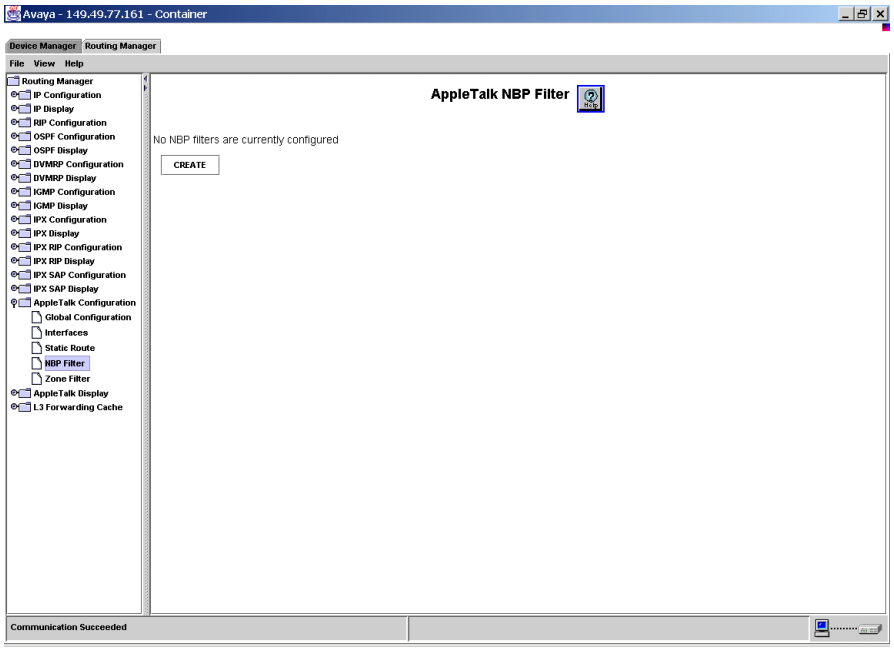
Field	Description
Type	The type of static route. Possible values are: • **High** - The static route is not superseded by a route update. • **Low** - The static route can be superseded by a route update.
Zone	The AppleTalk zone name assigned to this route. Zone names may be up to 32 characters in length.

You can add, modify, or delete AppleTalk Static Routes. For information, refer to "Modifying Tables" on page 85.

NBP Filter

To display and update the AppleTalk NBP Table, select **AppleTalk Configuration > NBP Table**. The AppleTalk NBP Filter window opens.

Figure 14-4. AppleTalk NBP Filter Window



The following parameters are displayed:

Table 14-4. AppleTalk NBP Filter Parameters

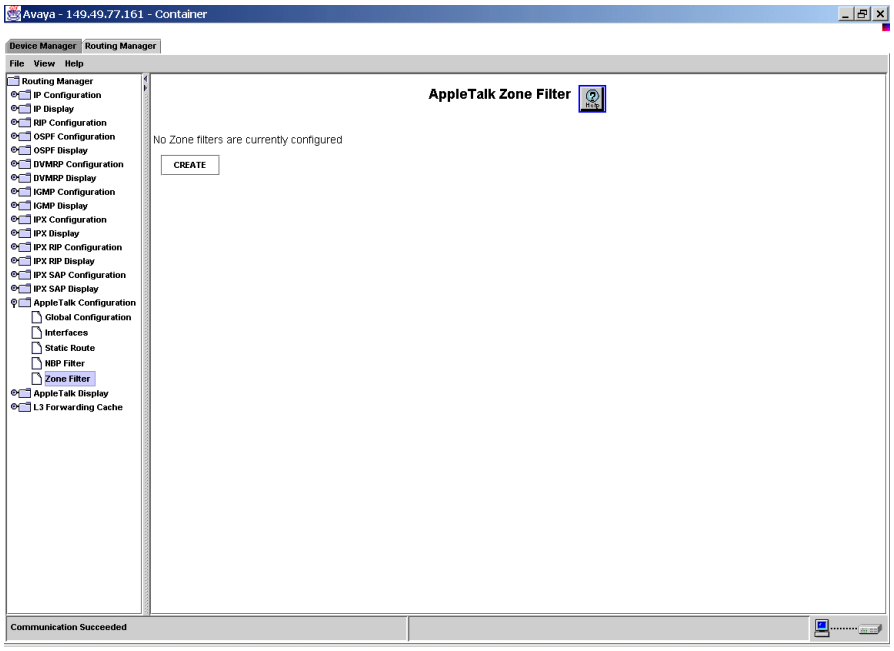
Field	Description
Access List	The access list number to be associated with the NBP filter. Possible values are between 600 through 631.
Name	The name of the NBP name object to be filtered.
Type	The type of filtering. The type field generally identifies the type of serronic mailbox on a server. Possible values are: • **Permit** • **Deny**
Interface	Select the interface(s) to apply this filter to.

You can add, modify, or delete AppleTalk NBP Filters. For information, refer to "Modifying Tables" on page 85.

Zone Filter

To display the AppleTalk Zone Filter window, select **AppleTalk Configuration > Zone Filter**. The AppleTalk Zone Filter window opens.

Figure 14-5. AppleTalk Zone Filter Window



The following parameters are displayed:

Table 14-5. AppleTalk Zone Filter Parameters

Field	Description
Access List	The access list number to be associated with the zone filter. Valid values are 632-663.
Name	The name of the AppleTalk zone filter.
Type	The type of filtering. Possible options include: • **Deny** • **Permit**
Interface	The interface on which to apply this filter.

You can add, modify, or delete AppleTalk Zone Filters. For information, refer to "Modifying Tables" on page 85.

AppleTalk Display

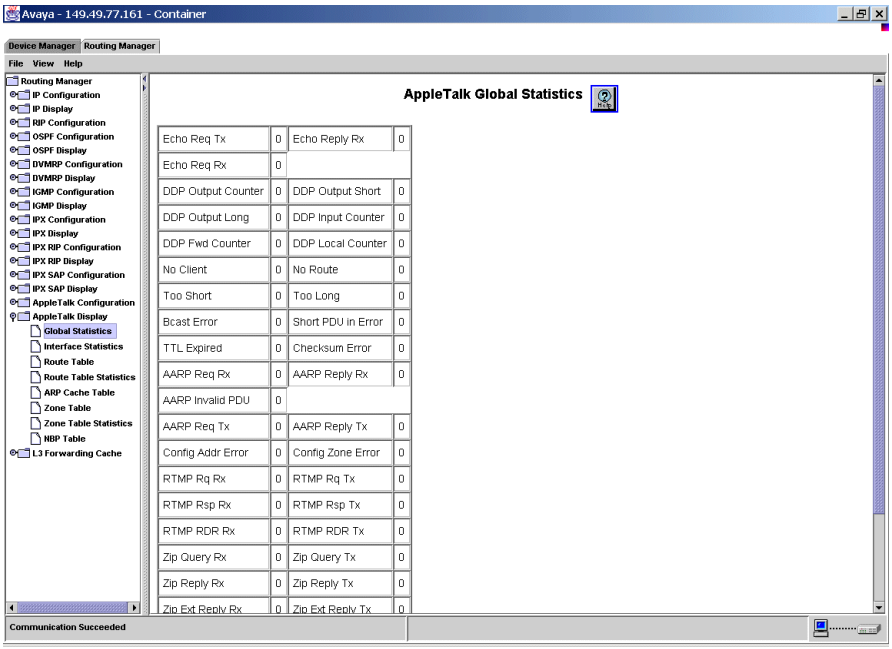
The Apple Talk Display folder provides access to the following windows:

- **Global Statistics**
- **Interface Statistics**
- **Route Table**
- **Route Table Statistics**
- **ARP Cache Table**
- **Zone Table**
- **Zone Table Statistics**
- **NBP Table**

Global Statistics

To display AppleTalk global statistics, select **AppleTalk Display > Global Statistics**. The AppleTalk Global Statistics window opens.

Figure 14-6. AppleTalk Global Statistics Window



The following parameters are displayed:

Table 14-6. AppleTalk Global Statistics Parameters

Parameter	Number of...	Parameter	Number of...
Echo Req Tx	Echo requests transmitted.	**Checksum Error**	Packets which had checksum in error.
Echo Req Rx	Echo requests received.	**AARP Reply Rx**	AppleTalk ARP replies received.
DDP Output Counter	DDP packets sent from this node.	**AARP Reply Tx**	AppleTalk ARP replies transmitted.
DDP Output Long	DDP packets sent using the long format.	**Config Zone Error**	Zone configuration errors detected.
DDP Fwd Counter	DDP packets forwarded through this node.	**RTMP Rq Rx**	RTMP requests received

Table 14-6. AppleTalk Global Statistics Parameters (Continued)

No Client	Packets received for which the destination socket was not known.	**RTMP Rq Tx**	RTMP requests transmitted.
Too Short	Packets received that were smaller than the minimum size allowed for an AppleTalk packet.	**RTMP Rsp Rx**	RTMP responses received.
Bcast Error	Broadcast errors detected.	**RTMP Rsp Tx**	RTMP responses transmitted.
TTL Expired	Packets dropped because they timed out.	**RTMP RDR Rx**	RTMP route data requests received.
AARP Req Rx	AppleTalk ARP requests received.	**RTMP RDR Tx**	RTMP route data requests transmitted.
AARP Invalid PDU	AppleTalk ARP requests received which were invalid.	**Zip Query Rx**	Zip queries received.
AARP Req Tx	AppleTalk ARP requests transmitted.	**Zip Query Tx**	Zip queries transmitted.
Config Addr Error	Configuration address errors detected.	**Zip Reply Rx**	Zip replies received.
Echo Reply Rx	Echo replies received.	**Zip Reply Tx**	Zip replies transmitted.
DDP Output Short	DDP packets sent using the short format.	**Zip Ext Reply Rx**	Zip extended replies received.
DDP Input Counter	DDP packets received.	**Zip Ext Reply Tx**	Zip extended replies transmitted.
DDP Local Counter	DDP packets received destined for this node.	**Zip GNI Rq Rx**	Zip get net info request received.
No Route	DDP packets for which no route existed to the destination.	**Zip GNI Rq Tx**	Zip get net info request transmitted.

Table 14-6. AppleTalk Global Statistics Parameters (Continued)

Too Long	Packets received that were larger than the maximum size allowed.	**Zip GNI Rsp Rx**	Zip get net info response received.
Short PDU in Error	Packets that have short PDUs in error.	**Zip GNI Rsp Tx**	Zip get net info response transmitted.

You can refresh or clear the statistics available in the Appletalk Global Statistics windows.

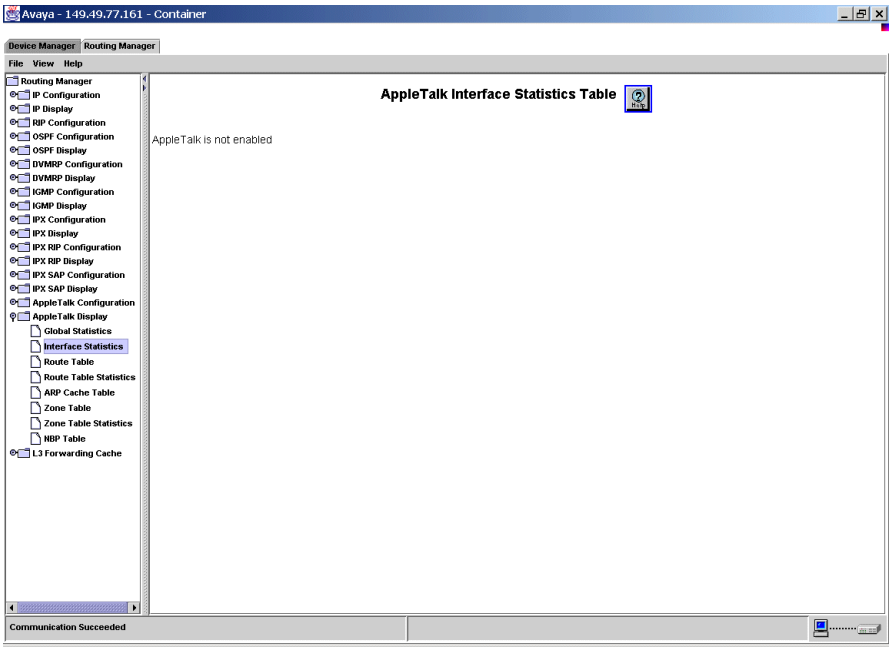
To refresh the statistics, click **REFRESH**. The statistics are refreshed.

To clear the statistics, click **CLEAR**. The statistics are cleared.

Interface Statistics

To display AppleTalk interface statistics, select **AppleTalk Display > Interface Statistics**. The AppleTalk Interface Statistics window opens.

Figure 14-7. AppleTalk Interface Statistics WIndow



The following parameters are displayed:

Table 14-7. AppleTalk Interface Statistics Parameters

Field	Description
Interface	The name assigned to the selected AppleTalk interface.
Network Range	The network range associated with the AppleTalk interface.
Network Number	The network number of this node.
Node	The node number of this node.
Seed	Displays whether the AppleTalk interface seeded the network.

Table 14-7. AppleTalk Interface Statistics Parameters (Continued)

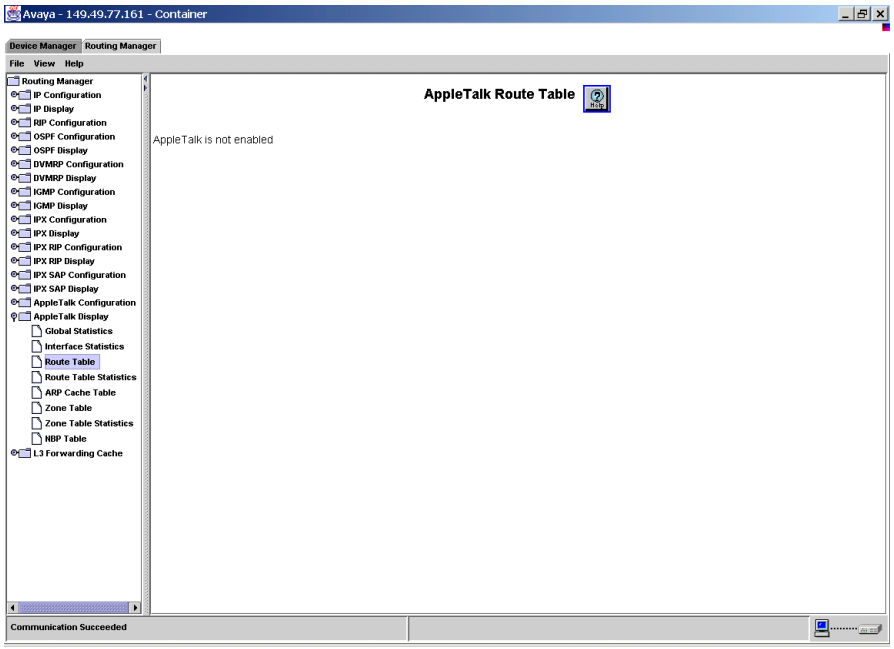
Field	Description
State	The state of the AppleTalk interface. Possible values are: • **Up** - indicates that the AppleTalk interface is active. • **Down** - indicates that the AppleTalk interface is inactive.

You can refresh the statistics available in the AppleTalk Interfaces Statistics windows. To refresh the statistics, click **REFRESH**. The statistics are refreshed.

Route Table

To display the AppleTalk route table configuration, select **AppleTalk Display > Route Table**. The AppleTalk Route Table window opens.

Figure 14-8. Route Table Window



The following parameters are displayed:

Table 14-8. Route Table Parameters

Field	Description
Select	Select the AppleTalk route table entry to be acted upon.
Network Range	Displays the network range.
Metric	The port metric for the network range.
State	The state of the entry. Possible values are: • **Good** • **Suspect** • **Going Bad** • **Bad**

Table 14-8. Route Table Parameters (Continued)

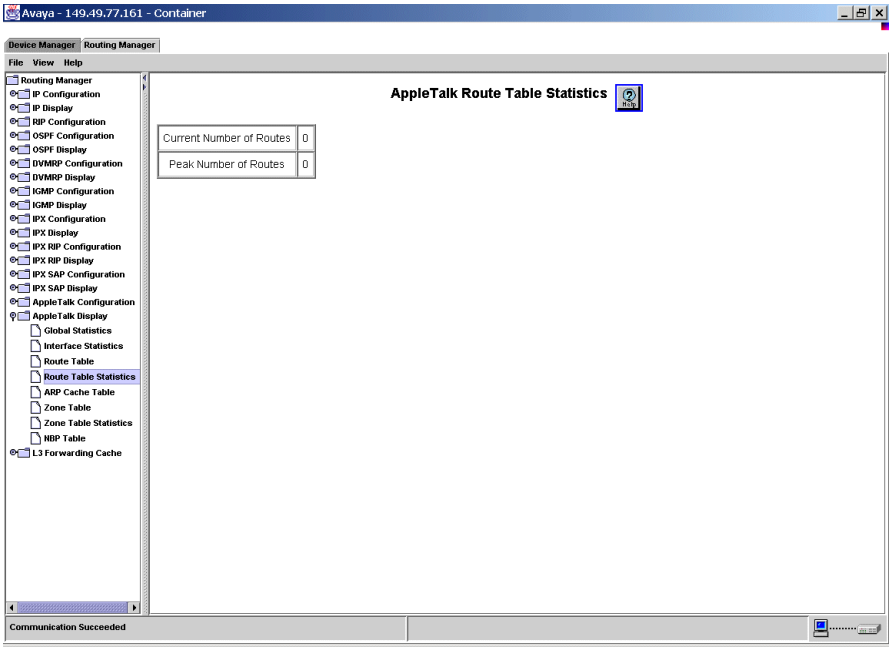
Field	Description
Owner	Displays the AppleTalk component responsible for the addition of the route. Possible values are: • **Local** • **Staticx** • **RTMP**
Next Hop	The next hop address where forwarded packets are routed.
Interface	The interface associated with the route table entry.
Zones	The zone associated with the selected AppleTalk route.

You can add, modify, or delete AppleTalk Route Table entries. For information, refer to "Modifying Tables" on page 85.

Route Table Statistics

To display AppleTalk route table statistics, select **AppleTalk Display > Route Table Statistics**. The AppleTalk Route Table Statistic window opens.

Figure 14-9. Route Table Statistics Window



The following parameters are displayed:

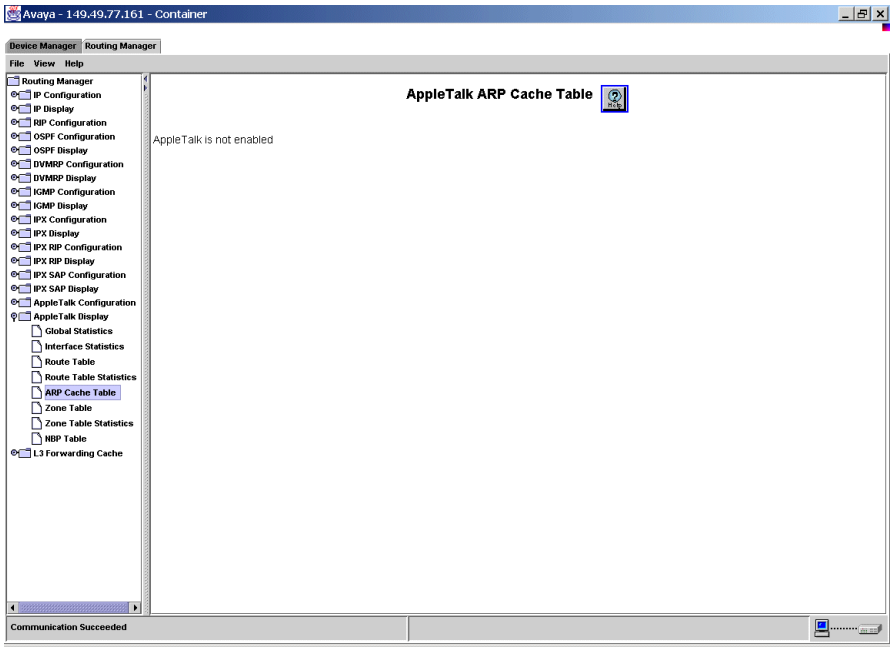
Table 14-9. Route Table Statistics Parameters

Field	Description
Current Number of Routes	The current number of AppleTalk routes.
Peak Number of Routes	The peak number of AppleTalk routes.

ARP Cache Table

To display the AppleTalk cache table configuration, select **AppleTalk Display > ARP Cache Table**. The AppleTalk ARP Cache Table window opens.

Figure 14-10. ARP Cache Table Window



The following parameter is displayed:

Table 14-10. ARP Cache Table Parameters

Field	Description
Select	The AppleTalk ARP cache table entry to be acted upon.
Network Range	Displays the network range.
Node	Displays the node number for the entry.
MAC Address	Displays the MAC address associated with the AppleTalk ARP cached table entry.
Interface	Displays the interface associated with the ARP cache table entry.

Table 14-10. ARP Cache Table Parameters (Continued)

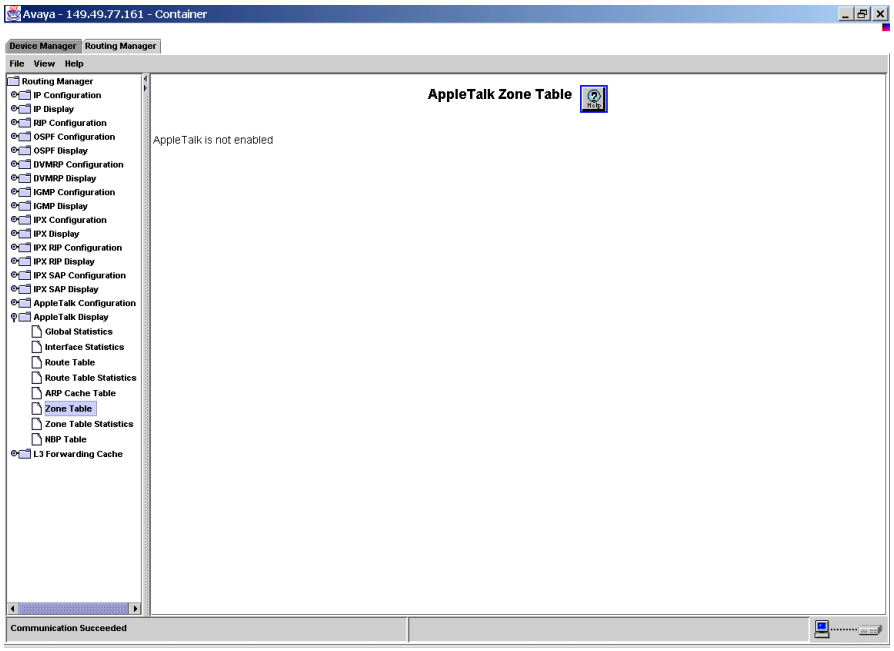
Field	Description
Type	Displays the type of ARP cache table entries. Possible values are: • **Local** • **Broadcast** • **Dynamicx** • **Router Neighbor**

You can modify AppleTalk ARP Cache entries. For information, refer to "Modifying Tables" on page 85.

Zone Table

To display AppleTalk zone table configuration, select **AppleTalk Display > Zone Table**. The AppleTalk Zone Table window opens.

Figure 14-11. Zone Table Window



The following parameters are displayed:

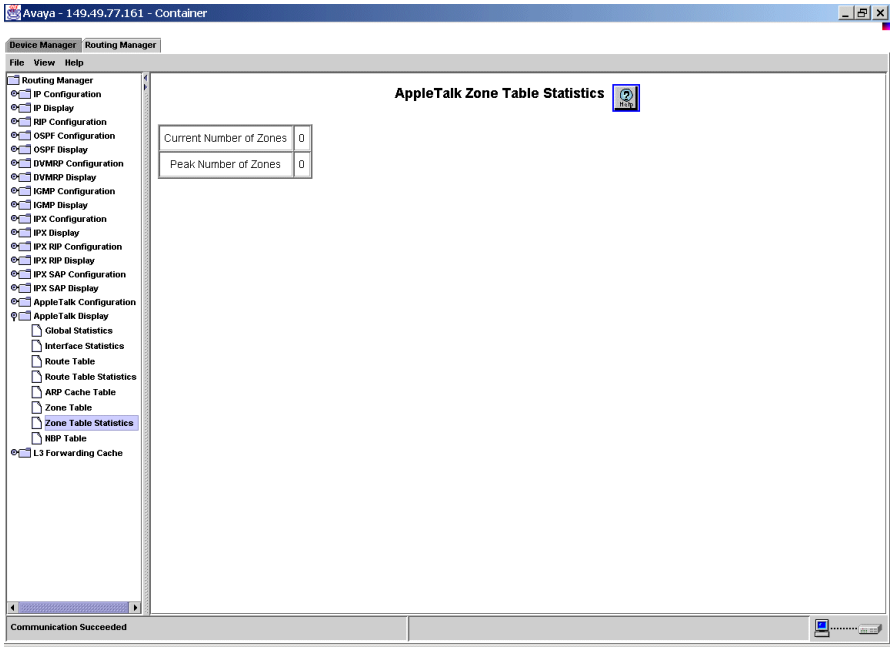
Table 14-11. Zone Table Parameters

Field	Description
Index	The zone index.
Name	The name of the zone.
Network Range	The network range associated with the zone.

Zone Table Statistics

To display AppleTalk zone table statistics, select **AppleTalk Display > Zone Table Statistics**. The AppleTalk Zone Table Statistics window opens.

Figure 14-12. Zone Table Statistics Window



The following parameters are displayed:

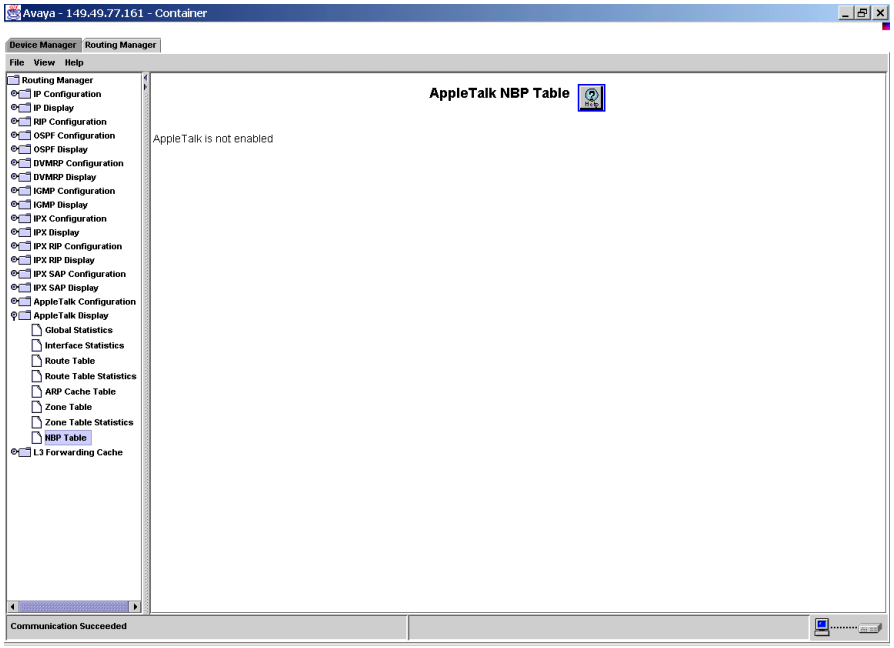
Table 14-12. AppleTalk Zone Table Statistics Parameters

Field	Description
Current Number of Zones	The current number of AppleTalk zones.
Peak Number of Zones	The peak number of AppleTalk zones.

NBP Table

To display the AppleTalk NBP table, select **AppleTalk Display > NBP Table**. The AppleTalk NBP Table window opens.

Figure 14-13. NBP Table Window



The following parameters are displayed:

Table 14-13. NBP Table Parameter

Field	Description
Index	The index of the name binding protocol entry.
Name	The name of the NBP entry.
Type	The type of object named.
Interface	The AppleTalk interface associated with the NBP table entry.
Zone	The zone field associated with the NBP table entry.

15 L3 Forwarding Cache

This chapter provides instructions for all L3 Forwarding Cache routing functions using the Avaya P580/P882 Manager.

Configuring L3 Forwarding Cache

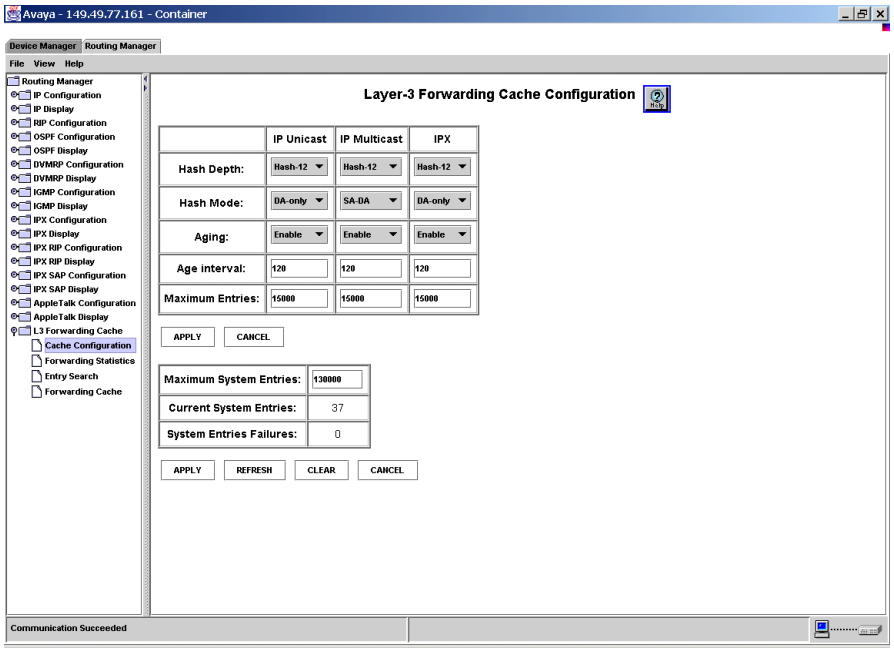
The L3 Forwarding Cache folder provides access to the following windows:

- **Cache Configuration**
- **Forwarding Statistics**
- **Entry Search**
- **Forwarding Cache**

Cache Configuration

To display and update the Layer-3 forwarding cache configuration, select **L3 Forwarding Cache > Cache Configuration**. The Layer-3 Forwarding Cache Configuration window opens.

Figure 15-1. Layer-3 Forwarding Cache Configuration Window



The following parameters are displayed:

Table 15-1. L3 Forwarding Cache Configuration Parameters

Field	Description
Hash Depth	The type of hash depth used for IP unicast, IP multicast, and IPX datagrams. The possible values are: • **Hash-8** - An 8-bit memory bucket used to store information about the source or destination protocol address (or both). • **Hash-10** - A 10-bit memory bucket used to store information about the source or destination protocol address (or both). • **Hash-12** - A 12-bit memory bucket used to store information about the source or destination protocol address (or both).

Table 15-1. L3 Forwarding Cache Configuration Parameters

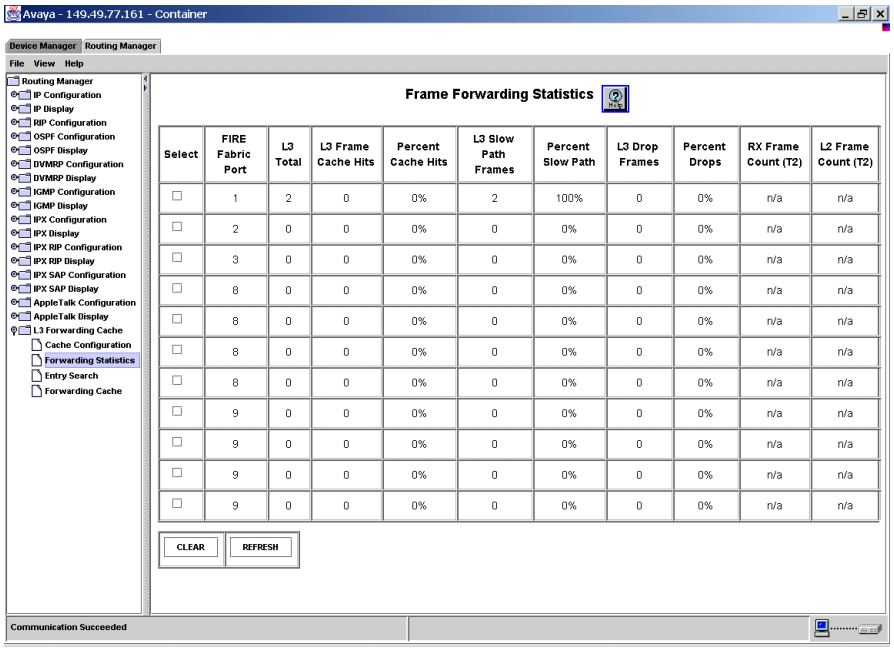
Field	Description
Hash Mode	Select the table hash lookup mode for the IP unicast, IP multicast, and IPX forwarding table. • **DA-only** - Forward entries input to the forwarding tables according to the protocol destination addresses only. • **SA-DA** - Forward entries input to the forwarding tables according to the destination and source addresses.
Aging	Select the IP unicast, IP multicast, and IPX forwarding table entry aging status. Possible values are: • **Enabled** • **Disabled**.
Age Interval	The amount of time (in seconds) allowed to pass from a host's last IP Multicast request before the device stops forwarding a multicast session to a host.
Maximum Entries	The number of active entries in the IP unicast, IP multicast, and IPX forwarding table. The supervisor module forwards additional flows.
Maximum System Entries	Enter the maximum system entries. The default value is 130000.
Current System Entries	Displays the number of current system entries.
Maximum Entries Failure	Displays the number of system entry failures.

You can modify L3 Forwarding Cache Configuration parameters. You can also add, modify, or delete L3 Forwarding Cache entries. For information, refer to "Modifying Tables" on page 85.

Forwarding Statistics

To display frame forwarding statistics, select **L3 Forwarding Cache > Forwarding Statistics**. The Frame Forwarding Statistics window opens.

Figure 15-2. Frame Forwarding Statistics Window



The following statistics are displayed:

Table 15-2. Forwarding Statistics

Field	Description
FIRE Fabric Port	The fabric port associated with the Layer 3 module.
L3 Total	The total number of frames received on this interface.
L3 Frame Cache Hits	The number of packets received on this interface that were successfully matched against existing forwarding entries in the Layer 3 address cache.
Percent Cache Hits	The total percentage of successful matches between packets received on an interface and that matched the Layer 3 address cache entries.

Table 15-2. Forwarding Statistics (Continued)

Field	Description
L3 Slow Path Frames	The number of frames received on this interface that were not successfully matched against existing forwarding entries in the Layer 3 address cache. These frames are forwarded to the supervisor module (slow path).
Percent Slow Path	The total percentage of unsuccessful matches between packets received on an interface and that did not match the Layer 3 address cache entries.
L3 Drop Frames	The number of Layer 3 frames that were dropped because they did not match the Layer 3 address cache entries.
Percent Drops	The total percent of Layer 3 frames that were dropped.
RX Frame Count (R2)	The total number of frames received on this interface.
L2 Frame Count (T2)	The number of Layer 2 frames received on a fabric port that were forwarded to an associated VLAN.

You can refresh or clear the statistics available in the L3 Frame Forwarding Statistics windows.

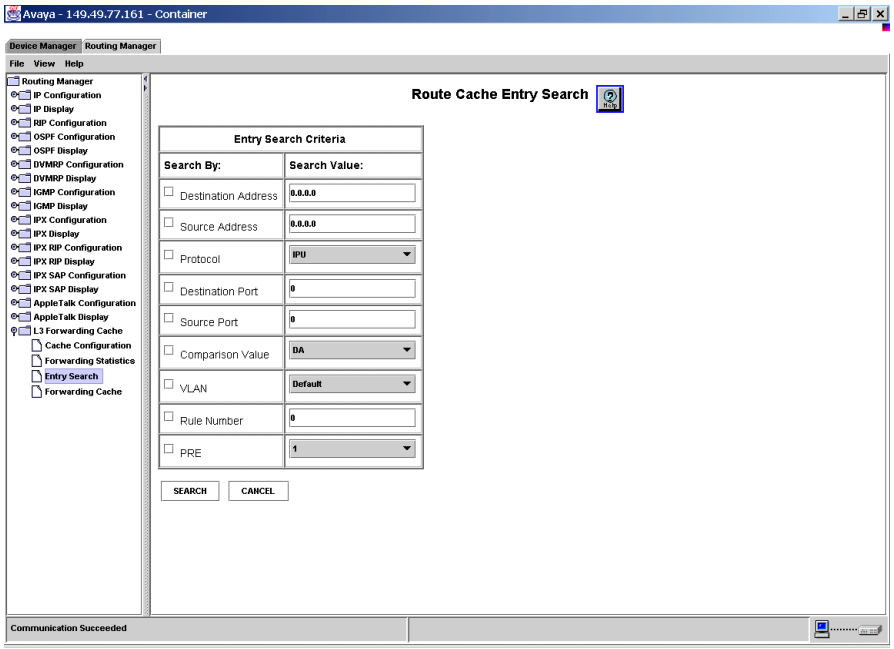
To refresh the statistics, click **REFRESH**. The statistics are refreshed.

To clear the statistics, click **CLEAR**. The statistics are cleared.

Entry Search

To display and configure route cache entry search criteria, select **L3 Forwarding Cache > Entry Search**. The Route Cache Entry Search window opens.

Figure 15-3. Route Cache Entry Search Window



The following parameters are displayed:

Table 15-3. Route Cache Entry Search Parameters

Field	Description
Destination Address	The destination IP address to be searched within the routing cache.
Source Address	The source IP address to search for within the routing cache.
Protocol	Select the protocol to search on for all entries within the routing cache that match the specified source port (IPU, IPM, IPX).
Destination Port	The destination port to search for all entries within the routing cache.
Source Port	The source port to search for.

Table 15-3. Route Cache Entry Search Parameters (Continued)

Field	Description
Comparison Value	The comparison value to be used. Possible values are: • **DA** - Destination address. • **DASA** - Destination and source address. • **DAPROT** - Destination address and protocol. • **DADP** - Destination address and destination port number. • **DASAPROT** - Destination and source address and protocol. • **DASADPSP** - Destination and source address and the corresponding destination and source port numbers.
VLAN	The VLAN to be searched for.
Rule Number	The rule number associated with an access list.
PRE	Select the PRE associated with the specified fabric port ID.

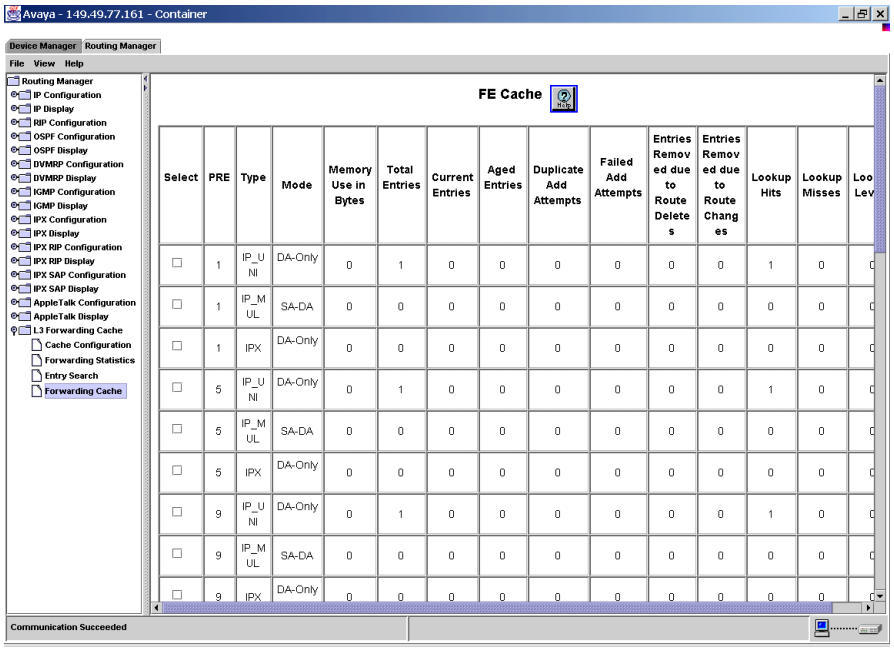
To search the L3 routing cache:

1. Enter the criteria by which you want to search.
2. Ensure that the Search by checkbox next to the criteria is checked.
3. Click **SEARCH**. A window opens in the Table Area with the results of the search.

Forwarding Cache

To display and configure forwarding cache configuration, select **L3 Forwarding Cache > Forwarding Cache**. The FE Cache window opens.

Figure 15-4. FE Cache Window



The following parameters are displayed:

Table 15-4. FE Cache Parameters

Field	Description
PRE	The Packet Routing Engine in question.
Type	The type of packet. Possible values are: • **IP Unicast** • **IP Multicast**
Mode	The table mode. The table mode indicates what values are used in a comparison to determine whether or not a packet is forwarded.Possible values are: • **DA-Only** • **SA & DA** • **SA only**
Memory Use in Bytes	The amount of memory used by each entry.

Table 15-4. FE Cache Parameters (Continued)

Field	Description
Total Entries	The number of cumulative entries since the last time the statistics were cleared.
Current Entries	The number of active entries.
Aged Entries	The number of entries aged out.
Duplicate Add Attempts	The number of attempts at adding slow path entries.
Failed Add Attempts	The number of failed attempts at adding forwarding entries.
Entries Removed due to Route Deletes	The number of entries removed because of route deletions.
Entries Removed due to Route Changes	The number of entries removed because of route changes.
Lookup Hits	The number of cache hits.
Lookup Misses	The number of cache misses.
Lookup Levels	The number of levels in the cache.

You can modify FE Cache parameters. For information, refer to "Modifying Tables" on page 85.

A Menus

This appendix gives the full structure of the menus in the Avaya P580/P882 Management Application.

Device Manager Menus

This section provides the menu structure of the Avaya P580/P882 Device Manager.

File Menu

Table A-1. File Menu - Device Manager

Item	Description
Refresh	Refreshes the display with information from the device.
Exit	Exits the Avaya P580/P882 Manager.

View Menu

Table A-2. View Menu - Device Manager

Item	Description
Configuration	Switches the Device Manager to configuration mode.
Port RMON	Switches the Device Manager to monitoring mode.
Toolbars > Show Application Toolbar	Toggles the display of the Application toolbar.
Toolbars > Show Get/Set Toolbar	Toggles the display of the Get/Set toolbar.

Actions Menu

Table A-3. Actions Menu - Device Manager

Item	Description
Device Information	Displays information for the device.
Port LAG	Displays and enables configuration of LAGs.
Switch Connected Addresses	Displays a list of stations connected to each of the device's ports.
Device Web Site	Opens a web browser to the device's web site.
Save Running Configuration	Saves the running configuration to the device.
Reset Device	Resets the device.

Help Menu

Table A-4. Help Menu - Device Manager

Item	Description
Help Contents	Opens the on-line help contents page for information.
About Avaya P580/P882 Device Manager	Copyright information about the Avaya P580/P882 Device Manager.

Routing Manager Menus

This section provides the menu structure of the Avaya P580/P882 Routing Manager.

File Menu

Table A-5. File Menu - Routing Manager

Item	Description
Device Web Site	Opens a web browser to the device's web site.
Exit	Exits the Avaya P580/P882 Manager.

View Menu

Table A-6. View Menu - Routing Manager

Item	Description
Status Bar	Toggles the display of the status bar.
Collapse Tree	Collapses the Routing Manager Tree.

Help Menu

Table A-7. Help Menu - Routing Manager

Item	Description
Content	Opens the on-line help for information.
About Avaya P580/P882 Manager	Copyright information about the Avaya P580/P882 Device Manager.

Index