



**Avaya Integrated Management
Release 5.2**
G430 Manager User Guide

Issue 1
May 2009

© 2009 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Software Documentation, Document number 03-600758.

To locate this document on the Web site, simply go to <http://www.avaya.com/support> and search for the document number in the search box.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. see your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site:

<http://www.avaya.com/support>

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:

<http://www.avaya.com/support>

Contents

Preface	13
Purpose.	13
Intended audience.	13
Organization of this guide.	13
Conventions used in this book.	15
Support resources.	15
Avaya Professional Services	15
Avaya Global Services Delivery	16
Avaya Global Technical Services.	17
Customized Management Solutions for Avaya Integrated Management.	17
Avaya Contact Information	17
Product documentation	18
How to access books on the web.	18
Chapter 1: Introduction	19
Avaya G430 Manager overview	19
Starting the Avaya G430 Manager	20
The Avaya G430 Device Manager as part of the Avaya Network Management	20
Running the Avaya G430 Manager from the Avaya Network Management Console	20
Avaya G430 Manager through web management	20
The user interface	22
Application tabs	22
Status line	22
Managing tables	23
Chapter 2: Device Manager	25
The G430 Device Manager user interface	25
Application toolbar	26
Get/Set toolbar	27
Tree view	29
Desktop.	29
Chassis view	29
Selecting elements.	31
Dialog area	31
Avaya G430 modes	31
Refreshing device information	32
Using dialog boxes and tables	32
Using the Avaya G430 Device Manager help	33

Contents

Opening the help to the contents page	33
Opening the help to a topic of interest	33
Chapter 3:	Device
Configuration	35
Viewing Device configuration	35
Device Configuration - General tab	36
Device Configuration - Advanced tab	39
Device Configuration - FRU tab	41
Device Configuration - 802.1x tab	43
Device Configuration - Protocol Status tab	44
Viewing Module Configuration	46
Module Configuration - General tab	47
Viewing Port Configuration	49
Port Configuration - General tab	50
Port Configuration - Advanced tab	53
Port Configuration - 802.1X tab	55
Port Configuration - LLDP tab	59
Configuring the external modem	61
Configuring the dialer	64
Resetting the device	66
Chapter 4: Power over Ethernet	67
PoE overview	67
Viewing PoE information	67
Viewing PoE port information	67
Viewing PoE configuration	68
PoE module configuration	68
PoE port configuration	69
Chapter 5: Media Gateway Functions	71
Media gateway overview	71
Media gateway configuration	71
Viewing media gateway configuration	72
MG Config	72
MGC Config	74
Viewing Media Module configuration	75
Avaya Site Administration	76

Chapter 6: VoIP Engine Configuration	77
VoIP overview	77
VoIP resources.	78
VoIP status	81
Chapter 7: Embedded Tools	85
Configuring the DHCP server	85
Configuring DHCP	85
Configuring Basic DHCP options.	86
Creating a new DHCP pool	87
Configuring DHCP pool parameters	89
Configuring DHCP assignment parameters	90
Configuring the TFTP server	93
Configuring the Converged Network Analyzer application	94
Configuring an External Test Plug	94
Configuring Schedulers	97
Chapter 8: WAN Configuration	99
WAN overview	99
Ethernet LAN Port Configuration	99
Ethernet LAN Port Configuration - General tab	100
Ethernet LAN Port Configuration - Advanced tab	103
Ethernet WAN Port Configuration	103
Ethernet WAN Port Configuration - General tab	105
Ethernet WAN Port Configuration - PPPoE Client tab.	108
Ethernet WAN Port Configuration - DHCP Client tab	110
Ethernet WAN Port Configuration - Extended Keep Alive Tab	114
Configuring the ETR port	115
The Services Interface.	117
Configuring Backup Interfaces	117
Viewing the Backup Interfaces table	117
The Backup Interface wizard	119
Welcome screen	120
Primary Interface screen	121
Backup Interface screen.	122
Backup Interface Parameters screen.	123
Confirmation screen	124
Dynamic CAC	125

Chapter 9: VLANs	127
VLAN Configuration overview	127
VLANs overview	127
Master VLAN list	128
VLAN tags	128
Configuring VLANs	129
VLAN Tree	129
Selection List	131
Port Configuration area	132
Managing VLANs	133
Creating VLANs	133
Renaming VLANs	134
Synchronizing VLAN names	135
Deleting VLANs	136
Managing Port VLAN settings	137
Selecting ports	137
Viewing Port VLAN settings	137
Using the Port Configuration Area	138
Configuring VLANs using drag-and-drop	138
Updating the device	138
Chapter 10: Port Mirroring	139
Port Mirroring overview	139
Configuring Port Mirroring	139
The Port Mirroring wizard	140
Port Mirroring wizard - Create Welcome	141
Port Mirroring wizard - Edit/Delete Welcome	142
Port Mirroring wizard - Source Port Selection	142
Port Mirroring wizard - Destination Port Selection	144
Port Mirroring wizard - Frames Direction Selection	145
Port Mirroring wizard - Confirmation	146
Chapter 11: Port RMON	147
Displaying the Port RMON Window	147
The Pie Chart	148
The Traffic Graph	148
Viewing Traffic Statistics	148
Zooming In and out of the graph	148
Scrolling within the graph	149

Unfreezing the graph	149
Traffic Types	149
Chapter 12: Switch Connected Addresses	151
Switch Connected Addresses overview	151
Viewing the Switch Connected Addresses window	151
Sorting the List of Stations	152
Chapter 13: Port Redundancy	153
Overview of Port Redundancy	153
Configuring Port Redundancy	154
Adding a Port Redundancy	155
Port Redundancy wizard	156
Port Redundancy wizard - Welcome	157
Port Redundancy wizard - Primary Port Selection	158
Port Redundancy wizard - Secondary Port Selection	159
Port Redundancy wizard - Name and Type	160
Port Redundancy wizard - Confirmation	161
Deleting Port Redundancies	162
Updating the device	162
Chapter 14: Trap Managers Configuration.	163
Trap Manager overview	163
Configuring Trap Managers.	164
Editing the Trap Managers Table	166
Chapter 15: Routing Manager	167
The Routing Manager user interface	167
Toolbar	168
Tree view	169
Table/Form Area	170
Editing tables	170
Creating new table entries	171
Modifying table entries	171
Deleting table entries	171
Saving table information in a file	171
Saving configuration changes	172
Running changes	172
Committed changes	172

Contents

Resetting a router	172
Using the Avaya G430 Routing Manager help	173
Opening the Help to the contents page	173
Opening the Help to a topic of interest.	173
Chapter 16: Layer 2	175
Layer 2 Interfaces	175
Chapter 17: Policy Based Routing Manager.	177
The Policy Based Routing Manager user interface	177
Toolbar	178
Tree view	179
Table view	179
The Application Editor tool	179
Saving configuration changes	179
Applied changes	180
Committed changes	180
Using the Avaya G430 Policy Based Routing Manager help	180
Opening the Help to the Contents Page	180
Opening the Help to a topic of interest.	180
Chapter 18: IP Route	181
Displaying IP Global Parameters	181
Configuring IP interfaces	182
Viewing the Dynamic IP Interfaces Table	185
Viewing the Routing Table	186
Viewing the Static Routing Table	189
Viewing the ARP Table	191
Configuring GRE tunneling	193
DHCP	196
Viewing DHCP/BOOTP Global Parameters.	196
Configuring the DHCP/BOOTP parameters	198
RIP	199
Viewing RIP Global Parameters.	199
Configuring RIP Interfaces	200
OSPF	203
Viewing OSPF Global Parameters	203
Configuring OSPF Interfaces	204

Configuring OSPF Area Parameters	206
Viewing the OSPF Link State Database	207
Viewing the OSPF External Database	209
Viewing OSPF Neighbors	210
VRRP	211
Viewing VRRP Global Parameters	211
Viewing the VRRP Table.	212
Header Compression	214
Configuring cRTP Interfaces	214
Configuring TCP Header Compression Interfaces	216
Chapter 19: Policy Based Routing	219
Policy Based Routing overview.	219
Using the Tree view	220
Using the Table view.	220
Policy Based Routing list	221
Adding Policies	222
Deleting Policies	222
Policy Based Routing Rules list	222
Adding rules	226
Modifying rules.	226
Copying rules	226
Moving rules	227
Deleting rules	227
Next Hop list	227
Adding routes	228
Modifying routes.	229
Copying routes.	229
Moving routes	229
Deleting routes.	230
Policy Enforcement Points	230
Configuration	231
Policy Based Routing List Configuration	231
Next Hop List Configuration	233
Using Address Wildcards	234
Using the IP Simulate function	235
IP Simulate overview	235
Using IP Simulate	235

Chapter 20: Applications Editor Tool	239
Applications Editor overview	239
Using the Applications Editor	239
Adding Application Protocols	241
Modifying an Application Protocol	241
Deleting an Application Protocol	241
Applying Changes	242
Reports	242
Appendix A: Menus	243
Device Manager Menus	243
File Menu	244
View Menu	244
Configure Menu	244
Actions Menu	246
Tools Menu	246
Help Menu	247
Routing Manager Menus	247
File Menu	247
Edit Menu	248
View Menu	248
Action Menu	248
Help Menu	249
Policy Based Routing Menus	249
File Menu	249
Edit Menu	250
View Menu	250
Tools Menu	250
Help Menu	251
Applications Editor Menus	251
File Menu	251
Edit Menu	252
Help Menu	252
Appendix B: Web Management	253
Web Management overview	253
Configuring the Avaya G430 Device	253

Appendix C: ICMP Packet Types & Codes	255
ICMP Packet Type/Code List	255
Index	259

Preface

Welcome to Avaya G430 Manager. This chapter provides an introduction to the structure and assumptions of this guide. It includes the following sections:

- [Purpose](#) - A description of the goals of this guide.
- [Intended audience](#) - The intended audience of this guide.
- [Organization of this guide](#) - A brief description of the subjects contained in the various sections of this guide.

Purpose

The Avaya G430 Manager guide contains information needed to use the management system efficiently and effectively.

Intended audience

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 G430 Manager** - Information pertaining to the entire Avaya G430 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 G430 Manager, including instructions on starting the Avaya G430 Manager.
- **Avaya G430 Device Manager** - Information pertaining to Avaya G430 Device Management.

- **Device Manager** - An introduction to the Avaya G430 Device Manager, including a description of the user interface.
- **Device Configuration** - Viewing and modifying the different device configurations.
- **Power over Ethernet** - An overview of Power over Ethernet (PoE) and instructions on viewing and configuring PoE parameters.
- **Media Gateway Functions** - An overview of the Media Gateway functions and information on viewing and configuring Media Gateway components.
- **VoIP Engine Configuration** - An overview of VoIP Engine functionality and information on viewing and configuring VoIP Engine parameters.
- **WAN Configuration** - An overview of WAN module and information on viewing and configuring WAN parameters.
- **Embedded Tools** - An overview of embedded tools and information on configuring the Avaya G430's embedded server functions and tools.
- **VLANs** - Viewing and editing VLAN information.
- **Port Mirroring** - Configuring port mirroring for ports on an Avaya G430 device.
- **Port RMON** - Viewing graphical representations of the traffic on the ports of the Avaya G430 device.
- **Port Redundancy** - Configuring port redundancy for ports on an Avaya G430 device.
- **Switch-Connected Addresses** - Viewing information on addresses connected to the device.
- **Trap Managers Configuration** - Viewing and modifying the Trap Managers table.
- **Avaya G430 Routing Manager** - Information pertaining to Avaya G430 routing management.
 - **Routing Manager** - An introduction to configuring routing and a description of the Avaya G430 Routing Manager user interface.
 - **Layer 2** - Detailed descriptions of layer 2 configuration that enable you to view layer 2 interfaces at the management station.
 - **IP Route** - Detailed descriptions of IP route configuration that enable you to display and update IP interfaces, the IP routing table, the ARP table, GRE tunneling parameters, DHCP/BOOTP parameters, RIP interfaces, OSPF interfaces, area parameters, link-state database and neighbours, the IP access control table, and redundancy parameters.
- **Avaya G430 Policy Based Routing Manager** - Information pertaining to Avaya G430 Policy Based Routing management.
 - **Policy Based Routing Manager** - An introduction to configuring Policy Based Routing and a description of the Avaya G430 Policy Based Routing Manager user interface.
 - **Policy Based Routing** - Detailed descriptions of Policy Based Routing configuration that enable you to display and update Policy Based Routing lists, Next Hop routing tables, and Policy Enforcement Points.

- **Applications Editor Tool** - Detailed description of the Applications Editor Tool, which enables you to refine protocol traffic through Policy Based Routing by customizing individual protocols.
- **Appendices** - Additional information about the Avaya G430 Manager.
- **Menus** - The full structure of the menus in the Avaya G430 Manager.
- **Web Management** - Instructions on how to manage Avaya G430 device through the Internet.
- **ICMP Packet Types and Codes** - A list of ICMP Packet Types and Codes as used in IP Simulate.

Conventions used in this book

The following typographical conventions are used:

- **Bold** type is used to indicate selections from menus, dialog box, windows, buttons and tabs in a window, and the **Enter** key on the keyboard. It is also used for emphasis.
- `Courier bold` font is used to indicate commands that you type.
- `Courier bold italic` font is used to indicate variable information within the commands that you type.
- `Courier` font is used to indicate information that appears as command results, or output.
- Arrows indicate options that you select from cascading menus: for example, Select **File > Open** means choose the **Open** option from the **File** menu.

Support resources

Avaya provides a variety of planning, consulting, and technical services. The following sections describe the resources and services that are available.

Avaya Professional Services

The Avaya Professional Services (APS) team of Avaya Integrated Management (AIM) consultants offers customers the following services:

- Platform-readiness verification
- AIM architectural planning, design, and overview

- Remote turnkey implementation and installation
- AIM server configuration
- Customer acceptance verification
- Custom on-site services
- Onsite and remote knowledge transfer

The APS Data Group consists of the following teams:

- **Avaya Integrated Management Consultants**

The Avaya Integrated Management (AIM) consulting team offers planning, design, implementation, consulting, and knowledge transfer services for the entire Avaya Integrated Management Suite. This includes ASA, Val Manager, NMC with SUM, MSA and FPM. The thrust of the APS team is to bring the correct methodology to these complex application deployments that span various regions, and to provide continuity to the overall project. Through proper integration and consulting, our customer can leverage the AIM suite to lower total cost of ownership, and proactively manage their VoIP network comfortably and confidently.

- **Data Network Implementation Engineering**

The Data Network Implementation Engineering (formerly RNIS) team implements and upgrades or upgrades existing or new data networks. The team analyzes the network design requirements and performance expectations of the customer. The team then creates the hardware and software installation specification used to implement data devices that include Cajun, VPN, Wireless LAN, Secure Gateways, Extreme, Juniper, and multivendor data equipment.

The APS Data Group provides support on a contract basis. Contact your local Avaya Account Team or Business Partner to purchase any implementation offer from the team. For more information, refer to Table 1: [Customer-Accessible Resources](#) on page 18, or contact Jon Machak at 234-213-3788 or machak@avaya.com

Avaya Global Services Delivery

Avaya Global Services Delivery (GSD) provides support to the Avaya Integrated Management client teams, field technicians, and customers. The GSD will bill customers for support on a time and materials basis if the following conditions exist:

- Customers do not provide remote access.
- Customers do not have a current maintenance agreement.
- Customers do not procure and install the required systems and software as defined in the Integrated Management Services Support Plan.
- Customers request support that is outside the purchase agreement.

The GSD does not support hardware or software that customers purchase from third-party vendors

Avaya Global Technical Services

Avaya Global Technical Services answers customer calls about products in Avaya Integrated Management. The team will either answer your questions directly or connect you with an associate who can answer questions about the products.

Customized Management Solutions for Avaya Integrated Management

The Integrated Management Product Team understands the customer's needs and is focused on customer satisfaction. For more information on contact information, see [Customer-Accessible Resources](#) on page 18. The Product Team will assist customers with Avaya Integrated Management Projects and will provide:

- **Project Management** - An Integrated Management project person will work with the customer to access configuration and customization requirements for any or all applications within each Avaya Integrated Management offer. If custom work is required, the evaluation will include a proposed statement of work and price. Note that this offer is not intended to provide installation for customers that choose to implement Integrated Management applications using Avaya Services or third-party implementation services.
- **Training** - Basic training can be performed remotely using an interactive medium to display the applications and a conference bridge for audio. On-site training can be customized to meet the customer's needs. Customized training will focus on application functionality that is relevant to the customer and provide focused knowledge transfer to facilitate application-specific training.

Avaya Contact Information

Table 1 provides contact information that you may use if you need assistance during the process of installing, configuration and setting up of Avaya Integrated Management.

Table 1: Customer-Accessible Resources

Resource	Contact Information
Avaya Support Center	http://www.avaya.com/support
Avaya Global Technical Services	+1 800 242-2121 x15921
Avaya Professional Services (APS) Consulting	+1 800 730-9108, prompt 3
Integrated Management Product Team	Send email to: mjk@avaya.com
Toll Fraud Intervention	+1 800 643-2353, prompt 1

Product documentation

The latest version of Avaya Integrated Management product documentation, including this book, is available from the Avaya Support Web site. To view or download these books from the Web, you must have access to the Internet, an Internet browser, and the Adobe Reader. The Adobe Reader 8.0 is provided on the Avaya Integrated Management CDs and is also available from <http://www.adobe.com>. For more information on how to view or download these books, see [How to access books on the web](#) on page 18

How to access books on the web

To view or download books from the Avaya Support Web site, follow these steps:

1. Access <http://www.avaya.com/support>.
2. Click **Find Documentation and Technical Information by Product Name**.
3. Click the letter **I** in the alphabet listing.
4. Locate the **Integrated Management - All Application** and click the corresponding link.
5. Click **View all documents** to display a list of available books for that product or offer.

Chapter 1: Introduction

This chapter provides an introduction to the Avaya G430 Manager. It includes the following sections:

- [Avaya G430 Manager overview](#) - An overview explaining the different aspects of Avaya G430 Device management.
- [Starting the Avaya G430 Manager](#) - Instructions on how to access the Avaya G430 Manager from your management platform.
- [The user interface](#) - Detailed descriptions of the user interface common to all applications in the Avaya G430 Manager.
- [Managing tables](#) - An explanation of the symbols used to label table rows.

Avaya G430 Manager overview

The Avaya G430 Manager is a new media gateway targeting small and medium branches of 1 to 150 users. G430 is a replacement for G350 and is also a variation of G250.

The G430 Manager supports three G700 form factor media modules and two expansion modules. Each expansion module can receive up to two G700 form factor media modules, thus allowing the gateway to cover a wide spectrum of users at an optimal cost.

The Avaya G430 Manager provides full management capabilities for Avaya G430 devices. This includes the ability to view three aspects of the device management:

- **Device Manager** - Provides a view of the configuration of the device, including VLAN configuration, port redundancy, port mirroring, switch connected addresses and traps. For more information, see chapters 2-14.
- **Routing Manager** - Provides a view of the Layer 3 routing and forwarding functions of the device. For more information, see chapters 15-17.
- **Policy Based Routing Manager** - Provides a view of the configuration and maintenance of Policy Based Routing on the Avaya G430 device. For information, see chapters 18-19.

For information on alternating between the different views, see [“Application tabs” on page 22](#).

Starting the Avaya G430 Manager

This section provides instructions for starting the Avaya G430 Manager.

The Avaya G430 Device Manager as part of the Avaya Network Management

If you install the Avaya G430 Device Manager as a part of the Avaya Network Management, the following sections provide instructions for starting the Avaya G430 Manager.

Running the Avaya G430 Manager from the Avaya Network Management Console

From the management platform map:

1. Select the label representing the Avaya G430 device you want to manage.

2. Click .

Or

Double-click the Avaya G430 device.

Or

Select **Tools > Avaya Device Manager**.

Avaya G430 Manager through web management

To start the Avaya G430 web management:

1. Point your web browser to **http://xxx.xxx.xxx.xxx**, where **xxx.xxx.xxx.xxx** is the IP address of the Avaya G430 device you want to manage. The system displays the **Enter Network Password** dialog box.

Figure 1: Enter Network Password dialog box

The dialog box is titled "135.27.162.80: Enter SNMP parameters". It features a blue title bar with a close button (X) on the right. The main content area is divided into two sections. The first section, labeled "SNMPv1", has a radio button selected and a text box labeled "Community:". The second section, labeled "SNMPv3", has an unselected radio button and three text boxes labeled "User name:", "Authentication password:", and "Privacy password:". At the bottom of the dialog are two buttons: "OK" and "Cancel".

2. Select the desired SNMP mode of operation.

If **SNMPv1** is selected, enter the correct SNMPv1 community string in the **Community** field.

Or

If **SNMPv3** is selected, enter a valid username from the SNMPv3 username list and corresponding authentication and privacy passwords.

Note:

Some operations in the Avaya G430 Manager require SNMPv3 authentication credentials. Verify that you are an SNMPv3 user or use the Secure Access Administration application for creating a new user. You can use the command line interface to create users on the media gateway.

3. Click **OK**. The system displays the Avaya G430 Welcome page.

If the required Java plug-in is installed on your computer, the Java Plug-in Security Warning dialog box opens after a few seconds.

If the required Java plug-in is not installed, the plug-in is automatically downloaded to your computer. Follow the instructions on the Avaya G430 Welcome page to install the plug-in.

The user interface

The Avaya G430 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, Policy Based Routing Manager, and Routing Manager applications for the Avaya G430 device.
- Application Area - An area where the selected application opens.
- [Status line](#) - Displays the communication status between the Avaya G430 Manager and the Avaya G430 device.

Application tabs

You can access the three main components of device management using the following Application Tabs in the Avaya G430 Manager:

- **Device Manager** - View the Avaya G430 Device Manager for device configuration and Port RMON.
- **Policy Based Routing Manager** - View the Policy Based Routing and Next Hop Routing configuration for the device.
- **Routing Manager** - View the Avaya G430 Routing configuration.

To alternate to a different view, click the appropriate application tab. The system displays the selected application.

Status line

The Status line shows the communication status between the application and the Avaya G430 device. The Status line displays a status message and an appropriate graphic. The following table shows the possible statuses with their corresponding graphics, and provides an explanation for each status.

Table 2: Communication statuses




Status	Graphic	Description
Ready		The application is ready to communicate with the Avaya G430 device.
Communicating		The application is currently communicating with the Avaya G430 device.




Table 2: Communication statuses

Status	Graphic	Description
Communication Error		The last attempted communication with the Avaya G430 device was not successful.

Managing tables

The Avaya G430 Manager interface displays the status of each row in a table. The following table shows a list of symbols that appear at the start of a table row, with their corresponding explanations.

Table 3: Table symbols

Symbol	Explanation
	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.

Chapter 2: Device Manager

This chapter provides an introduction to the Avaya G430 Device Manager. It includes the following sections:

- [The G430 Device Manager user interface](#) - An introduction to the Avaya G430 Device Manager user interface, including instructions on selecting elements and using the toolbar buttons.
- [Avaya G430 modes](#) - Instructions on alternating between the configuration and Port RMON modes in the Avaya G430 Device Manager.
- [Refreshing device information](#) - Instructions on how to refresh the information in the Avaya G430 Manager.
- [Using dialog boxes and tables](#) - An explanation of the icons found in the dialog boxes and tables in the Avaya G430 Device Manager.
- [Using the Avaya G430 Device Manager help](#) - An explanation of the options for accessing the online help in the Avaya G430 Device Manager.

The G430 Device Manager user interface

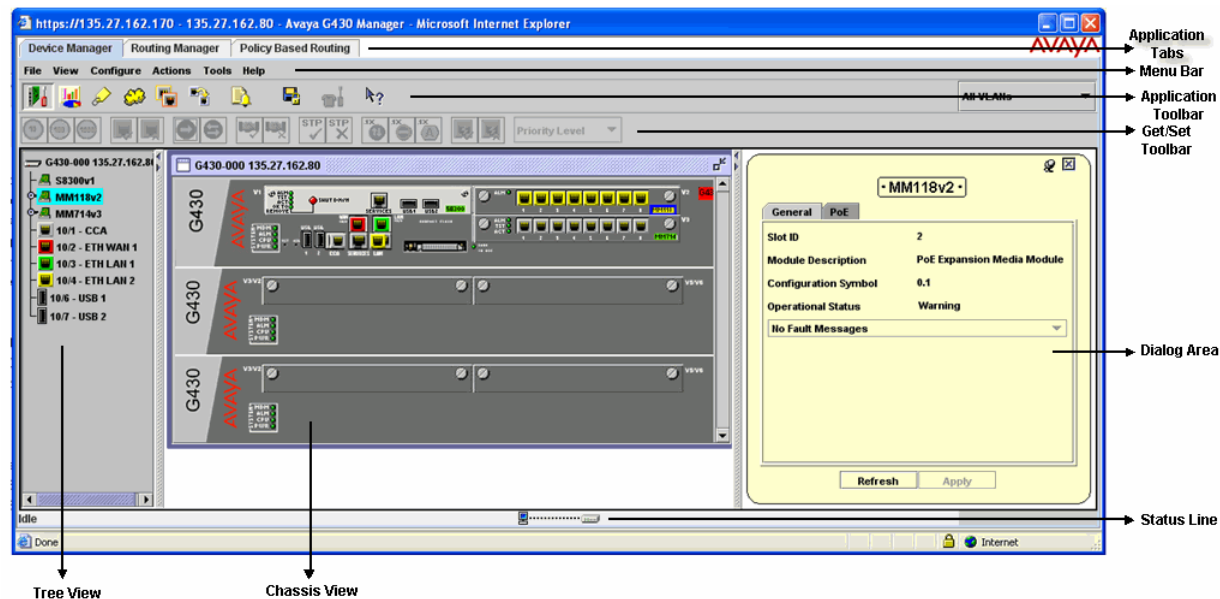
The Avaya G430 Device Manager user interface consists of the following elements:

- Application tabs - Tabs for toggling between the Avaya G430 Manager functions (Device Manager, Routing Manager, Policy-Based Routing Manager).
- Menu bar - Menus for accessing the Avaya G430 Device management functions. For more information, see Appendix A: *Menus*.
- [Application toolbar](#) - Toolbar buttons for accessing the Avaya G430 Device management functions.
- [Get/Set toolbar](#) - Toolbar buttons for viewing and changing the configuration of ports.
- [Tree view](#) - A resizable window containing a hierarchical representation of the modules and ports of the Avaya G430 device.
- [Chassis view](#) - A graphical representation of the Avaya G430 device.
- [Dialog area](#) - A resizable window where all dialog boxes and tables first open.

For information on other parts of the user interface, see [“The user interface” on page 22](#).

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

Figure 2: The Avaya G430 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 following table describes the buttons on the Application toolbar and gives the equivalent menu options.

Table 4: Application toolbar

Button	Description	Menu Option
	Sets the Device Manager to the Configuration Mode.	View > Configuration
	Sets the Device Manager to the Port RMON mode.	View > Port RMON
	Shows Switch-Connected Addresses.	View > Switch-Connected Addresses
1 of 2		

Table 4: Application toolbar (continued)

Button	Description	Menu Option
	Displays the VLAN window.	Configure > VLAN
	Displays the Port Redundancy table.	Configure > Port Redundancy
	Starts the Port Mirroring wizard.	Configure > Port Mirroring
	Displays the Trap Manager table.	Configure > Trap Managers
	Commits configuration changes.	Actions > Commit
	Launches Avaya Call Processing on the selected media gateway or voice port.	Tools > Administer Station/Gateway
	Opens the online help.	Help > Help On
2 of 2		

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

You can toggle the display of the application toolbar. To toggle the display of the application toolbar, select **View > Toolbars > Show Application Toolbar**.

Get/Set toolbar

The Get/Set toolbar provides buttons for getting and setting configuration parameters for selected ports. When a port 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 represent 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.








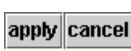
Selected ports can be configured using the Get/Set toolbar. To change the configuration of a port:

1. Click the button that represents the value of the parameter you want to apply to the port.
2. Click **apply** to update the device with the changes.
3. Click **cancel** to discard the changes. Options not applicable to the selected port are greyed out.

Multiple ports can be simultaneously configured using the Get/Set toolbar. When multiple ports with non-identical configurations are selected, only the parameters whose settings are identical on the selected ports 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 following table displays the buttons on the Get/Set toolbar and explains their functions and settings.

Table 5: Get/Set toolbar

Button	Description
	Get and set the port's speed: 10 Mbps, 100 Mbps, 1000 Mbps.
	Get and set the port's status: Enabled, Disabled.
	Get and set the port's mode: Half duplex, Full duplex.
	Get and set the port's auto-negotiation status: Auto-negotiation Enabled, Auto-negotiation Disabled.
	Get and set the port's STP mode: Enabled, Disabled.
	Get and set the port's Power over Ethernet.
	Get and set the port's priority. Select a priority level between 1 and 8 using the drop down listbox.
	Apply or cancel the configuration changes made with the Get/Set Toolbar.

Note:

The **apply or cancel** button appears only when changes are made to the configuration.

To toggle the display of the Get/Set toolbar, select **View > Toolbars > Show Get/Set Toolbar**.

Tree view

The Tree view shows a hierarchical representation of the structure of the Avaya G430 Device. To select ports, modules or media modules, click their icons in the Tree view. When an element is selected in the Tree view, the corresponding element is selected in the Chassis view.

The highest level of the Tree view represents the device. The second level represents modules and the third level represents ports. This also includes ports on expansion 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.

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 and floating dialog boxes and tables can also be minimized. Minimized windows appear at the bottom of the Desktop.

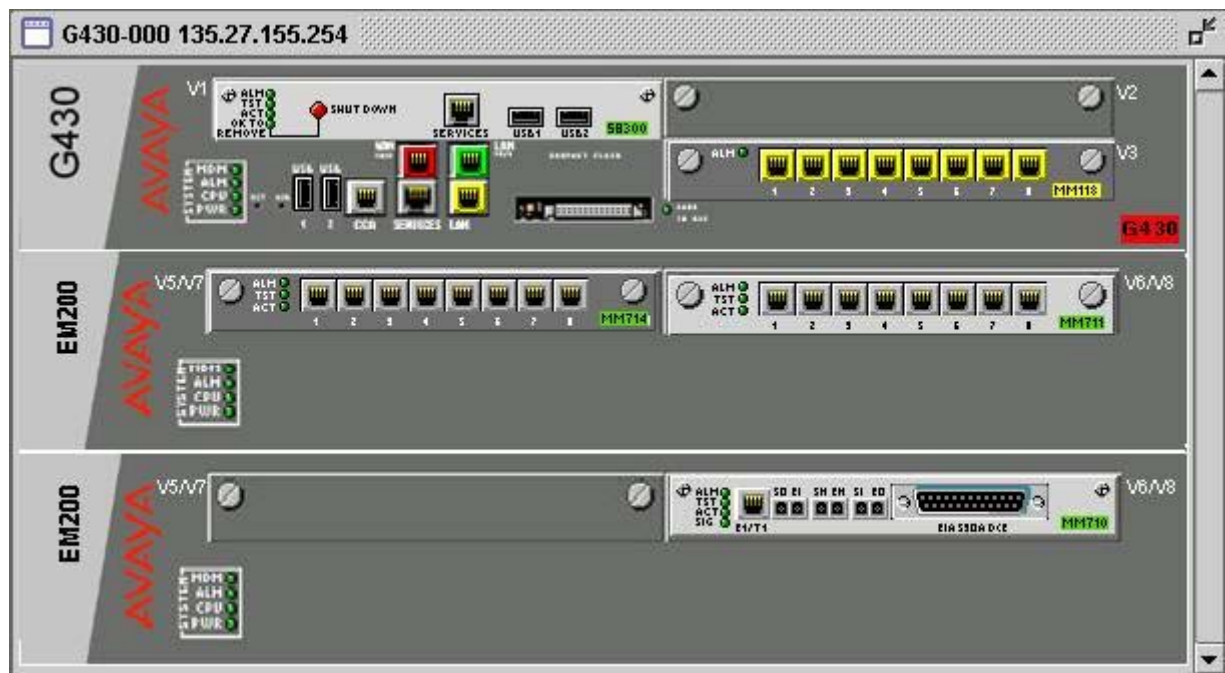
Chassis view

The Chassis view is a graphical representation of the Avaya G430 device. The Avaya G430 device contains several Avaya G430 modules. The Chassis view shows all of the devices' modules and ports. The colors of the modules and ports in the Chassis view reflect their status.

When you add or remove an EM200 to the G430 device, the Chassis view is automatically refreshed.

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.

Figure 3: Avaya G430 Chassis view



When viewing selected dialog boxes, the color of the port indicates the status of the port with regard to the application. The port selected to be the base port appears dark blue. The ports selected to be additional ports appear cyan.

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

Table 6: Chassis View port colors

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

Selecting elements

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 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 **Control** while clicking each element to be selected.

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 G430 modes

The Avaya G430 Device Manager has two modes:

- Configuration mode
- Port RMON mode

Note:

When the Avaya G430 Manager is installed as a standalone manager, and when running the Avaya G430 Manager through web management, Port SMON is not available.

When in configuration mode, you can view and change the configuration of the Avaya G430 Device and individual ports. When in Port RMON mode, you can view the graphical representations of the traffic on individual ports.

To switch to configuration mode:

Click .

Or

Select **View > Configuration**.

To switch to Port RMON mode:

Click .

Or

Select **View > Port RMON**.

Refreshing device information

To refresh the Avaya G430 device information, select **View > Refresh**. The Avaya G430 Device Manager refreshes its device information and updates the display.

Using dialog boxes and tables

Dialog boxes and tables in the Avaya G430 Manager application have a common set of buttons. The following table displays the buttons and explains their functions:

Table 7: Dialog box buttons

Button	Function
Refresh	Refreshes the information in the table or dialog box. This clears the changes made to the table or dialog box which is 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.
Delete	Deletes the selected rows of the table.
Undo	Undoes all the changes to the selected row in a table.

Using the Avaya G430 Device Manager help

This section explains how to use the online help in the Avaya G430 Device Manager. In the online help you can open the contents page or directly open a topic of interest.

Note:

When running the Avaya G430 Manager through web management, online help is available only if you install the online help on your network and configure the device with the location of the help files.

Opening the help to the contents page

To open the contents page of the online help, select **Help > Contents**.

Opening the help to a topic of interest

To open the help directly to a topic of interest:

1. Click .

Or

Select **Help > Help On**. The cursor changes to the shape of an arrow with a question mark.

2. Click on a point of interest in the Avaya G430 Device Manager. The system displays the explanation of your topic of interest.

Chapter 3: Device Configuration

This chapter explains how to view and set the various configuration parameters relevant to the Avaya G430 Device. It includes the following sections:

- [Viewing Device configuration](#) - View high-level information about the Avaya G430 Device.
- [Viewing Module Configuration](#) - View information specific to an Avaya G430 module in the device.
- [Viewing Port Configuration](#) - View information specific to the ports on the Avaya G430 Device.
- [Configuring the external modem](#) - View information specific to an external modem connected to the Avaya G430 Device.
- [Configuring the dialer](#) - View information specific to an external dial-up modem connected to the Avaya G430 Device.
- [Resetting the device](#) - Reset the Avaya G430 Device.

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

Click .

Or

Select **View > Configuration**.

Viewing Device configuration

The Device Configuration dialog box provides you with high-level configuration information specific to the Avaya G430 Device. This information is divided into the following:

- [Device Configuration - General tab](#) - Provides detailed information about the device such as the device's name, addresses, contact person, location, type, description, the number of modules in the device, and the management VLAN ID.
- [Media Gateway Configuration tab](#) - Provides detailed information on the configuration settings of the media gateway function of the device. For more information on Media Gateway Configuration, see [“Media Gateway Functions” on page 71](#).
- [Media Gateway Controller Configuration tab](#) - Provides detailed Quality of Service statistics for the media gateway function of the device. For more information, see [“Media Gateway Functions” on page 71](#).
- [Voice over IP Resources tab](#) - Provides administration parameters for the VoIP engine. For more information on VoIP Resources, see [“VoIP Engine Configuration” on page 77](#).
- [Voice over IP Status tab](#) - Provides detailed operating statistics for the VoIP engine. For more information, see [“VoIP Engine Configuration” on page 77](#).

Device Configuration - General tab

To view the General tab of the **Device Configuration** dialog box:
Select **Configure > Device Information**.

Figure 4: Device Configuration dialog box - General tab

• G430-000 135.27.155.254 •

VoIP resources

VoIP status

Protocol Status

802.1x

General

Advanced

MGC Config

MG Config

System Name	Shirish
MG Identifier	000
FW version	
Contact	Avaya
Physical Location	please do not use this switch
System Description	ledia Gateway, SW Version 29.1
Number Of Modules	6
VLAN MAC Address	00:07:3B:E4:67:F1
Current DS mode	N/A
Next DS mode	N/A
Current PMI Interface	Vlan 1
Current PMI IP Address	10.13.4.100
Current PMI Subnet Mask	255.255.224.0
Next PMI Interface	Vlan 1
Next PMI IP Address	10.13.4.100
Default Gateway	10.13.1.1

Refresh

Apply

Undo

Delete

Insert

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

Table 8: Device Configuration fields - General tab

Field	Description
System Name	The logical name of the device, as defined on the SNMP agent of the device.
MG Identifier	The identification number of the media gateway.
FW version	The firmware release the device is running.
Contact	The individual responsible for the maintenance of this device.
Physical Location	The current physical location of this device.
System Description	A description of the device.
Number Of Modules	The number of media modules and expansion modules in the chassis.
VLAN MAC Address	The MAC address of the VLAN interface.
Current DS Mode	The speed of the serial link.
Next DS Mode	The speed of the backup serial link, if configured.
Current PMI Interface	The interface currently designated as the Primary Management Interface.
Current PMI IP Address	The IP address of the Primary Management Interface.
Current PMI Subnet Mask	The Subnet mask of the Primary Management Interface.
Next PMI Interface	The interface configured by the gateway to be the new Primary Management Interface. If you set this parameter using the CLI, the new setting takes effect only after the next device reset.
Next PMI IP Address	The IP address configured by the gateway to be the new Primary Management Interface. If you set this parameter using the CLI, the new setting takes effect only after the next device reset.
Default Gateway	The IP address of the default network gateway device.
ICC VLAN	The VLAN of which the device is a member.
1 of 2	

Table 8: Device Configuration fields - General tab (continued)

Field	Description
Operational Status	The operational status of the device. Possible values are: <ul style="list-style-type: none"> ● OK - Device is operational. ● Down - Device is reporting faults, making it unable to function. ● Fatal - Device is reporting faults that are unrecoverable.
Fault Messages	The number of fault messages reported by the device.
2 of 2	

For more information on the user interface, see [“Using dialog boxes and tables” on page 32](#).

Device Configuration - Advanced tab

The Device Configuration dialog box - Advanced tab provides you with network bridging information about the Avaya G430 Device.

Figure 5: Device Configuration dialog box - Advanced tab

• G430-000 135.27.162.80 •

General	Advanced	MGC Config	MG Config	VoIP resources	VoIP status
STP Mode		Enable			
STP Priority		32768			
STP Version		RSTP			
STP Max Age (mili sec.)		20000			
STP Hello Time (mili sec.)		2000			
STP Forward Delay (mili sec.)		15000			
STP Bridge Max Age (mili sec.)		20000			
STP Bridge Hello Time (mili sec.)		2000			
STP Bridge Forward Delay (mili sec.)		15000			
Aging Time (sec)		300			
LLDP Mode		Enable			
LLDP Tx Interval (sec)		30			
LLDP Tx Hold Multiplier		4			
LLDP Tx Delay (sec)		1			
LLDP Re-Init Delay (sec)		2			

Refresh Apply Undo Delete Insert

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

Table 9: Device Configuration fields - Advanced tab

Field	Description
STP Mode	The spanning Tree status of the device.
STP Priority	The priority value used in Spanning Tree calculations.
STP Version	The version of the Spanning Tree on the device. Possible values are: <ul style="list-style-type: none"> ● STP Compatible - Standard Spanning-Tree Protocol ● RSTP - Rapid Spanning-Tree Protocol
STP Max Age (milliseconds)	The maximum amount of time before the Spanning Tree table recalculates if there is any change in the device status.
STP Hello Time (milliseconds)	The amount of time between Spanning Tree updates, if there are no detected changes in the device's network connections.
STP Forward Delay (milliseconds)	The amount of time for the device to begin forwarding packets after joining a network.
STP Bridge Max Age (milliseconds)	The maximum amount of time before Spanning recalculates if there is any change in the network bridging status.
STP Bridge Hello Time (milliseconds)	The amount of time between Spanning Tree updates when there are no detected changes in the overall bridged network topology.
STP Bridge Forward Delay (milliseconds)	The amount of time for the device to begin forwarding packets after recalculating its Spanning Tree table based on a change in the network topology.
Aging Time (seconds)	The amount of time MAC addresses remain in the CAM table.
LLDP Mode	The status of Link Layer Discovery Protocol (LLDP) Mode on the device: <ul style="list-style-type: none"> ● Enable - Use LLDP Mode. ● Disable - Do not use LLDP Mode.
LLDP Tx Interval	The amount of time between packet transmissions on the device.
LLDP Tx Hold Multiplier	The LLDP time-to-live value expressed as a multiple of the value configured in the LLDP Tx Interval field.
LLDP Tx Delay	The delay between successive LLDP frame transmissions initiated by status changes in LLDP.
LLDP Re-Init Delay	The amount of time the device is instructed to wait before re-initiating LLDP.

For more information on the user interface, see [“Using dialog boxes and tables” on page 32](#).

Device Configuration - FRU tab

The Device Configuration dialog box - FRU Tab provides you with information about the Field Replaceable Units (FRU) of the Avaya G430 Device.

Figure 6: Device Configuration dialog box - FRU tab

• G430-001 135.27.155.254 •

VoIP resources		VoIP status		Protocol Status		802.1x		FRU	
General		Advanced		MGC Config		MG Config			
EM200 # 1		Not Present							
EM200 # 2		Not Present							
PoE PSU # 1		Not Present							
PoE PSU # 2		Not Present							
PoE PSU # 3		Not Present							
Media Resource		MP80 VoIP DSP Module							
Memory Module		512MB DDR SDRAM memory module							
Compact Flash		No CompactFlash card is installed							

Refresh Apply Undo Delete Insert

Device Configuration

The following table provides the list of fields in the FRU tab of the Device Configuration dialog box and their possible values.

Table 10: Device Configuration - FRU tab

Field	Description / Possible values
EM200#1	Present or Not Present
EM200#2	Present or Not Present
PoE PSU #1	Present or Not Present
PoEPSU #2	Present or Not Present
PoE PSU #3	Present or Not Present
Media Resource	Possible values include: <ul style="list-style-type: none">● Not Present● MPxx VoIP DSP Module, where xx = 20/80.
Memory Module	512MB DDR SDRAM Memory Module with ECC.
Compat Flash	If the compact flash is installed, you can see a description of the size and the type of the compact flash. If the compact flash is not installed, the field value appears as No Compact Flash is installed.

Device Configuration - 802.1x tab

The Device Configuration dialog box - 802.1x tab provides you with support for the general configuration of the 802.1x application.

Figure 7: Device Configuration dialog box - 802.1x tab

The following table provides a list of the fields in the 802.1x tab of the Device Configuration dialog box and their descriptions.

Table 11: Device Configuration fields - 802.1x tab

Field	Description
IEEE-802.1x Mode	802.1x application status of the device. Possible values are: <ul style="list-style-type: none"> • Enable • Disable
Num of Supplicants per Port	The number of supplicants per port allowed in MAC-Based-Authentication. This parameter is not relevant in port-based-authentication mode. Possible values are between 1-8. The default value is 2 .
802.1x LLDP Transmitted VLAN-IDs	When enabled, allows transmission of port LLDP information (PVID, Port Vlan) in the LLDP packet sent to the Avaya IP phone connected to the port.
1 of 2	

Table 11: Device Configuration fields - 802.1x tab (continued)

Field	Description
Max Number of Supplicants	The maximum number of supplicants in a device or system.
Current Number of Supplicants	The current number of supplicants connected to the device or system.
Authenticated Supplicants	The number of authenticated supplicants connected to the device or system.
Authenticating Supplicants	The number of supplicants connected to the device or system and who are being authenticated (not authenticated yet).
2 of 2	

Device Configuration - Protocol Status tab

The Protocol Status tab gives the status of all the protocols, irrespective of whether G430 supports the protocol or not.

Figure 8: Device Configuration Fields - Protocol Status tab

• G430-001 135.27.155.254 •

Protocol	Status
SCP Config File	On
SCP Image File	Not Supported
SSH	On
Telnet	On
SNMPv3	On
HTTP	On
HTTPS	Not Supported
Telnet Client	Off
ICMP Redirection	Not Supported
ICMP	On
Recovery Password	On
SSH Client	Not Supported
SNMPv1	On
ICMP Echo	On
FTP Client	On
TFTP	On

Buttons: Refresh, Apply, Undo, Delete, Insert

The following table provides a list of the fields in the Protocol Status tab of the Device Configuration dialog box and their description.

Table 12: Device Configuration fields - Protocol Status tab

Protocol	Supported by G430
SCP Config File	Y
SCP Image File	N
SSH	Y
Telnet	Y

Table 12: Device Configuration fields - Protocol Status tab

SNMPv3	Y
HTTP	Y
HTTPS	N
Telnet Client	Y
ICMP Redirection	N
ICMP	Y
Recovery Password	Y
SSH Client	N
SNMPv1	Y
ICMP Echo	Y
FTP Client	Y
TFTP	Y

Note:

All the fields in the Protocol Status tab are read-only. The Protocol Status fields reflect the CLI response for the command **Show protocol**. You cannot administer a protocol from the Device Manager. You can change a protocol only from the Device CLI.

The possible values for the protocols include **On**, **Off** and **Not Supported**.

Viewing Module Configuration

The Module Configuration dialog box provides you with information specific to a selected module.

- [Module Configuration - General tab](#) - Provides detailed information about the module, such as the module's position in the device, the module's type, description, number of ports, mode of operation, and the faults occurring on the module.
- Module Configuration - Power tab - Provides information about the module's Power over Ethernet (PoE) configuration. For more information, see ["Power over Ethernet" on page 67](#).

Note:

The information fields in the Module Configuration dialog box vary according to the type of module selected.

Module Configuration - General tab

To view the General tab of the Module Configuration dialog box for a selected module:

Click the module symbol in the Tree view.

Or

Click the module's label in the Chassis view.

Figure 9: Module Configuration dialog box - General tab

The screenshot shows a dialog box titled "MM716v5". Inside, there is a table with the following data:

MM Type	MM716
MM Description	Analog Media Module
Serial #	071640603824
HW Version	3A
FW Version	89
Number of Ports	24
Operational Status	OK

Below the table is a dropdown menu showing "No Fault Messages". At the bottom of the dialog box are two buttons: "Refresh" and "Apply".

Note:

Module Configuration fields may vary based on the Media Module.

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

Table 13: Module Configuration Dialog Box

Field	Description				
MM Type	Model of the media module. Support for the different devices is described below:				
	Module	Description	G350	G450	G430
	MM710	1 x voice T1/E1 port	Y	Y	Y
	MM711	8 x universal analog	Y	Y	Y
	MM712	8 x DCP 2 wire ports	Y	Y	Y
	MM714	Analog 4 line + 4 trunk	Y	Y	Y
	MM714 B				Y
	MM720	8 x ISDN BRI	Y	Y	Y
	MM722	2 x ISDN BRI	Y	Y	Y
	MM717	24 x DCP 2 wire ports	Y	Y	Y
	MM716	24 analog stations	Y	Y	Y
	MM340	1 x T1/E1 data		Y	
	MM342	1 x USP (V.35/X.21)	Y	Y	
	S8300B	Locally hosted CM server in ICC or LSP mode	Y	Y	
	S8300C	Locally hosted CM server in ICC or LSP mode	Y	Y	
	S8300D				
	MM312	24 DCP phone ports	Y		
	MM314	24 PoE Ethernet	Y		
MM Description	Description of the media module.				
Serial #	Unique identifier for an individual media module.				
HW Version	Release version of the Media module hardware.				
FW Version	Release version of the Media module firmware.				
Number of Ports	The number of ports in the media module.				
1 of 2					

Table 13: Module Configuration Dialog Box (continued)

Field	Description
Operational Status	The operational status of the media module. Possible values are: <ul style="list-style-type: none"> ● OK - Media module is operational. ● Down - Media module is reporting faults, making it unable to function. ● Fatal - Media module is reporting faults that are unrecoverable.
Fault Messages	The number of fault messages reported by the Media Module.
2 of 2	

Viewing Port Configuration

The Port Configuration dialog box contains tabs that provide you with information specific to a selected port.

- [Port Configuration - General tab](#) - Provides detailed information about the port, such as the port name, type, functionality, status, VLAN ID, mode of operation, and about the faults occurring on the port.
- [Port Configuration - Advanced tab](#) - Provides detailed information about the port's STP configuration and port classification.
- [Port Configuration - Power tab](#) - Provides information about the port's PoE configuration. For more information about PoE, see ["Power over Ethernet" on page 67](#).
- [Port Configuration - 802.1X tab](#) - Provides detailed information about the port's 802.1x security configuration.
- [Port Configuration - LLDP tab](#) - Provides detailed information about the port's LLDP configuration.
- [Get/Set toolbar](#) - Provides an alternative, quick method to view and change the port's configuration. For more information on Get/Set toolbar, see ["Get/Set toolbar" on page 27](#).

Port Configuration - General tab

To view the General tab of the **Port Configuration** dialog box for a selected port:

Click the port symbol in the Chassis view.

Or

Click the port's icon in the Tree view.

Figure 10: Port Configuration dialog box - General tab

The screenshot shows a dialog box titled "MM118v2, Port-1". It has five tabs: "General", "Advanced", "802.1x", "PoE", and "LLDP". The "General" tab is selected. The dialog contains the following fields and values:

Field	Value
Port Name	NO NAME
Port Type	Avaya G430 10or100TPortAndInPWR
Port Functionality	10/100 with Inline Power
Administrative Status	Enable
Tagging Mode	Clear
VLAN ID	1
Port Priority Level	User Priority 0
Auto Negotiation Mode	Enable
Auto Negotiation Status	In Progress
Duplex Mode	Half Duplex
Speed Mode	Ethernet
Flow Control Mode	No Flow Control
Operational Status	Warning
Fault Messages	1 Fault Message

At the bottom of the dialog are two buttons: "Refresh" and "Apply".

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

Note:

Some fields vary based on the media module on which the port resides.

Table 14: Port Configuration dialog box - General tab

Field	Description
Port Name	The user can define a logical name to the port for ease of use.
Port Type	The port type; optionally includes reference to the module to which it is attached and the port connector type.
Port Functionality	The physical media type of the selected port. If the port conforms to a certain standard (Repeater, Transceiver, 10BaseT, etc.), this standard is displayed. If the port does not conform to any standard, Private is displayed.
Administrative Status	The administrative state of the selected port: <ul style="list-style-type: none"> ● Enabled - the port is enabled and can transmit and receive packets. ● Disabled - the port is disabled and cannot transmit or receive packets.
Tagging Mode	The port's operational mode regarding VLANs. The possible modes are: <ul style="list-style-type: none"> ● Transmits each outgoing packet belonging to the port's VLAN in the untagged format. Otherwise, it discards the packet. ● VLAN tagging, per IEEE 802.1Q VLAN standard. The port transmits frames with a VLAN ID of 1 - 4090 for the Avaya G430 Device.
VLAN ID	The VLAN number of the port.
Port Priority Level	The priority level of packets exiting the port or ports on the module. For effective transmission, multimedia packets must be received at regular intervals. To ensure this, you can assign priorities to packets coming out of a port. Whenever the traffic load is extreme and a port cannot accept all incoming packets, packets from the port with the highest priority pass through first. However, a fairness mechanism allows low priority packets to eventually enter the bus. Possible values are: User Priority 0...User Priority 7
1 of 2	

Table 14: Port Configuration dialog box - General tab (continued)

Field	Description
Auto Negotiation Mode	<p>The configured state of the Auto-Negotiation protocol between two stations. When enabled, Auto-Negotiation detects the highest common denominator for communication between endstations, and sets both to the same highest common setting. It also delivers remote link status.</p> <p>For 10BaseT and 100BaseT ports, Auto-Negotiation determines the speed and Duplex Mode of communication between the endstations. For Gigabit ports, Auto-Negotiation determines the Flow Control setting of the ports.</p> <p>For more information, see <i>Auto-Negotiation</i> in <i>The Reference Guide</i>.</p>
Auto Negotiation Status	<p>The operational state of the Auto-Negotiation protocol between two stations. Possible statuses are:</p> <ul style="list-style-type: none"> ● Pass - the Auto-Negotiation protocol is enabled and a common protocol is established. ● In Progress - the Auto-Negotiation protocol is in the process of detecting the communication capabilities of the endstations and setting them to the highest common denominator. ● Fail - the Auto-Negotiation protocol is not able to detect the communication capabilities of the end station, or it is unable to set them to the highest common denominator. ● Disabled - The Auto-Negotiation protocol is disabled.
Duplex Mode	<p>The state of communication of the selected port. Possible values are:</p> <ul style="list-style-type: none"> ● Full Duplex - the port can send and receive simultaneously. ● Half Duplex - the port can either receive or send, but cannot do both simultaneously.
Speed Mode	<p>The rate of communication of the selected port. Possible values are:</p> <ul style="list-style-type: none"> ● Ethernet ● Fast Ethernet ● Gigabit Ethernet
Flow Control Mode	The state of flow control on the selected port.
Operational Status	<p>The warning level of the selected port. Possible values are:</p> <ul style="list-style-type: none"> ● OK ● Warning ● Fatal
Fault Messages	A list of fault messages.
2 of 2	

For more information on user interface, see [“Using dialog boxes and tables” on page 32](#).

Port Configuration - Advanced tab

To view the Advanced tab of the Port Configuration dialog box for a selected port:

1. Click the port symbol in the Chassis view.

Or

Click the port's icon in the Tree view. The system displays the general tab of the Port Configuration dialog box.

2. Click the Advanced tab. The system displays the advanced tab of the Port Configuration dialog box.

Figure 11: Port Configuration dialog box - Advanced tab

The screenshot shows the 'Advanced' tab of the 'Port Configuration' dialog box for 'MM118v2, Port-1'. The dialog box has a yellow background and a title bar with a close button. Below the title bar are five tabs: 'General', 'Advanced' (selected), '802.1x', 'PoE', and 'LLDP'. The 'Advanced' tab contains the following configuration options:

Port STP Mode	Enable
Port STP State	Not Connected
STP Admin Edge	Edge
STP Oper Edge	Edge
STP Admin P2P	Auto
STP Oper P2P	False
STP Admin Path Cost	100
STP Path Cost	100
STP Priority	128
STP Force Migration	<input type="checkbox"/>
Port Classification	Regular

At the bottom of the dialog box are two buttons: 'Refresh' and 'Apply'.

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

Table 15: Port Configuration dialog box - Advanced tab

Field	Description
Port STP Mode	Configured status of the Spanning Tree. Possible values are: <ul style="list-style-type: none"> ● Enable ● Disable
Port STP State	The Spanning Tree state on the port. Possible values are: <ul style="list-style-type: none"> ● Blocking - The port is blocking the attempts to join the Spanning Tree. ● Listening - The port is discovering other devices in the Spanning Tree. ● Learning - The port is calculating Spanning Tree values prior to joining the Spanning Tree. ● Forwarding - The port is forwarding traffic within the Spanning Tree.
STP Admin Edge	The administrative state of the edge port parameter. Possible states include: <ul style="list-style-type: none"> ● TRUE - This port is assumed to be an edge port. ● FALSE - This port is not assumed to be an edge-port.
STP Oper Edge	The operational state of the edge port parameter. <ul style="list-style-type: none"> ● TRUE - This port is operating in the state specified in the STP Admin Edge. ● FALSE - A BPDU is received by the port.
STP Admin P2P	The administrative point-to-point status of the LAN segment attached to this port. Possible statuses include: <ul style="list-style-type: none"> ● True - The port should always be treated as if it is connected to a point-to-point link. ● False - The port should be treated as having a shared media connection. ● Auto - The port is considered to have a point-to-point link if it is an Aggregator and all of its members are aggregative. The port can also have a point-to-point link if the MAC entity is configured for full duplex operation, either through auto-negotiation or by management means.
STP Oper P2P	The operational point-to-point status of the LAN segment attached to this port. It indicates whether or not a port is considered to have a point-to-point connection. The value is determined by the STP Admin P2P.
1 of 2	

Table 15: Port Configuration dialog box - Advanced tab (continued)

Field	Description
STP Admin Path Cost	The value assigned by the administrator for the contribution of this port towards the spanning tree root. A value of 0 assigns the automatically calculated default Path Cost value to the port. STP Admin Path Cost complements the STP Path Cost, which returns the operational value of the path cost.
STP Path Cost	The operational cost factor used by the Spanning Tree Algorithm to determine the most efficient route for forwarding traffic to its destination, while removing loops in the network. For more information, see <i>Spanning Tree Algorithm (STA)</i> in <i>The Reference Guide</i> .
STP Priority	The priority factor used by STP to determine the activity status of an individual port on the Spanning Tree.
STP Force Migration	When selected and in RSTP mode, the port is forced to transmit the RSTP BPDUs.
Port Classification	The classification of a specific port. Port Classification allows network managers to specify each port level's importance. The possible states are: <ul style="list-style-type: none"> ● Regular - Normal Users ● Valuable - Servers or critical users. For more information, see <i>Port Classification</i> in <i>The Reference Guide</i> .
2 of 2	

For more information on user interface, see [“Using dialog boxes and tables” on page 32](#).

Port Configuration - 802.1X tab

802.1x port security requires a user connected to a port on the network to be authenticated by an authentication server.

When a user connects to a port configured with 802.1x port security, the port forwards an authentication packet to a Radius authentication server. The authentication server checks if the user is authorized to use the port, and either allows or blocks the user's access to the port.

The port can be configured to automatically reauthenticate the user. If the reauthentication fails, the user is denied further access to the port. For more information, see [“Port Configuration - General tab” on page 50](#).

The 802.1x application supports two modes of operation:

- Port-based-authentication, which is backwards compatible with the previous 802.1x application behavior. This is used for a single-suppliant case.

- MAC-based-authentication for cases where multiple supplicants are connected per port.
For more information, see [“Device Configuration - 802.1x tab” on page 43](#).

The 802.1X tab of the Port Configuration dialog box provides you with detailed 802.1X authentication information about the selected port.

Figure 12: Port Configuration dialog box - 802.1X tab

• MM118v2, Port-1 •

General Advanced **802.1x** PoE LLDP

EAP State	Initialize
Backend Auth State	Initialize
Controlled Port Status	Authorized
Controlled Port Control	Auto
802.1x Port Mode	Port Based Authenticati...
Initialize	<input type="checkbox"/>
Reauthenticate	<input type="checkbox"/>
Quiet Period (sec)	60
Tx Period (sec)	30
SuppTimeout (sec)	30
Server Timeout (sec)	30
Max Request	2
ReAuthPeriod (sec)	3600
ReAuthEnabled	False
Current Number of Supplica...	0
Authenticated Supplicants	0
Authenticating Supplicants	0

Refresh Apply

The following table provides a list of fields in the 802.1X table of the Port Configuration dialog box and their descriptions:

Table 16: Port Configuration dialog box - 802.1X tab parameters

Field	Description
EAP State	<p>Entry Access Protocol authentication status. Possible values are:</p> <ul style="list-style-type: none"> • Initialize • Disconnected • Connecting • Authenticating • Authenticated • Aborting • Held • Force Auth • Force Unauth
Backend Auth State	<p>The current status of the Backend Authentication state machine. Possible values are:</p> <ul style="list-style-type: none"> • Request • Response • Success • Fail • Timeout • Idle • Initialize
Controlled Port Status	<p>The current value of the Controlled Port status. Possible values are:</p> <ul style="list-style-type: none"> • Authorized • Unauthorized
Controlled Port Control	<p>The current status of the Controlled Port control. Possible values are:</p> <ul style="list-style-type: none"> • Force Authorized • Force Unauthorized
IEEE-802.1X Port Mode	<p>The 802.1x mode of operation. Possible values are:</p> <ul style="list-style-type: none"> • Port Based Authentication - used for a single-supplicant case. This mode is backwards compatible with the previous 802.1x application behavior. • MAC Based Authentication - for cases where multiple supplicants are connected per port. For more information, see "Device Configuration - 802.1x tab" on page 43.
Initialize	<p>Forces initialization of the port. Selecting the Initialize check box and clicking Apply forces the port to be initialized immediately. This check box is active only when IEEE-802.1x mode is enabled.</p>
1 of 2	

Table 16: Port Configuration dialog box - 802.1X tab parameters (continued)

Field	Description
Reauthenticate	Forces reauthentication of the port. Selecting the Reauthenticate check box and clicking Apply forces the port to be reauthenticated immediately. This check box is active only when IEEE-802.1x mode is enabled.
Quiet Period (seconds)	The amount of time, in seconds, between authentication requests.
Tx Period (seconds)	The amount of time, in seconds, in which an authentication request must be answered.
Supp Timeout (seconds)	The amount of time, in seconds, after which an authentication request is suppressed.
Server Timeout (seconds)	The amount of time, in seconds, before timing out an authentication request.
Max Request	The maximum number of times a request for authentication is sent before timing out.
ReAuthPeriod (seconds)	The amount of time, in seconds, after which the port connection is reauthenticated.
ReAuth Enabled	The state of reauthentication of the port. Possible values are: <ul style="list-style-type: none"> • True - The port connection is reauthenticated after the reAuth Period. • False - The port connection is not reauthenticated. The reAuth Period is ignored.
Current Number of Supplicants	The current number of supplicants on this port.
Authenticated Supplicants	The number of authenticated supplicants on this port.
Authenticating Supplicants	The number of supplicants connected to the port who are being authenticated (not authenticated yet).
2 of 2	

For more information on user interface, see [“Using dialog boxes and tables” on page 32](#).

Port Configuration - LLDP tab

Link Layer Discovery Protocol (LLDP) is a neighbor discovery protocol, which allows Ethernet network devices to search for, and request information from other LLDP enabled devices on the network. LLDP defines a standard method for Ethernet network devices, such as switches, routers, and wireless LAN access points, to advertise information about themselves to other nodes on the network.

LLDP also allows Ethernet network devices to search for, and request information from other devices using the LLDP protocol.

The following details are advertised using LLDP on the Avaya G430 Device:

- System Name
- Chassis ID
- Port ID
- System Description
- System Capabilities
- Port Description
- Management Address

Note:

Chassis ID and Port ID are always advertised when LLDP is enabled.

To view the LLDP tab of the Port Configuration dialog box for a selected port:

1. Click the port symbol in the Chassis view.

Or

Click the port's icon in the Tree view. The system displays the General tab of the Port Configuration dialog box.

2. Click **LLDP**. The system displays the LLDP tab of the Port Configuration dialog box.

Figure 13: Port Configuration dialog box - LLDP tab

• MM118v2, Port-1 •

General

Advanced

802.1x

PoE

LLDP

LLDP Admin Status

TX and RX

LLDP TLVs Transmission

System Name

System Description

System Capabilities

Port Description

Management Addr

LLDP TLVs Reception

Chassis

Port Id

Port Descrip

System Na

System Descrip

System Cap

Manag

Refresh

Apply

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

Table 17: Port Configuration Dialog Box - LLDP tab parameters

Field	Description
LLDP Admin Status	The status of the LLDP mode on the device. Possible values are: <ul style="list-style-type: none">● Tx Only - The LLDP mode is enabled, and is configured to only accept Tx traffic.● Rx Only - The LLDP mode is enabled, and is configured to only accept Rx traffic.● Tx and Rx - The LLDP mode is enabled and is configured to accept both Tx and Rx traffic.● Disabled - The LLDP mode is disabled.
1 of 2	

Table 17: Port Configuration Dialog Box - LLDP tab parameters (continued)

Field	Description
LLDP TLVs Transmission	
System Name	The system's network name. When selected, the system advertises its name to the network.
System Description	A brief description of the system (G430). When selected, this TLV is advertised.
System Capabilities	A brief description of the system's capabilities. When selected, this TLV is advertised.
Port Description	A brief description of the device port. When selected, this TLV is advertised.
Management Addr	The device's management address. When selected, this TLV is advertised.
LLDP TLVs Reception	
Chassis Id	The received Chassis ID TLV.
Port Id	The received Port ID TLV of the device port.
Port Description	The received Port Description TLV of the device port.
System Name	The received System Name TLV associated with the Chassis ID.
System Description	The received System Description TLV associated with the Chassis ID.
System Capabilities	The received System Capabilities TLV associated with the Chassis ID.
Management Address	The received IP Management Address TLV associated with the Chassis ID.
2 of 2	

Configuring the external modem

You can configure and view information specific to an external modem connected through the USB ports using the **L2 Device Manager** dialog box. These ports are context sensitive, and the Modem tab for each port is distinct.

Note:

To configure a dial-up modem, see [““Configuring the dialer” on page 64”](#).

Device Configuration

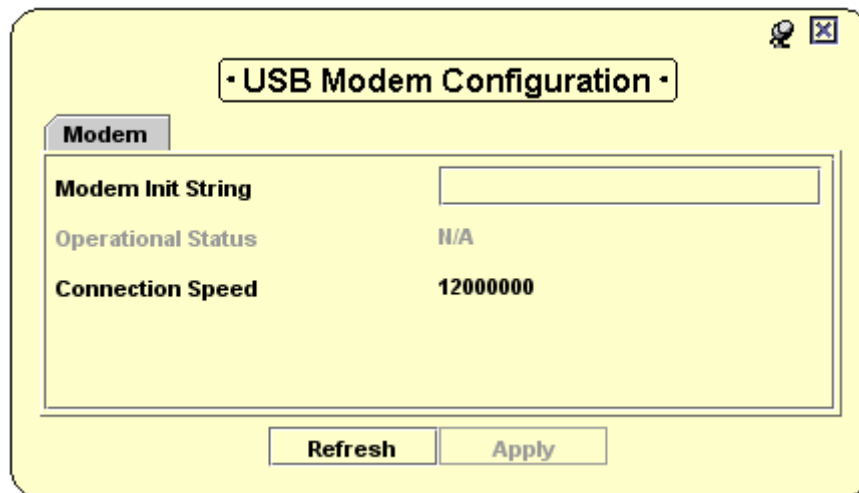
To view the L2 Device manager for an USB port:

In the Chassis view, click an USB icon.

Or

In the Tree view, click an USB icon.

Figure 14: G430 L2 Device Manager dialog box - USB port



The screenshot shows a dialog box titled "• USB Modem Configuration •". It has a "Modem" tab selected. Inside the tab, there are three rows of information: "Modem Init String" with an empty text input field, "Operational Status" with the value "N/A", and "Connection Speed" with the value "12000000". At the bottom of the dialog, there are two buttons: "Refresh" and "Apply".

Note:

The Avaya G430 Media Gateway has two USB ports. However, the Avaya G430 Manager cannot identify on which of the ports a modem is connected. Therefore, when you click either of the ports, you can configure a modem connected to either of the ports.

The following table provides a list of the fields in the L2 Device Manager for the USB port.

Table 18: L2 Device Manager dialog box - USB port parameters

Field	Description
Modem Init String	The string used to initialize the external modem.
Connection Speed	The connection speed of the modem. Note: This field is visible only if a modem is connected.

Table 18: L2 Device Manager dialog box - USB port parameters

Field	Description
Operational Status	<p>The operational status of the external modem. Possible states include:</p> <ul style="list-style-type: none">● Modem Undetected - no modem is detected.● Modem Ready - the modem is ready.● Modem Connected Dial-In - the modem detected a dial-in modem.● Modem Connected Dial-Out - the modem detected a dial-out modem.

Configuring the dialer

You can configure an external dial-up modem attached to the device using the **Dialer Configuration** dialog box.

To view the Dialer:

Select **Configure > Dialer**.

Figure 15: Dialer Configuration dialog box

✕

Dialer Configuration

Dialer Modem Port	USB
Dialer Admin Status	Enable
Persistent Delay	1
Persistent Initial Delay	0
Maximum Attempts	0
Re-enable Delay	0
IPCP Timeout	45
Dialer Order	Sequential
Dial String 1	
Dial String 2	
Dial String 3	
Dial String 4	
Dial String 5	
Dialer Status	N/A
Last Dialed String	N/A

Refresh

Apply

The following table provides a list of fields in the **Dialer Configuration** dialog box.

Table 19: Dialer Configuration parameters

Field	Description
Dialer Modem Port	The port through which the dialer operates. Possible values include: <ul style="list-style-type: none"> ● USB ● None Selecting USB automatically creates the “Dialer PPP” interface.
Dialer Admin Status	The admin status of the dialer. Possible values include: <ul style="list-style-type: none"> ● Enable ● Disable
Persistent Delay	The number of seconds the dialer waits, after an error disrupts the system, before attempting the re-establish a connection. The default value is 0.
Persistent Initial Delay	The number of seconds the dialer waits, after the system is configured or rebooted, before attempting to establish a connection. The default value is 0.
Maximum Attempts	The maximum number of connection attempts the dialer makes after an error has disrupted the system. The default value is 0.
Re-enable Delay	The amount of time the dialer waits before re-enabling. The default value is 0.
IPCP Timeout	The number of seconds the dialer waits for a reply before considering the request a failure. The default value is 45.
Dialer Order	The order the dialer attempts its connection in. Possible values are: <ul style="list-style-type: none"> ● Sequential - the dialer attempts each dial string in sequential order. ● Round Robin - the dialer attempts each dial string in random order. ● Last Successful - the dialer attempts the last dial string with which it made a successful connection.
Dial String 1	A string the dialer is instructed to dial.
Dial String 2	A string the dialer is instructed to dial.
Dial String 3	A string the dialer is instructed to dial.
Dial String 4	A string the dialer is instructed to dial.
Dial String 5	A string the dialer is instructed to dial.
1 of 2	

Table 19: Dialer Configuration parameters (continued)

Field	Description
Dialer Status	The status of the dialer. Possible values include: <ul style="list-style-type: none"> ● Init Modem ● Idle ● Waiting for Modem ● Max Attempts Disabled ● Pre Dial Reset ● Wait for Connect ● Wait for DCD ● Hang Up ● Persistent Delay ● Wait for IPCP ● Connected
Last Dialed String	The last string to which the dialer attempted to connect.
2 of 2	

Resetting the device

You can reset the entire Avaya G430 Device, or one or more of its individual modules.

To reset the entire Avaya G430 Device:

1. Select **Action > Reset Device**. The system displays the confirmation dialog box.
2. Click **Yes**.

To reset an individual Avaya G430 Media Module:

1. Click the label of the media module you want to reset.
To select multiple modules, press **Control** while clicking additional module labels.
2. Select **Actions > Reset Media Module(s)**. The system displays the confirmation dialog box.
3. Click **Yes**.

To reset an external modem (USB):

1. Click the label of the modem you want to reset.
2. Select **Actions > Reset Modem**. The system displays the confirmation dialog box.
3. Click **Yes**.

Chapter 4: Power over Ethernet

This chapter provides information about Power over Ethernet (PoE) and includes the following sections:

- [PoE overview](#) - An overview of the Power over Ethernet feature in the Avaya G430 device.
- [Viewing PoE information](#) - Information about viewing PoE port information and configuring PoE on a module and port level.

PoE overview

PoE provides power to IP telephones over an Ethernet line. The power is transmitted through the device's ports to the IP telephones over the same cable carrying IP packets.

The Avaya G430 Device automatically discovers the connection and removal of IP telephones from the in-line powered ports and provides power accordingly.

In addition, you can configure power priorities per port ensuring that important equipment is guaranteed power whenever necessary.

Viewing PoE information


This section provides information about viewing port information and configuring PoE on the port and module level. This section includes:

- [Viewing PoE port information](#)
- [Viewing PoE configuration](#)

Note:

Power over Ethernet for the G430 Device is not available in the 5.2 release.

Viewing PoE port information

The Chassis view provides immediate information about PoE. Ports that are currently supplying power to IP telephones are labeled with the  icon.

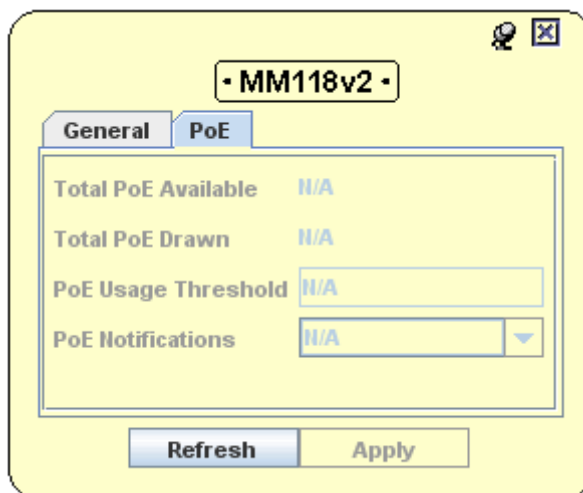
Viewing PoE configuration

You can view the PoE configuration information on the module and port levels.

PoE module configuration

To view the PoE configuration on a module that supports PoE, select the **Power** tab in the module's configuration dialog box. For information on opening the Module Configuration dialog box, see [“Viewing Module Configuration” on page 46](#).

Figure 16: Module configuration - Power tab



The following table provides a list of fields in the Power tab of the Module Configuration dialog box and their descriptions:

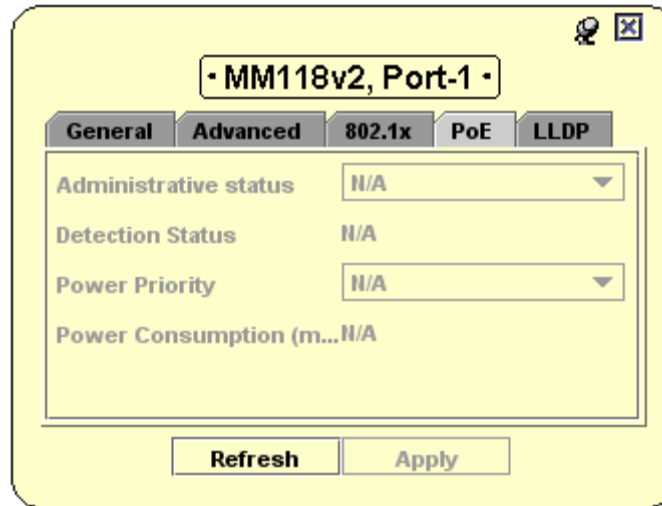
Table 20: Module configuration - Power fields

Field	Description
Total PoE Available	The power available to distribute to devices connected to this module.
Total PoE Drawn	Total power currently distributed to devices connected to this module.
PoE Usage Threshold	Percentage of the total available power currently distributed to devices connected to this module.
PoE Notifications	When selected, PoE notifications are available at the module level.

PoE port configuration

To view the PoE configuration on a port that supports PoE, select the **Power** tab in the port's configuration dialog box. For more information on opening the Port Configuration dialog box, see [“Viewing Port Configuration” on page 49](#).

Figure 17: Port configuration - Power tab



The following table provides a list of the fields in the Power tab of the Module Configuration dialog box and their descriptions:

Table 21: Port configuration - Power fields

Field	Description
Administrative Status	The administrative state of the port in terms of power management. Possible states include: <ul style="list-style-type: none"> ● Enable - This port supplies power to IP telephones. ● Disable - This port cannot supply power to IP telephones.
Detection Status	The operational status of port power detection. Possible states include: <ul style="list-style-type: none"> ● Searching - This port is currently being polled. ● Delivering Power - This port is supplying power to an IP telephone. ● Fault - This port is currently not supplying power to an IP telephone due to a fault condition on the port. ● Disabled - This port is currently not configured to supply power to an IP telephone. ● Test - This port is being tested for its ability to deliver power. ● Other Fault - This port is currently not delivering power to an IP telephone due to a fault condition other than on the port.

Table 21: Port configuration - Power fields (continued)

Field	Description
Power Priority	<p>The priority of the port in terms of power management. When the demand for power exceeds the modules capacity, ports with lower priority are prevented from supplying power before ports with a higher priority. Possible priorities include:</p> <ul style="list-style-type: none"> ● Critical ● High ● Low
Power Consumption (mW)	The power consumption of the port in milliwatts.

Chapter 5: Media Gateway Functions

This chapter provides information about Avaya G430's Media Gateway functionality. It includes the following sections:

- [Viewing media gateway configuration](#) - An overview of the media gateway in the Avaya G430 Device.
- [Media gateway configuration](#) - Information about viewing and configuring media gateway components.
- [Avaya Site Administration](#) - Information about Avaya's gatekeeper software.

Media gateway overview

The media gateway is a family of components, which can deliver data, voice, fax, and messaging capabilities over an IP network. It is a VoIP system that acts as an IP PBX and messaging server, and a VoIP gateway. In addition, it performs the function of a gatekeeper and an IP media management resource for tone detection and generation, conferencing, and call classification.

The media gateway components are controlled through the Media Gateway Processor (MGP). The MGP detects when a media module is inserted or removed and transfers information from the VoIP engine to other components.

The Avaya G430's Media Gateway converges the power of Avaya Call Processing (ACP) software with the power of distributed switching from the Avaya G430 Device. It provides IP PBX functionality using open standards and an open operating system. The device connects to the ACP either using an internal or an external call controller. The ACP serves as the Avaya G430 Device's gatekeeper.

Media gateway configuration

This section describes how to view and set the various configuration parameters relevant to the G430 Media Gateway. It includes the following sections:

- [Media gateway configuration](#) - View information specific to a G430 Media Gateway module in the device.
- [Viewing Media Module configuration](#) - View information specific to a media module in the device.

Viewing media gateway configuration

The Media Gateway Configuration dialog box provides you with information about a selected module.

To view the configuration of the Media Gateway:

1. Select **Configure > Device Configuration**. The system displays the Device Manager dialog box.
2. Select the **MG Config** tab. The system displays the MG Config dialog box.

MG Config

The **MG Config** tab provides information about the Media Gateway QoS parameters.

Figure 18: MG Config tab

The screenshot shows a dialog box titled "G430-000 135.27.162.80". It has three tabs: "MG Config", "VoIP resources", and "VoIP status". The "MG Config" tab is active, showing two sub-tabs: "General" and "Advanced". The "Advanced" sub-tab is selected, displaying the following information:

QoS Parameters	
QoS Control	Remote
DSCP	0
802 Priority	0

MGP Operational Status	Fatal
------------------------	-------

Below the status table, there is a dropdown menu showing "2 Fault Messages". At the bottom of the dialog box, there are five buttons: "Refresh", "Apply", "Undo", "Delete", and "Insert".

The following table lists the fields in the MG Config tab of the Module Configuration dialog box and their descriptions.

Table 22: MG Config parameters

Field	Description
QOS Control	The source of QoS control. This parameter can only be changed through the CLI. Possible values are: <ul style="list-style-type: none">● Local - The processor is using the local QoS parameters. The 802 priority and DSCP fields can be configured.● Remote - The processor is receiving QoS parameters from a remote Media Gateway. All QoS parameters are read-only.
DSCP	Priority based on a technology by which packets are marked in the IP header Type of Service (ToS) byte as belonging to a specific class. Possible values are 0 - 63 .
802 Priority	Priority based on the 802.1x standard, which assigns rights and privileges to users on a telephony network. Possible values are 0 - 7 .
Operational Status	Operational Status of the Media Gateway. Possible values are: <ul style="list-style-type: none">● OK - The Media Gateway is operating properly.● Fatal - The Media Gateway is down.
Fault Messages	A list of fault messages.

MGC Config

The **MGC Config** tab provides information about the Media Gateway Controller's settings, IP address, and registration information.

Figure 19: MGC Config tab

G430-000 135.27.162.80		
MG Config	VoIP resources	VoIP status
General	Advanced	MGC Config
MGC IP Address 255.255.255.255		
Registered status Not Registered		
H248 Link status Down		
Configurable MGC list		
#	IP address	
1	135.27.162.81	

Refresh Apply Undo Delete Insert

The MGC registers with the Media Gateway, after which it receives its IP address from the Media Gateway. After you register, the **H.248 Link status** changes to **Up**, and an IP address appears.

The following table lists the MGC IP Settings fields and their descriptions.

Table 23: MGC Config - MGC IP Settings Parameters

Field	Description
MGC IP Address	The IP address of the call controller serving the media gateway.
Registered status	Shows whether this media gateway is currently registered with any call controller.
H248 Link status	Status of the link connecting the media gateway to the active call controller.
Configurable MGC list	A list of Media Gateway Controllers accessible to the G430 Device and their associated IP addresses.

Viewing Media Module configuration

The Media Module Configuration dialog box enables you to view the hardware and firmware information for a specific media module, and its operational status.

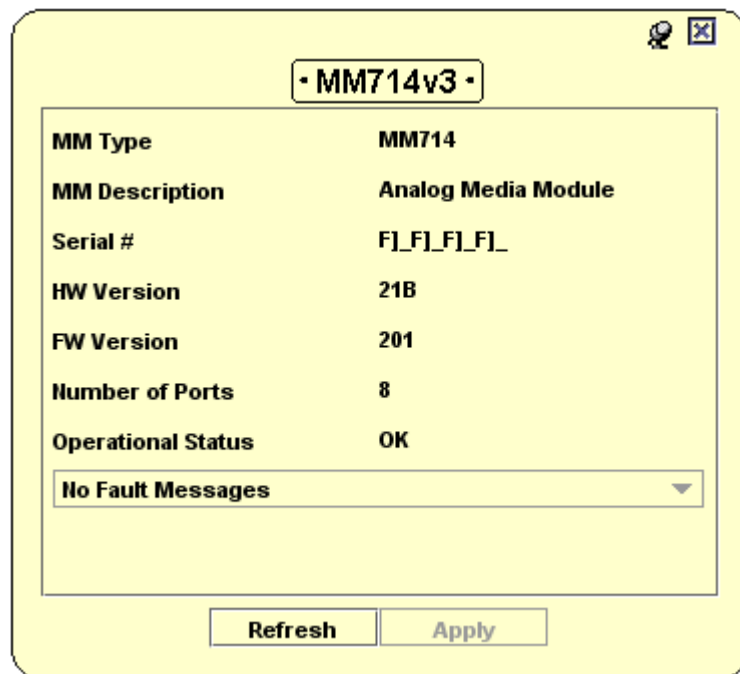
To view the configuration for a selected media module:

In the Configuration Mode, click the media module symbol in the Tree view.

Or

Click the media module's label in the Chassis view.

Figure 20: Media Module Configuration dialog box



The dialog box displays configuration details for a media module. At the top, a title bar shows '- MM714v3 -'. Below this, a table lists various attributes and their values. At the bottom, there is a dropdown menu for fault messages and two buttons: 'Refresh' and 'Apply'.

Attribute	Value
MM Type	MM714
MM Description	Analog Media Module
Serial #	F]_F]_F]_F]_
HW Version	21B
FW Version	201
Number of Ports	8
Operational Status	OK

No Fault Messages

Refresh Apply

Media Gateway Functions

The following table lists the fields in the Media Module Configuration dialog box and their descriptions.


Table 24: Media Module Configuration parameters

Field	Description
MM Type	The type of media module.
MM Description	An optional description of the specific media module.
Serial #	The serial number of the media module.
HW Version	The version of the media module's hardware.
FW Version	The firmware version of the media module.
Number of Ports	The number of ports on the media module.
Operational Status	The operational status of the media module. Possible values are: <ul style="list-style-type: none">● OK - The media module is operating normally.● Down - The media module is down due to a fault.● Fatal - The media module is down due to a fatal error.
Fault Messages	A list of fault messages.

Avaya Site Administration

Avaya Site Administration (ASA) is an administration tool for the Avaya Call Processing call control software. ASA is used to configure the current MGC or an individual voice port.

To launch the ASA on an MGC or a voice port:

1. Click the MGC or voice port in the Tree view or Chassis view.
2. Click .

Or

Select **Action > Administer Station/Gateway**.

If you have a registered call controller MM installed in your Avaya G430 Media Gateway, you can launch the ASA on the call controller.

To launch the ASA on a registered call controller Media Module:

1. Select the registered call controller Media Module.
2. Select **Tools > Administer Call Controller**.

For more information about ASA, see Avaya Site Administration Documentation.

Chapter 6: VoIP Engine Configuration

This chapter provides information and instructions for viewing and configuring the VoIP Engine features. It includes the following sections:

- [VoIP overview](#) - An overview of the VoIP Engine feature within the Media Gateway.
- [VoIP resources](#) - Instructions for viewing and configuring the VoIP Engine parameters.
- [VoIP status](#) - Instructions for determining the operational status of the VoIP Engine.

VoIP overview

The VoIP Engine translates information between different VoIP and data protocols. The Media Gateway comes with an internal VoIP engine that supports up to 32 simultaneous sessions. Each media gateway supports different numbers of channels.

You can view information and configure parameters for the VoIP Engine using the VoIP Engine dialog box.

To view the VoIP Engine dialog box:

Select **View > Configure**.

In the Device Manager dialog box, there are two tabs for managing the VoIP engine:

- [VoIP resources](#) - Administrative parameters common to all VoIP engines.
- [VoIP status](#) - Operating Status for a selected VoIP engine.

VoIP resources

The **VoIP resources** tab provides the administration parameters common to all VoIP engines, such as QoS parameters, RTCP configuration, and RSVP configuration.

Figure 21: VoIP resources tab

The screenshot shows a web-based configuration interface for a VoIP engine. At the top, there is a header bar with three tabs: "MG Config", "VoIP resources" (which is selected), and "VoIP status". Below this, there is a sub-header bar with three sub-tabs: "General", "Advanced", and "MGC Config". The "General" sub-tab is currently active. The main content area is divided into several sections. At the top, there is a text box containing the identifier "G430-000 135.27.162.80". Below this, the "General" section contains the following parameters: "RTP Port min" set to 2048, "RTP Port max" set to 65535, and "QOS Control" set to Remote. A "QOS" section follows, containing "802 Priority" set to 6, "EF DSCP" set to 46, and "BBE DSCP" set to 43. An "RTCP monitoring" section contains "Monitoring enabled" (unchecked), "IP address" set to 0.0.0.0, "Port" set to 5005, and "Report Period" set to 5. An "RSVP" section contains "RSVP Enabled" (unchecked), "Retry on failure" (checked), "Retry Delay" set to 15, and "Service profile" set to "guaranteed" (selected from a dropdown menu). At the bottom of the interface, there are five buttons: "Refresh", "Apply", "Undo", "Delete", and "Insert".

MG Config		VoIP resources		VoIP status	
General		Advanced		MGC Config	
RTP Port min					
		2048			
RTP Port max					
		65535			
QOS Control					
		Remote			
QOS					
802 Priority		6			
EF DSCP		46			
BBE DSCP		43			
RTCP monitoring					
Monitoring enabled		<input type="checkbox"/>			
IP address		0.0.0.0			
Port		5005			
Report Period		5			
RSVP					
RSVP Enabled		<input type="checkbox"/>			
Retry on failure		<input checked="" type="checkbox"/>			
Retry Delay		15			
Service profile		guaranteed			

Refresh Apply Undo Delete Insert

General:

The upper section of this dialog box displays general information common to all VoIP engines.

The following table lists the general fields in the **VoIP resources** tab of the VoIP Engine dialog box and their description.

Table 25: VoIP resources - General parameters

Field	Description
RTP Port min	The minimum range of UDP ports assigned by the call controller for RTP traffic. The value ranges between 1 - 65534 .
RTP Port max	The maximum range of UDP ports assigned by the call controller for RTP traffic. The value ranges between 3 - 65535 .
QOS Control	The source of QoS control. This parameter can only be changed through the CLI. Possible values are: <ul style="list-style-type: none"> ● Local - The processor uses the local QoS parameters. If the processor is using the local QoS parameters, the 802 Priority, EF DSCP, and BBE DSCP fields can be configured. ● Remote - The processor receives its QoS parameters from the Media Gateway Controller. All QoS parameters are read-only.

QoS

QoS can be controlled either locally or remotely. If the control is local, it is possible to configure QoS, RTCP, and RSVP parameters. If the control is remote, QoS parameters are determined by the MGC.

The following table lists the QoS fields and their descriptions.

Table 26: VoIP resources - QoS parameters

Field	Description
802 Priority	Priority based on a CoS standard which assigns rights and privileges to users of a telephony network. Possible values range between 0 - 7 .
EF DSCP	A type of differentiated service used to provide guaranteed bandwidth across a network. If sufficient bandwidth is available, the Expedited Forwarding class can be used. The value ranges between 0 - 63 .
BBE DSCP	A DiffServ class which is used per call to achieve the greatest possible bandwidth. The values range between 0 - 63 .

RTCP Monitoring

RTCP is an IP protocol that is used to monitor the quality of RTP packets. Quality is measured in terms of delay, jitter, and packet loss. If RTCP monitoring is enabled, the VoIP engines send the RTCP packets to the RTCP monitor. You must configure an IP address for the RTCP monitor, and determine intervals at which the RTCP data is checked.

The following table lists the RTCP monitoring fields and their descriptions..

Table 27: VoIP resources - RTCP monitoring parameters

Field	Description
Monitoring enabled	The status of RTCP monitoring. <ul style="list-style-type: none"> ● Selected - RTCP monitoring is enabled. ● Cleared - RTCP monitoring is disabled.
IP address	The IP address of the RTCP monitor.
Port	The port monitored by RTCP.
Report Period	The interval between RTCP reports.

RSVP

RSVP is a protocol that signals the router to reserve bandwidth for call sessions. If RSVP is enabled, the media gateway tries to reserve a specific amount of bandwidth per call session. If this fails, the media gateway tries to reallocate the bandwidth during the call session.

The following table lists the RSVP fields and their descriptions.

Table 28: VoIP resources - RSVP parameters

Field	Description
RSVP Enabled	The Status of RSVP usage. <ul style="list-style-type: none"> ● Selected - The Media Gateway tries to reserve bandwidth per call. If it fails, the Media Gateway again tries during the call. ● Cleared - RSVP is not enabled.
Retry on failure	The action that the VoIP engine takes after an RSVP request fails. <ul style="list-style-type: none"> ● Selected - The VoIP engine resends a RSVP request if the first attempt fails. ● Cleared - The VoIP Engine drops the RSVP request, and the Retry Delay field is ignored.
Retry Delay	The interval time between a failed RSVP request and a new request by the VoIP engine. The interval ranges between 0.5 - 60 seconds.
Service profile	The type of service that is provided.

VoIP status

The **VoIP status** tab provides information about a specific engine's operational status, jitter buffer size, and number of sessions that are open.

For Avaya G430 Devices, the **VoIP status** tab also provides the **VoIP DSP Core Status** table. This table displays information about the VoIP DSP Cores in the DSP media resource cards for the VoIP engine selected in the **VoIP Status** table.

Figure 22: VoIP status tab - G430

- G430-001 135.27.155.254 -

MG Config VoIP resources **VoIP status**

General Advanced MGC Config

- VoIP Status -

Slot #	Socket #	Channels in Use	Total Voice Channels	Jitter Buffer size	VoIP State	Operation Status
V1	1	0	20	2560	Release	OK
V2	2	0	80	2560	Release	OK

- VoIP DSP Core Status -

Core #	Total Channels	Channels in Use	VoIP State	Operational Status
1	20	0	Release	Idle
2	20	0	Release	Idle
3	20	0	Release	Idle
4	20	0	Release	Idle

No Fault Messages

Refresh Apply Undo Delete Insert

The information in the **VoIP Status** tab is provided by the VoIP engine and is refreshed periodically.

The following table lists the fields in the **VoIP status** tab and their descriptions.

Table 29: VoIP Status parameters

Field	Description
Slot #	The slot in which the VoIP engine resides.
Socket #	The socket number of the VoIP engine.
Channels in Use	The number of channels currently being used.
Total Voice Channels	The total number of voice channels available.
Jitter Buffer size	The jitter buffer is a temporary storage area built into the receiver of each gateway. It uses a mechanism to remove the random delays between packets, which occur as the packets are routed through the network.
VoIP State	The administrative state of the DSP core (read-only). Possible values are: <ul style="list-style-type: none"> ● Busy Outs ● Release ● Camp-On Busy Out ● Unknown
Operational Status	The operational status of the VoIP engine.

The following table lists the fields in the **VoIP DSP Core Status** table and their descriptions.

Table 30: VoIP DSP Cores Status parameters

Field	Description
Core #	The identification number of the DSP core in the selected DSP VoIP engine.
Total Channels	The total number of available DSP core channels.
Channels in Use	The number of channels currently in use in the DSP core.
VoIP State	The administrative state of the DSP core (read-only). Possible values are: <ul style="list-style-type: none"> ● Busy Out ● Release ● Camp-On Busy Out ● Unknown
Operational Status	The operational status of the DSP core.

For more information on user interface, see [“Using dialog boxes and tables” on page 32](#).

Chapter 7: Embedded Tools

This chapter provides information and instructions for configuring the embedded tools of the Avaya G430. It includes the following sections:

- [Configuring the DHCP server](#) - Instructions on configuring DHCP Server functionality.
- [Configuring the TFTP server](#) - Instructions on configuring TFTP Server functionality.
- [Configuring the Converged Network Analyzer application](#) - Instructions on configuring the Converged Network Analyzer (CNA) functionality.

Configuring the DHCP server

DHCP (Dynamic Host Configuration Protocol) server enables you to automatically assign IP addresses and other network parameters to remote stations not configured with static network parameters. A pool of allocated addresses and parameters are created on the server. The remote station, on network login, requests network parameters from the DHCP server. The DHCP server provides the remote station with parameters such as IP address, subnet mask, default gateway, and Domain Name Server (DNS) information.

The Avaya G430 Device acts as a DHCP server for devices physically connected to the Avaya G430 Device, and for other devices on the same network.

Configuring DHCP

DHCP configuration includes the following steps:

- [Configuring Basic DHCP options](#) - Basic configuration options for DHCP service.
- [Creating a new DHCP pool](#) - New allocation pool creation options for DHCP service.
- [Configuring DHCP pool parameters](#) - Allocation pool configuration options for DHCP service.
- [Configuring DHCP assignment parameters](#) - Parameter allocation options for DHCP service.

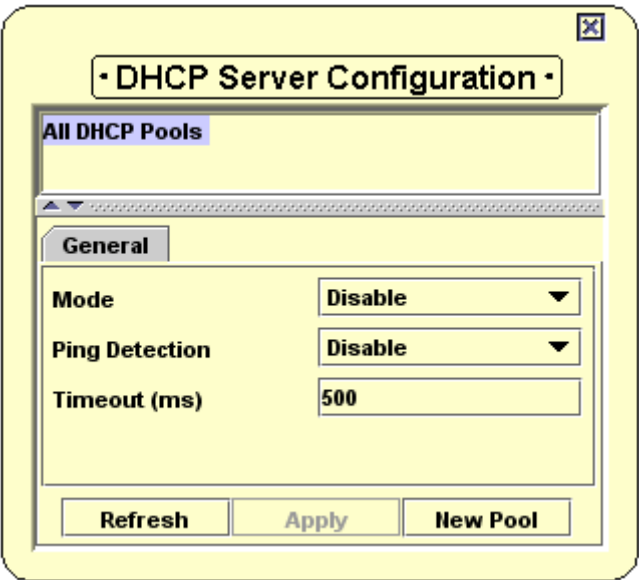
The DHCP Server dialog box is split into two sections. The top section shows the **All DHCP Pools** tree, a view of all available DHCP pools. You can click **All DHCP Pools** to manage the basic DHCP function and create a new pool, or click a specific pool to configure options for that pool.

To configure the DHCP server, select **Servers > DHCP Server** from the **Configure** menu. The system displays the General tab of the **DHCP Server Configuration** dialog box.

Configuring Basic DHCP options

The DHCP Server - General tab provides basic configuration options for activating the DHCP service.

Figure 23: DHCP Server Configuration - General tab



The following table provides a list of the fields in the DHCP Server Configuration - General tab and their descriptions:

Table 31: DHCP Server Configuration - General tab fields

Field	Description
Mode	Administrative status of the DHCP service. Possible values are: <ul style="list-style-type: none">• Enable• Disable
Ping Detection	When enabled, the DHCP server sends a ping packet to detect an IP address conflict before actually allocating the IP address to the DHCP client. Possible values are: <ul style="list-style-type: none">• Enable• Disable (default value)
1 of 2	

Table 31: DHCP Server Configuration - General tab fields (continued)

Field	Description
Timeout (milliseconds)	The timeout, in milliseconds, of the ping packet sent by the DHCP server to detect an IP address conflict before allocating the new IP address. Possible values are 25milliseconds – 1000 milliseconds. The default value is 500 milliseconds.
2 of 2	

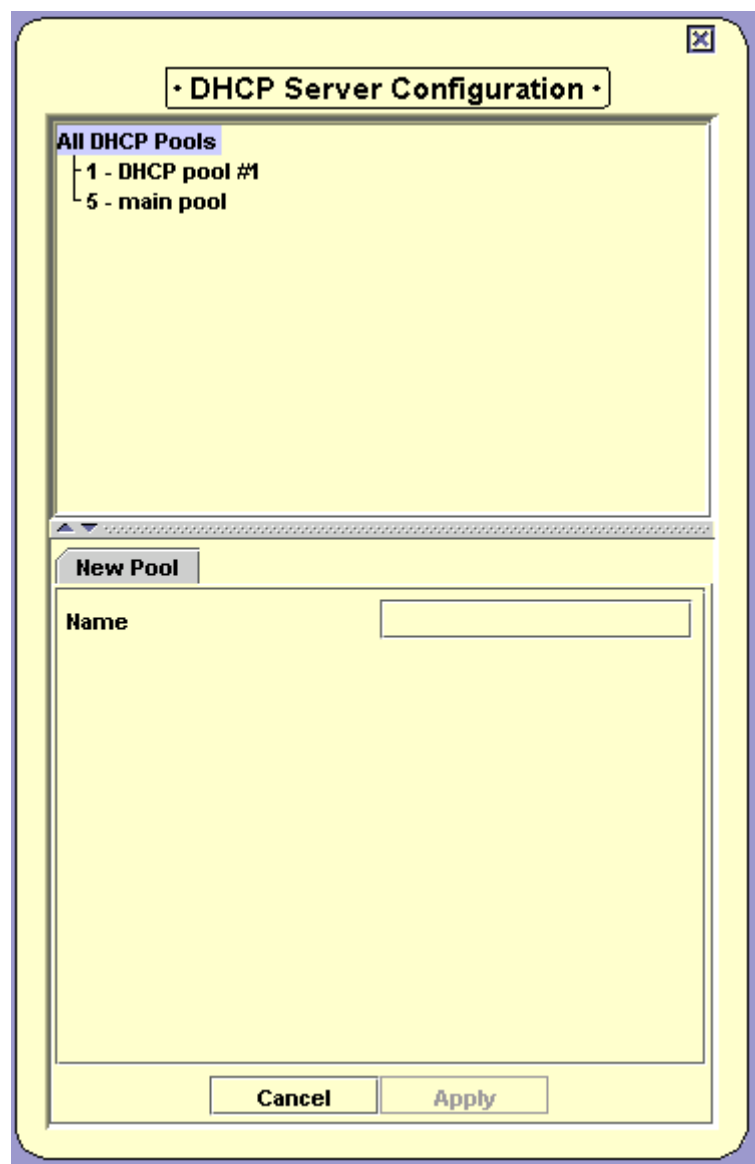
To refresh the tree view, click **Refresh**. To apply changes to the DHCP general configuration, click **Apply**.

To create a new pool, click **New Pool**. The system displays the New Pool tab of the **DHCP Server Configuration** dialog box.

Creating a new DHCP pool

The DHCP Server -New Pool tab provides configuration options for creating a new DHCP pool.

Figure 24: DHCP Server Configuration - New Pool tab



The following table provides a list of fields in the DHCP Server Configuration - New Pool tab and their descriptions:

Table 32: DHCP Server Configuration - New Pool tab fields

Field	Description
Name	Name of the new pool to be created.

To cancel changes, click **Cancel**. To apply changes and create the new pool, click **Apply**. The newly created pool appears in the **All DHCP Pools** tree.

Configuring DHCP pool parameters

The DHCP Server - Pool Config tab provides options for configuring parameters for the DHCP pool.

To open the DHCP Server Configuration - Pool Config tab:

Click a specific pool in the **All DHCP Pools** tree.

Figure 25: DHCP Server Configuration - Pool Config tab

DHCP Server Configuration

All DHCP Pools

- 1 - DHCP pool #1
 - 5 - main pool

Pool Config | General DHCP Option Config

Name	main pool
Mode	Disable
Start IP Address	1.2.3.20
End IP Address	1.2.3.100
Lease (Seconds)	691200
Client Identifier	
Bootfile	
Next Server	0.0.0.0
Server Name	

Refresh Apply

The following table provides a list of fields in the DHCP Server Configuration - Pool Configuration tab and their descriptions:

Table 33: DHCP Server Configuration - Pool Config tab fields

Field	Description
Name	Name of the selected pool.
Mode	Administrative status of the DHCP pool. Possible options are: <ul style="list-style-type: none"> • Enable • Disable
Start IP Address	First IP address assigned in the DHCP pool.
End IP Address	Last IP address assigned in the DHCP pool.
Lease (Seconds)	Amount of time a client holds an allocation from DHCP before making a new request.
Client Identifier	String identifying client station as eligible to receive allocation from the DHCP pool.
Bootfile	Bootfile assigned by DHCP.
Next Server	The next server to service DHCP allocations if this server is not available.
Server Name	The network name of the DHCP server. This field is optional. Default: None

To refresh the field information, click **Refresh**. To apply changes to the pool, click **Apply**.

Configuring DHCP assignment parameters

The DHCP Server - General DHCP Options Config tab provides options for configuring parameters for a remote station requesting network parameter information from the DHCP service.

To open the DHCP Server Configuration - General DHCP Options Config tab:

Click a specific pool entry in the All DHCP Pools tree.

Figure 26: DHCP Server Configuration - General DHCP Options Config tab

The screenshot shows a window titled "• DHCP Server Configuration •". Inside, there's a section "All DHCP Pools" with a sub-label "1 - DHCP pool #1". Below this is a tabbed interface with "Pool Config" and "General DHCP Option Config". The "General DHCP Option Config" tab is active, displaying a table with four columns: Code, Name, Type, and Value. The table contains four rows of configuration options. At the bottom of the window are four buttons: "Add Option", "Refresh", "Apply", and "Delete Option".

Code	Name	Type	Value
1	Subnet Mask	IP Address	255.255.255.0
3	Default Router	IP Address	2.2.2.1
15	DNS Name	Ascii	avaya.com
6	DNS Server	IP Address	3.3.3.1

The following table provides a list of fields in the DHCP Server Configuration - General DHCP Options Config tab and their descriptions:

Table 34: DHCP Server Configuration - General DHCP Options Config tab fields

Field	Description
Code	The system definition of the DHCP option. Possible values are: <ul style="list-style-type: none"> ● Subnet Mask - The subnet mask to be assigned to the requesting device. ● Default Router - The IP address of the router to be used as the default gateway for the requesting device. ● DNS Server - The IP address of the DNS to be used for address resolution for the requesting device. ● DNS Name - The name of the DNS to be used for address resolution for the requesting device.
Name	The name of the DHCP option. Possible values are: <ul style="list-style-type: none"> ● Subnet Mask - The value requested as Subnet Mask by the requesting device for which the associated Code value is to be returned. ● Default Router - The value requested as Default Router by the requesting device for which the associated Code value is to be returned. ● DNS Server - The value requested as DNS Server by the requesting device for which the associated Code value is to be returned. ● DNS Name - The value requested as DNS Name by the requesting device for which the associated Code Value is returned.
Type	The format of the DHCP option. Possible values are: <ul style="list-style-type: none"> ● Ascii - The value is assigned in ASCII character format. ● Hex - The value is assigned in hexadecimal format. ● Integer - The value is assigned in integer format. ● IP Address - The value is assigned in IP address format. ● Word - The value is assigned in text format.
Value	The value of the DHCP option, presented according to the Type field. <p>Note:</p> <p>If the Type field is set to IP Address, this field is disabled.</p>

To add a new DHCP configuration option, click **Add Option**. To refresh the table view, click **Refresh**. To apply changes to the table, click **Apply**. To delete a DHCP configuration option, click **Delete**.

For more information on user interface, see [“Using dialog boxes and tables” on page 32](#).

Configuring the TFTP server

The TFTP (Trivial File Transfer Protocol) service allows transfer of files across your network, using a connectionless, UDP-based protocol. TFTP is the protocol normally used for transferring stored device configuration files to and from remote devices, and for transferring device firmware updates.

To configure the TFTP server:

Select **Servers > TFTP Server** from the **Configure** menu.

Figure 27: TFTP Server Configuration dialog box

The screenshot shows a yellow dialog box titled "TFTP Server Configuration". It contains a dropdown menu for "Mode" set to "Enable". Below this, it displays memory usage statistics for NVRAM and RAM, showing both "Total Bytes Used" and "Total Bytes Capacity" for each. At the bottom, there are "Refresh" and "Apply" buttons.

The following table provides a list of fields in the **TFTP Server Configuration** dialog box and their descriptions:

Table 35: TFTP Server Configuration fields

Field	Description
Mode	Administrative status of the TFTP service. Possible values are: <ul style="list-style-type: none"> • Enable • Disable
NVRAM Total Bytes Used	Total bytes used for scripts in NVRAM.
NVRAM Total Bytes Capacity	The total byte capacity for scripts in NVRAM.
RAM Total Bytes Used	Total bytes used for scripts and images in RAM.

Table 35: TFTP Server Configuration fields

Field	Description
RAM Total Bytes Capacity	The total byte capacity for scrips and images in RAM.

For more information on user interface, see [“Using dialog boxes and tables” on page 32](#).

Configuring the Converged Network Analyzer application

The Converged Network Analyzer (CNA) is a distributed system for real-time monitoring of IP networks, using active measurements. The CNA runs connectivity tests with pings, topology tests with traceroute, and QoS tests with synthetic RTP streams. Test plugs are entities within the CNA system that receive instructions from a Scheduler for running the tests, performing the tests, and for sending back the results.

The following options are available for configuring the Converged Network Analyzer on the Avaya G430 Device:

- [Configuring an External Test Plug](#) - Configuration information for an external test plug.
- [Configuring Schedulers](#) - Scheduling information for the test plugs.

To access and configure the Converged Network Analyzer application:

Select **Configure > CNA**.

Configuring an External Test Plug

The CNA Configuration - Test Plug tab provides configuration options for an external test plug. A test plug is a piece of external hardware that connects to a device's network port and simulates network traffic without actually exposing the device to the network traffic.

Figure 28: CNA Configuration - Test Plug tab

The screenshot shows a configuration window titled "CNA Configuration". It has two tabs: "Test Plug" and "Schedulers". The "Test Plug" tab is selected. Inside this tab, there are three configuration items: "Global Administrative State" set to "Disable", "TestPlug 1 Administrative State" set to "Enable", and "TestPlug 1 Status" showing "Unregistered". At the bottom of the window are "Refresh" and "Apply" buttons.

The following table provides a list of fields in the CNA Configuration - Test Plug tab and their descriptions:

Table 36: CNA Configuration - Test Plug parameters

Field	Description
Global Administrative State	Administrative status of the CNA application. Possible values are: <ul style="list-style-type: none"> • Enable • Disable
Test Plug 1 Administrative State	Administrative status of the test plug. Possible values are: <ul style="list-style-type: none"> • Enable • Disable
1 of 2	

Table 36: CNA Configuration - Test Plug parameters (continued)

Field	Description
Test Plug 1 Status	<p>The status of the Test Plug operation. Possible values include:</p> <ul style="list-style-type: none"> ● Unregistered - The test plug is attempting to register and is currently unregistered. ● Scheduler List Exhausted - The test plug has exhausted its scheduler list at least once, and is now attempting to register. ● Idle - The test plug is registered, but idle. ● Test - The test plug is running a test. ● Suspend - The test plug is idle because a test was cancelled. ● No IP Address - No IP address is configured for the test plug interface. ● Bad IP Address - The configured test plug IP address is not properly configured for the test plug interface. ● Empty Scheduler List - The scheduler list is empty. No testing events are configured for this device. ● Failed Control Port Bind - The test plug failed to bind to the UDP control port. ● Failed FTP Port Bind - The test plug failed to bind to the UDP port for RTP tests. ● Suspend By Rate Limiter - The test plug is suspended by its test rate limiter.
2 of 2	

Configuring Schedulers

The CNA Configuration - Schedulers tab provides configuration options for scheduling test plugs.

Figure 29: CNA Configuration - Schedulers tab

Index	Address	Port	Mode
1	0.0.0.0	50002	Not In Service
2	0.0.0.0	50002	Not In Service
3	0.0.0.0	50002	Not In Service
4	0.0.0.0	50002	Not In Service
5	0.0.0.0	50002	Not In Service

The following table provides a list of fields in the CNA Configuration - Schedulers tab and their descriptions:

Table 37: CNA Configuration - Schedulers Tab fields

Field	Description
Index	The index of this scheduler in the scheduler list.
Address	Address of the scheduler.
Port	Scheduler registration TCP port. The default value is: 8888 .
Mode	Indicates whether the scheduler is active or inactive. Possible values include: <ul style="list-style-type: none"> ● Active ● Not In Service

Note:

Mode cannot be set to **Active** for a scheduler if the **Address** is set to **0.0.0.0**.

Chapter 8: WAN Configuration

This chapter provides information about configuring Avaya WAN Modules and includes the following sections:

- [WAN overview](#) - An overview of WAN functionality in the Avaya G430 Device.
- [Ethernet LAN Port Configuration](#) - Information about viewing and configuring built-in Ethernet LAN ports on the Avaya G430 Device.
- [Ethernet WAN Port Configuration](#) - Information about viewing and configuring built-in Ethernet WAN ports on the Avaya G430 Device.
- [Configuring the ETR port](#) - Information about viewing and configuring the ETR port.
- [The Services Interface](#) - Information about the Services port.
- [Configuring Backup Interfaces](#) - Information about viewing and configuring Backup Interfaces.

WAN overview

WAN Modules add WAN connectivity to the Avaya G430 Device. WAN connectivity provides a link to the WAN, enabling heavy data transfer over long distances. WAN connection can connect branch offices to headquarters. In addition, WAN connectivity is essential for providing access to the Internet.

Ethernet LAN Port Configuration

This section provides information on viewing and configuring parameters for the built-in Ethernet LAN port of the Avaya G430 Device. The Ethernet LAN port can be used to connect to the campus switched backbone network or to an end-user device.

To display the Ethernet LAN Port Configuration dialog box:

Click the Ethernet LAN port's symbol in the Chassis view or the Tree view. The system displays the Ethernet LAN Port Configuration dialog box, displaying two tabs:

- [Ethernet LAN Port Configuration - General tab](#)
- [Ethernet LAN Port Configuration - Advanced tab](#)

Ethernet LAN Port Configuration - General tab

The General tab of the Ethernet LAN Port Configuration dialog box enables you to set general functional parameters for the built-in Ethernet LAN port(s) on the Avaya G430 device. These parameters define how the port interfaces with the network in terms of VLAN assignment, speed, duplex and flow control.

Figure 30: Ethernet LAN Port Configuration dialog box - General tab

• Module-10, Port: 3, Ethernet LAN 1 •

General **Advanced**

Port Name	NO NAME
Port Type	Avaya G430 10or100TPort
Port Functionality	10/100Base-T
Administrative Status	Enable
Tagging Mode	Clear
VLAN ID	1
Port Priority Level	User Priority 0
Auto Negotiation Mode	Enable
Auto Negotiation Status	Pass
Duplex Mode	Full Duplex
Speed Mode	Fast Ethernet
Flow Control Mode	No Flow Control
Operational Status	OK
No Fault Messages	

Refresh Apply

The following table lists the fields in the Ethernet LAN Port Configuration - General tab and their descriptions:

Table 38: Ethernet LAN Port Configuration - General tab

Field	Description
Port Name	The user can define a logical name to the port for ease of use.
Port Type	The port type; optionally includes reference to the module to which it is attached and the port connector type.
Port Functionality	The physical media type of the selected port. If the port conforms to a certain standard (Repeater, Transceiver, 10BaseT, etc.), the standard is displayed. If the port does not conform to any standard, Private is displayed.
Administrative Status	The administrative state of the selected port: <ul style="list-style-type: none"> ● Enable - The port is enabled and can transmit and receive packets. ● Disable - The port is disabled and cannot transmit or receive packets.
Tagging Mode	The port's operational mode regarding VLANs. The possible modes are: <ul style="list-style-type: none"> ● Clear - Transmits each outgoing packet in untagged format, if the packet belongs to the port's VLAN. Otherwise, it discards the packet. ● IEEE-802.1Q - VLAN tagging, per IEEE 802.1Q VLAN standard. The port transmits frames with VLAN IDs between 1 - 4090 for the Avaya G430 Device.
VLAN ID	The VLAN number of the port.
Port Priority Level	The priority level of packets exiting the port or ports on the module. For effective transmission, multimedia packets must be received at regular intervals. To ensure this, you can assign priorities to packets coming out of a port. Whenever the traffic load is extreme and a port cannot accept all incoming packets, packets sent from a port with the highest priority passes through first. However, a fairness mechanism allows low priority packets to eventually enter the bus. Possible values are: User Priority 0, User Priority 7.
1 of 2	

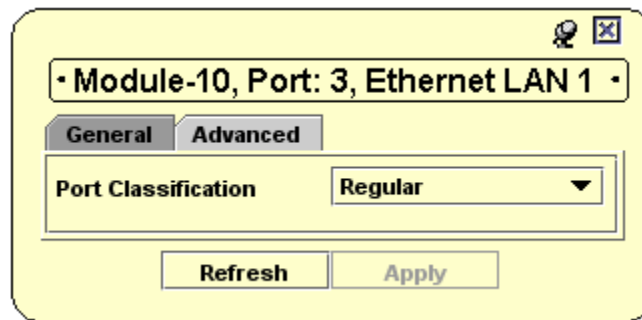
Table 38: Ethernet LAN Port Configuration - General tab (continued)

Field	Description
Auto Negotiation Mode	<p>The configured state of the Auto-Negotiation protocol between two stations. When enabled, Auto-Negotiation detects the highest common denominator for communication between endstations, and sets both to the same highest common setting. It also delivers remote link status.</p> <p>For 10BaseT and 100BaseT ports, Auto-Negotiation determines the speed and Duplex Mode of communication between the endstations. For Gigabit ports, Auto-Negotiation determines the Flow Control setting of the ports.</p> <p>For more information, see <i>Auto-Negotiation</i> in <i>The Reference Guide</i>.</p>
Auto Negotiation Status	<p>The operational state of the Auto-Negotiation protocol between two stations. Possible statuses are:</p> <ul style="list-style-type: none"> ● Pass - The Auto-Negotiation protocol is enabled and a common protocol is established. ● In Progress - The Auto-Negotiation protocol is in the process of detecting the communication capabilities of the endstations and setting them to the highest common denominator. ● Fail - The Auto-Negotiation protocol is not able to detect the communication capabilities of the end station, or is unable to set them to the highest common denominator. ● Disabled - The Auto-Negotiation protocol is disabled.
Duplex Mode	<p>The state of communication of the selected port. Possible values are:</p> <ul style="list-style-type: none"> ● Full Duplex - The port can send and receive simultaneously. ● Half Duplex - The port can either receive or send, but cannot do both simultaneously.
Speed Mode	<p>The rate of communication of the selected port. Possible values are:</p> <ul style="list-style-type: none"> ● Ethernet ● Fast Ethernet ● Gigabit Ethernet
Flow Control Mode	The state of flow control on the selected port.
Operational Status	<p>The warning level of the selected port. Possible values are:</p> <ul style="list-style-type: none"> ● OK ● Warning ● Fatal
Fault Messages	A list of fault messages.
2 of 2	

Ethernet LAN Port Configuration - Advanced tab

The Advanced tab of the Ethernet LAN configuration dialog box enables you to define port classification for the built-in Ethernet LAN port(s) on the Avaya G430 Device. Port classification identifies whether the port is connected to normal or higher-priority users and devices.

Figure 31: Ethernet LAN Port Configuration dialog box - Advanced tab



The following table lists the fields in the Ethernet LAN Port Configuration - Advanced tab, and their descriptions:

Table 39: Ethernet LAN Port Configuration - Advanced tab

Field	Description
Port Classification	<p>The classification of a specific port. Port Classification allows network managers to specify each port level's importance. The possible states are:</p> <ul style="list-style-type: none"> • Regular - Normal users. • Valuable - Servers or critical users. <p>For more information, see <i>Port Classification</i> in <i>The Reference Guide</i>.</p>

Ethernet WAN Port Configuration

This section provides information on viewing and configuring parameters for the built-in Ethernet WAN port of the Avaya G430 Device. Ethernet WAN ports are generally used to connect to an enterprise WAN or receive an Ethernet handoff from an Internet Service Provider.

To display the Ethernet WAN Port Configuration dialog box:

Click the Ethernet WAN port's symbol in the Chassis view or the Tree view.

The Ethernet WAN Port Configuration dialog box displays the following tabs:

- [Ethernet WAN Port Configuration - General tab](#)
- [Ethernet WAN Port Configuration - PPPoE Client tab](#)

WAN Configuration

- [Ethernet WAN Port Configuration - DHCP Client tab](#)
- [Ethernet WAN Port Configuration - Extended Keep Alive Tab](#)

The visibility of the tabs depend on the value of the Encapsulation parameter (this parameter can be viewed in the WAN Port Configuration tab and can only be changed through the CLI). The following table describes the WAN Port Configuration tab options:

Table 40: WAN Port Configuration tab options

Encapsulation Value	Visible Tabs
ARPA	General, PPPoE, DHCP Client, Extended Keep Alive
PPoE	General, PPPoE

Ethernet WAN Port Configuration - General tab

The General tab of the Ethernet WAN Configuration dialog box enables you to set general functional parameters for the built-in Ethernet WAN port. These parameters define how the port interfaces with the network in terms of speed, duplex, and Voice over IP (VoIP) queuing.

Figure 32: Ethernet WAN Port Configuration dialog box - General tab

Module-10, Port: 2, Ethernet WAN 1

DHCP Client

Keep Alive ICMP

General

PPPoE Client

Description

Port Type

10/100 BaseTX

Port Functionality

Fast Ethernet - 100mb

Administrative Status

Enable

MAC Address

00:07:3B:E4:67:F4

Operational Status

Down

Auto Negotiation Mode

Enable

Duplex Mode

Half Duplex

Speed Mode

Ethernet

Encapsulation

ARPA

Traffic Shaper Rate (bps)

Disable

VoIP Queue

N/A

Refresh

Apply

The following table lists the fields in the Ethernet WAN Port Configuration - General tab and their descriptions:

Table 41: Ethernet WAN Port Configuration - General tab

Field	Description
Description	The user can define a logical name to the port for ease of use.
Port Type	The port type; optionally includes reference to the module to which it is attached and to the port connector type.
Port Functionality	The physical media type of the selected port. If the port conforms to a certain standard (Repeater, Transceiver, 10BaseT, etc.), this standard is displayed. If the port does not conform to any standard, Private is displayed.
Administrative Status	The administrative state of the selected port: <ul style="list-style-type: none"> ● Enable - The port is enabled and can transmit and receive packets. ● Disable - The port is disabled and cannot transmit or receive packets.
MAC Address	The MAC address of the WAN port.
Operational Status	The operational status of the WAN port. Possible values are: <ul style="list-style-type: none"> ● OK ● Down ● Fatal
Auto Negotiation Mode	The configured state of the Auto-Negotiation protocol between two stations. When enabled, Auto-Negotiation detects the highest common denominator for communication between endstations, and sets both to the same highest common setting. It also delivers remote link status. For 10BaseT and 100BaseT ports, Auto-Negotiation determines the speed and Duplex Mode of communication between the endstations. For Gigabit ports, Auto-Negotiation determines the Flow Control setting of the ports. Possible values are: <ul style="list-style-type: none"> ● Enable - Auto-Negotiation is enabled for this interface. ● Disable - Auto-Negotiation is disabled for this interface. For more information, see <i>Auto-Negotiation</i> in <i>The Reference Guide</i> .
Duplex Mode	The state of communication of the selected port. Possible values are: <ul style="list-style-type: none"> ● Full Duplex - The port can send and receive simultaneously. ● Half Duplex - The port can either receive or send, but cannot do both simultaneously.
1 of 2	

Table 41: Ethernet WAN Port Configuration - General tab (continued)

Field	Description
Speed Mode	The rate of communication of the selected port. Possible values are: <ul style="list-style-type: none"> ● Ethernet ● Fast Ethernet ● Gigabit Ethernet
Encapsulation	The WAN encapsulation method of the selected port. Possible values are: <ul style="list-style-type: none"> ● ARPA - The port uses the ARPA protocol to establish a connection. ● PPPoE - The port uses PPP over Ethernet to establish a connection. <p>Note: This field is read-only.</p>
Traffic Shaper Rate (bps)	Reserved bandwidth for VoIP traffic. Possible values are: <ul style="list-style-type: none"> ● Integer values between 64000 - 2048000 ● Disable
VoIP Queue	The state of VoIP queuing. VoIP queuing changes the length of the high priority queue, providing support for the configuration during a maximum VoIP delay. Possible states include: <ul style="list-style-type: none"> ● On - Standard VoIP queuing is active. ● Off - VoIP queuing is not active. ● Fair-VoIP Queue - VoIP fair queuing is active. <p>Note: This option is not available when Traffic Shaper Rate is set to Disable.</p>
2 of 2	

Ethernet WAN Port Configuration - PPPoE Client tab

The PPPoE Client tab enables you to view the configuration and status information of the PPPoE client available for the embedded Ethernet WAN port. PPPoE allows you to set up PPP WAN connections over long-haul Ethernet media.

Figure 33: Ethernet WAN Port Configuration dialog box - PPPoE Client tab

The screenshot shows a configuration window for 'Module-10, Port: 2, Ethernet WAN 1'. It features a 'PPPoE Client' tab with various settings. The 'Encapsulation' is set to 'PPPoE', and the 'Traffic Shaper Rate (bps)' is set to 'Disable'. The 'VoIP Queue' is set to 'N/A'. The 'Operational Status' is 'Down'. The 'MAC Address' is '00:07:3B:E4:67:F4'. The 'Administrative Status' is 'Enable'. The 'Auto Negotiation Mode' is 'Enable'. The 'Duplex Mode' is 'Half Duplex'. The 'Speed Mode' is 'Ethernet'. The 'Port Functionality' is 'Fast Ethernet - 100mb'. The 'Port Type' is '10/100 BaseTX'. The 'Description' is 'who am i?'. The 'Refresh' and 'Apply' buttons are at the bottom.

The following table lists the fields in the Ethernet WAN Port Configuration - PPPoE Client tab and their descriptions:

Table 42: Ethernet WAN Port Configuration - PPPoE Client tab

Field	Description
Encapsulation	The encapsulation method used for the PPPoE connection. Possible values are: <ul style="list-style-type: none">• PPP• N/A
1 of 2	

Table 42: Ethernet WAN Port Configuration - PPPoE Client tab (continued)

Field	Description
Status	<p>The operational status of the PPPoE connection. Possible values are:</p> <ul style="list-style-type: none"> ● Up - The interface is up and can transmit and receive packets. ● Down - The interface is down due to a fault and cannot transmit or receive packets. ● Testing - The interface is in the testing mode and cannot transmit or receive regular data. ● Partially Down - The interface is up. However, some interfaces layered on top of this interface are down. Some packets can be transmitted and received. ● Admin Down - The interface has been shut down in the device configuration and cannot transmit or receive packets. ● Dormant Down - The interface is down due to no packets being sent or received for a long period of time. For more information, see the <i>Administration for the Avaya G430 Media Gateway</i>. ● KeepAlive Down - The interface is down due to not having received a Keep Alive packet in the configured interval. For more information, see <i>Avaya G430 Media Gateway Documentation</i>. ● N/A
Negotiated IP	Enable/Disable PPP-IPCP IP address negotiation. When enabled, the WAN fast Ethernet interface receives an IP address from the remote peer.
IP Address	The IP address received from the remote peer during the IP negotiation phase.
Request DNS Servers	<p>Requestion of DNS server information from the remote peer. Possible values are:</p> <ul style="list-style-type: none"> ● Enable - Request DNS server information from the remote peer. ● Disable - Do not request DNS server information from the remote peer.
2 of 2	

Note:

If the **Encapsulation** field of the Ethernet WAN Port Configuration - General tab is set to **ARPA**, the PPPoE client is not supported, and **N/A** is seen in all the fields of the Ethernet WAN Port Configuration - PPPoE Client tab.

Note:

All fields in the Ethernet WAN Port Configuration - PPPoE Client tab are read-only except for **Negotiated IP** and **Request DNS Servers**.

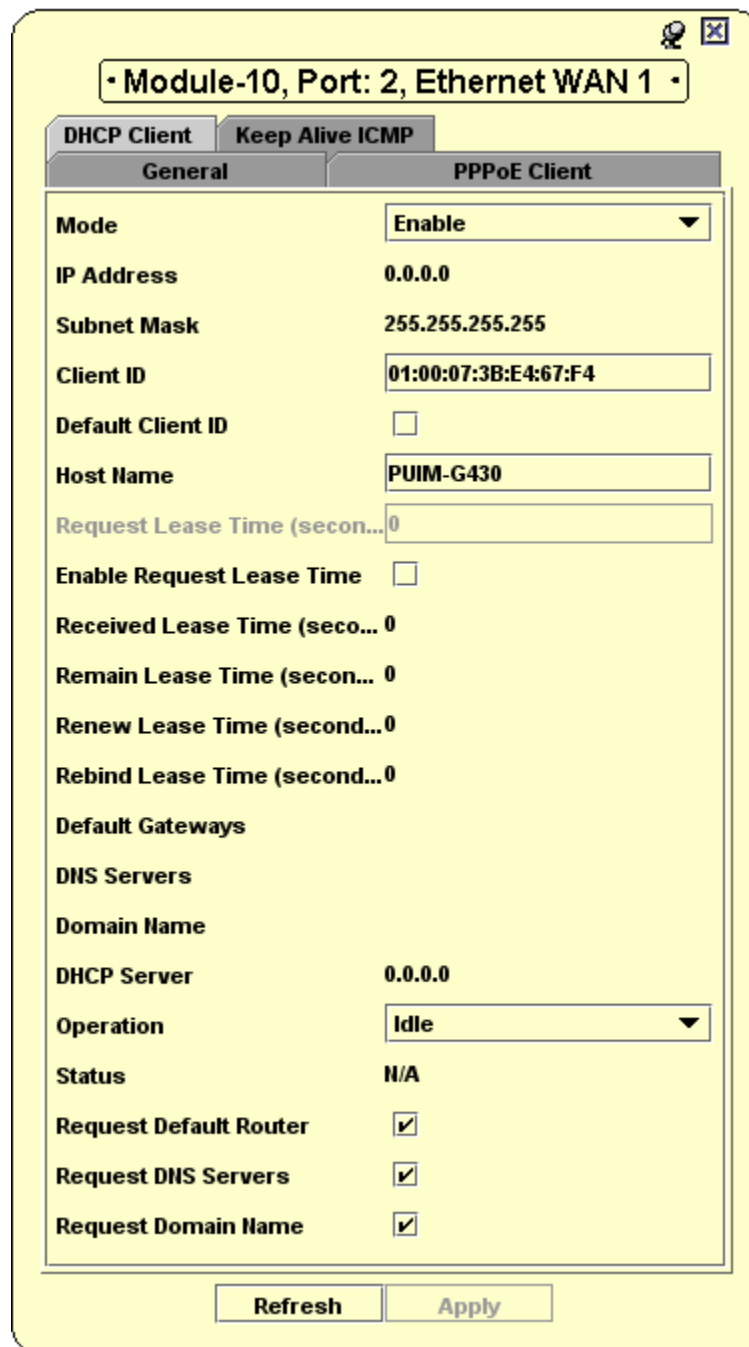
Ethernet WAN Port Configuration - DHCP Client tab

The DHCP Client tab enables you to view configuration and status information for the DHCP client, available for the embedded Ethernet WAN port.

Note:

The DHCP Client tab appears only if **Encapsulation** is set to **ARPA** in the Ethernet WAN Port Configuration - General tab.

Figure 34: Ethernet WAN Port Configuration dialog box - DHCP Client tab



The dialog box is titled "Module-10, Port: 2, Ethernet WAN 1". It features three tabs: "DHCP Client" (selected), "Keep Alive ICMP", and "PPPoE Client". The "General" sub-tab is active. The configuration includes fields for Mode (Enable), IP Address (0.0.0.0), Subnet Mask (255.255.255.255), Client ID (01:00:07:3B:E4:67:F4), Default Client ID (checkbox), Host Name (PUIM-G430), Request Lease Time (0), Enable Request Lease Time (checkbox), Received Lease Time (0), Remain Lease Time (0), Renew Lease Time (0), Rebind Lease Time (0), Default Gateways, DNS Servers, Domain Name, DHCP Server (0.0.0.0), Operation (Idle), Status (N/A), and checkboxes for Request Default Router, Request DNS Servers, and Request Domain Name. At the bottom are "Refresh" and "Apply" buttons.

Module-10, Port: 2, Ethernet WAN 1	
DHCP Client Keep Alive ICMP PPPoE Client	
General	
Mode	Enable
IP Address	0.0.0.0
Subnet Mask	255.255.255.255
Client ID	01:00:07:3B:E4:67:F4
Default Client ID	<input type="checkbox"/>
Host Name	PUIM-G430
Request Lease Time (secon...	0
Enable Request Lease Time	<input type="checkbox"/>
Received Lease Time (seco...	0
Remain Lease Time (secon...	0
Renew Lease Time (second...	0
Rebind Lease Time (second...	0
Default Gateways	
DNS Servers	
Domain Name	
DHCP Server	0.0.0.0
Operation	Idle
Status	N/A
Request Default Router	<input checked="" type="checkbox"/>
Request DNS Servers	<input checked="" type="checkbox"/>
Request Domain Name	<input checked="" type="checkbox"/>
Refresh Apply	

The following table lists the fields in the Ethernet WAN Port Configuration - DHCP Client tab and their descriptions:

Table 43: Ethernet WAN Port Configuration - DHCP Client tab

Field	Description
Mode	The row status for creating a new DHCP client on the VLAN or WAN fast ethernet connection. Possible values include: <ul style="list-style-type: none"> • Enable • Disable
IP Address	The IP Address allocated for the DHCP client.
Subnet Mask	The subnet mask allocated for the DHCP client. The value of the mask is an IP address with all of its network bits set to 1 and all of its host bits set to 0 .
Client ID	The client identifier used by the DHCP client. This identifier can be up to 255 bytes.
Default Client ID	The default identifier used for manual leased DHCP clients. When selected, the client uses the default client identifier. The default client identifier is: 01:Interface MAC Address .
Host Name	The host name used by the DHCP client. The default value is Default Host Name .
Request Lease Time (seconds)	The finite lease time, in seconds, requested by the DHCP client. The default value is 0 .
Enable Request Lease Time	The status of the Request Lease Time field on the device. When selected, the client requests a finite amount of lease time.
Received Lease Time (seconds)	The lease time, in seconds, received by the DHCP client.
Remain Lease Time (seconds)	The lease time, in seconds, that remains for the DHCP client.
Renew Lease Time (seconds)	The time defined on the DHCP client for renewing a phase in seconds.
Rebind Lease Time (seconds)	The time, in seconds, defined on the DHCP client for rebinding a phase.
Default Gateways	The default gateways defined for the DHCP client. Up to 8 IP addresses can be defined as default gateways.
DNS Servers	The DNS servers defined for the DHCP clients. Up to 8 IP addresses can be defined as DNS servers.
1 of 2	

Table 43: Ethernet WAN Port Configuration - DHCP Client tab (continued)

Field	Description
Domain Name	The domain name designated for the DHCP client. This name can be up to 255 bytes.
DHCP Server	The DHCP server that allocates a specific IP address to the DHCP client.
Operation	Instructs the client to perform Release or Renew operations.
Status	Indicates the status of the DHCP client. Possible statuses include: <ul style="list-style-type: none"> • Select • Request • Bound • Rebind • Renew • Release • Decline • Not Supported
Request Default Router	Instructs the client to request a connection with the default router.
Request DNS Servers	Instructs the client to request a connection with a predefined DNS server.
Request Domain Name	Instructs the client to request a connection using a predefined domain name.
2 of 2	

Note:

If the **Encapsulation** field of the Ethernet WAN Port Configuration - General tab is set to **ARPA**, the PPPoE client is not supported and returns a result of **N/A** in all the fields of the Ethernet WAN Port Configuration - PPPoE Client tab.

Note:

All the fields in the Ethernet WAN Port Configuration - PPPoE Client tab are read-only.

Ethernet WAN Port Configuration - Extended Keep Alive Tab

The Extended Keep Alive tab of the Ethernet WAN Port Configuration dialog box enables you to set parameters for the Extended Keep Alive feature of the Avaya G430 Device. Extended Keep Alive allows you to precisely tune the Keep Alive network traffic to gain an accurate representation of your network's connection status.

Figure 35: Ethernet WAN Port Configuration dialog box - Extended Keep Alive tab

Module-10, Port: 2, Ethernet WAN 1

General | PPPoE Client | DHCP Client | **Keep Alive ICMP**

Keep Alive ICMP Mode: disable

Keep Alive ICMP Method: icmpPing

Keep Alive ICMP IP Address: 0.0.0.0

Keep Alive ICMP Next Hop MAC: 00:00:00:00:00:00

Keep Alive ICMP Src IP Address: 0.0.0.0

Keep Alive ICMP Down Retries: 4

Keep Alive ICMP Up Retries: 1

Keep Alive ICMP Timeout (sec): 1

Keep Alive ICMP Interval (sec): 5

Keep Alive ICMP Status: disable

Refresh Apply

The following table lists the fields in the Ethernet WAN Port Configuration - Extended Keep Alive tab, and their descriptions:

Table 44: Ethernet WAN Port Configuration - Extended Keep Alive tab

Field	Description
Keep Alive ICMP Mode	The Keep Alive operation mode. Possible values are: <ul style="list-style-type: none">• Enable• Disable
1 of 2	

Table 44: Ethernet WAN Port Configuration - Extended Keep Alive tab (continued)

Field	Description
Keep Alive ICMP Method	The type of Keep Alive method used. Possible values are: <ul style="list-style-type: none"> ● icmpPing - ICMP Ping packets are exchanged by the devices at the endpoints of the connection to verify the connectivity. ● None
Keep Alive ICMP IP Address	The IP address to be selected for connection status.
Keep Alive ICMP Next Hop MAC	The MAC address to be selected for connection status.
Keep Alive ICMP Src IP Address	The source IP address of the Keep Alive. The value can be any IP address on the source interface. Default: The primary IP address for the interface.
Keep Alive ICMP Down Retries	The number of unsuccessful Keep Alive attempts used to determine the failure of the next hop router. Possible values: 1-32 .
Keep Alive ICMP Up Retries	The number of successful Keep Alive attempts used to determine the operational status of the next hop router. Possible values: 1-32 .
Keep Alive ICMP Timeout	The number of seconds the interface waits for a reply from the next hop router before considering the request a failure. Possible values: 1-10 . Default: 1
Keep Alive ICMP Interval	The Keep Alive interval in seconds. Possible values: 1-36 . Default: 5
Keep Alive ICMP Status	The Keep Alive status. Possible values are: <ul style="list-style-type: none"> ● Up ● Down ● Disable
2 of 2	

Configuring the ETR port

The Emergency Transfer Relay (ETR) port acts as a means of communication when there are severe network difficulties and other channels are down.

Note:

ETR configuration is enabled only when MM714B is active.

To view the ETR Interface table:

Select **Configure > WAN > ETR Interface**.

Figure 36: ETR Interface - G430

• MM714v2, Port-4, FXO Trunk •

Port Identifier 001V204

ETR Mode Auto

ETR State off

Refresh Apply

The G430 device manager allows the ETR configuration only on the Line-4 and Trunk-5 ports of MM714B. You can view only the ID for the rest of the ports.

The following table provides a list of fields in the ETR Interface form, supported for line 4 and trunk 5 ports, along with their descriptions:

Table 45: ETR Interface Form parameters

Field	Description
Port Identifier	The port identifier string.

Table 45: ETR Interface Form parameters (continued)

Field	Description
ETR State selection	The mode of operation. The status of Dynamic CAC on the WAN interface. Possible values are: <ul style="list-style-type: none"> • Auto • Manual On • Manual Off
ETR State	The current ETR state of operation.

The Services Interface

The Services port cannot be configured through the Avaya G430 Device Manager. The Services port allows an Out Of Band management interface in the Avaya G430 Device.

Configuring Backup Interfaces

The Backup Interface feature enables you to configure backup interfaces for WAN interfaces. The backup Interface feature includes a table for viewing all configured backup interfaces and a wizard for creating backup interfaces.

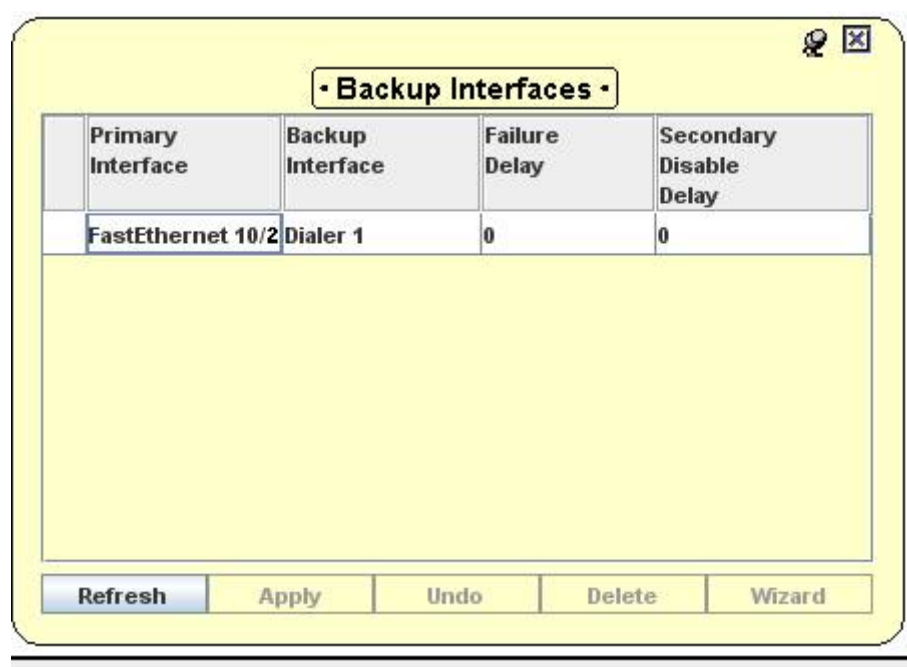
Viewing the Backup Interfaces table

The Backup Interfaces table provides a list of all the previously configured backup interfaces on the 10/2 and the dialer interface on the USB modem.

To view the Backup Interfaces table:

Select **Configure > WAN > Backup Interfaces**.

Figure 37: Backup Interfaces table




	Primary Interface	Backup Interface	Failure Delay	Secondary Disable Delay
	FastEthernet 10/2	Dialer 1	0	0

Refresh Apply Undo Delete Wizard

The Backup Interfaces table provides information about the backup interfaces configured on the device.

To configure a new Backup Interface, click **Wizard**. The system displays the Backup Interface wizard. For information on the Backup Interface wizard, see [“The Backup Interface wizard” on page 119](#).

To delete a Backup Interface:

1. Select the interface in the table.
2. Click **Delete**. The interface is marked as deleted in the Backup Interfaces table with the  icon in the far left column.
3. Click **Apply** to delete the Backup Interface.

The following table provides a list of fields in the Backup Interfaces table and their descriptions:

Table 46: Backup Interfaces Table parameters

Field	Description
Primary Interface	The name of the primary interface being backed up.
Backup Interface	The name of the Backup Interface.
Failure Delay	The amount of time, in seconds, between the trigger event and the activation of the Backup Interface.

Table 46: Backup Interfaces Table parameters (continued)

Field	Description
Secondary Disable Delay	The amount of time, in seconds, between the primary interface returning to an acceptable operational status and the deactivation of the Backup Interface.

The Backup Interface wizard

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

The Backup Interface wizard consists of the following screens:

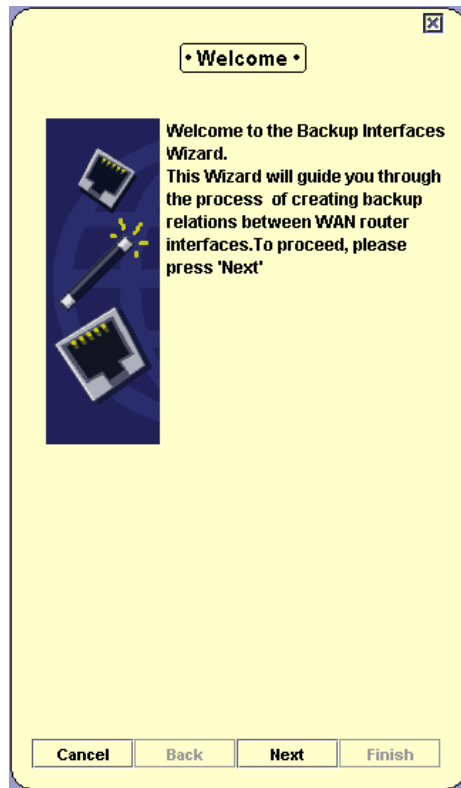
- [Welcome screen](#)
- [Primary Interface screen](#)
- [Backup Interface screen](#)
- [Backup Interface Parameters screen](#)
- [Confirmation screen](#)

The following sections describe each of the Backup Interface wizard screens.

Welcome screen

The Backup Interface wizard provides a simple, step-by-step method for creating and editing a Backup interface.

Figure 38: Backup Interface wizard - Welcome screen

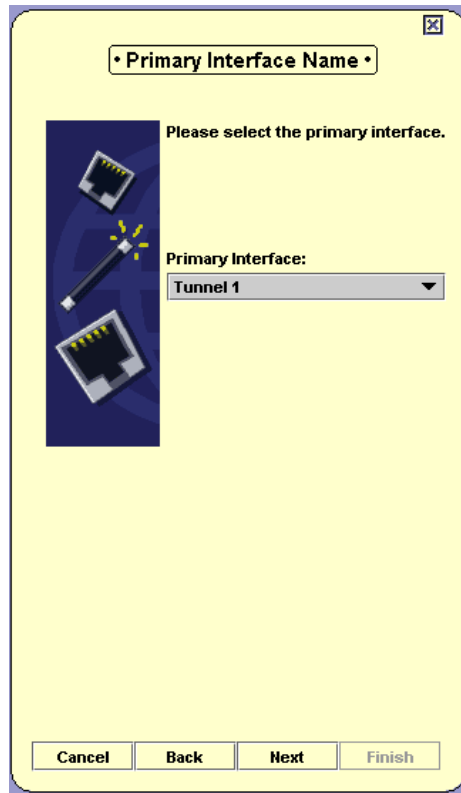


To continue, click **Next**. The Backup Interface wizard continues with the [“Primary Interface screen” on page 121](#).

Primary Interface screen

The Select Primary Interface screen enables you to select the interface to be backed up.

Figure 39: Backup Interface wizard - Select Primary Interface screen



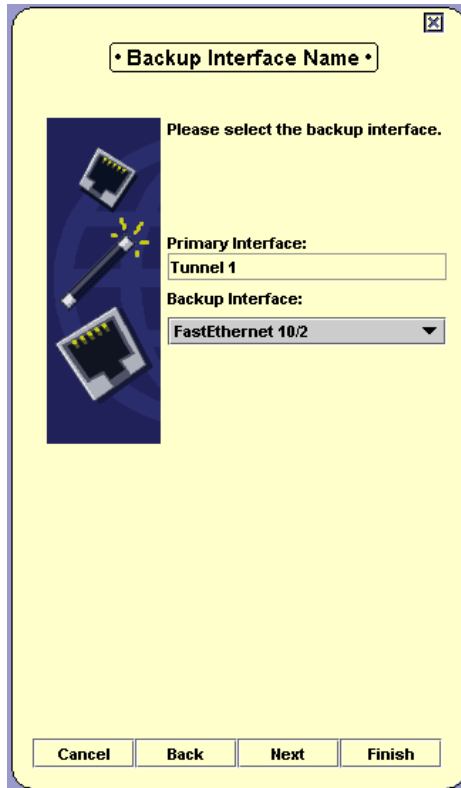
To select an interface to back up, select an interface name from the **Primary Interface** field.

To continue, click **Next**. The Backup Interface wizard continues with the ["Backup Interface screen" on page 122](#).

Backup Interface screen

The Select Backup Interface screen enables you to assign an interface to back up the primary interface.

Figure 40: Backup Interface wizard - Select Backup Interface screen



• Backup Interface Name •

Please select the backup interface.

Primary Interface:
Tunnel 1

Backup Interface:
FastEthernet 10/2

Cancel Back Next Finish

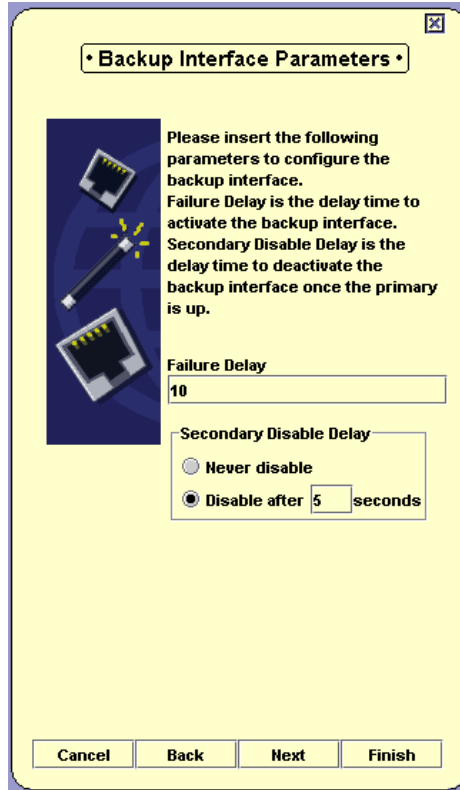
To select a Backup Interface, select an interface name from the **Backup Interface** field.

To continue, click **Next**. The Backup Interface wizard continues with the [“Backup Interface Parameters screen” on page 123](#).

Backup Interface Parameters screen

The Backup Interface Parameters screen enables you to configure the conditions under which the Backup interface is activated and deactivated.

Figure 41: Backup Interface wizard - Backup Interface parameters screen



• Backup Interface Parameters •

Please insert the following parameters to configure the backup interface.
Failure Delay is the delay time to activate the backup interface.
Secondary Disable Delay is the delay time to deactivate the backup interface once the primary is up.

Failure Delay
10

Secondary Disable Delay
☐ Never disable
☒ Disable after 5 seconds

Cancel Back Next Finish

To configure the number of seconds between the failure of the primary interface and the activation of the Backup Interface, enter a number in the **Enable Delay** field.

To configure the number of seconds between the restoration of the primary interface and the deactivation of the Backup Interface, enter a number in the **Disable Delay** field.

To continue, click **Next**. The Backup Interface wizard continues with the [“Confirmation screen” on page 124](#).

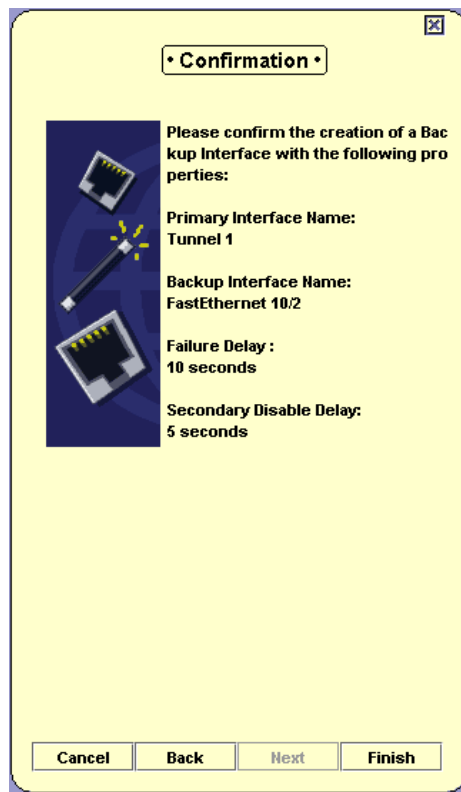
Confirmation screen

The Backup Interface wizard displays a summary of the information entered using the previous screens.

Note:

The Backup Interface is not yet created.

Figure 42: Backup Interface Wizard - Confirmation screen



To make changes to the summary information:

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

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

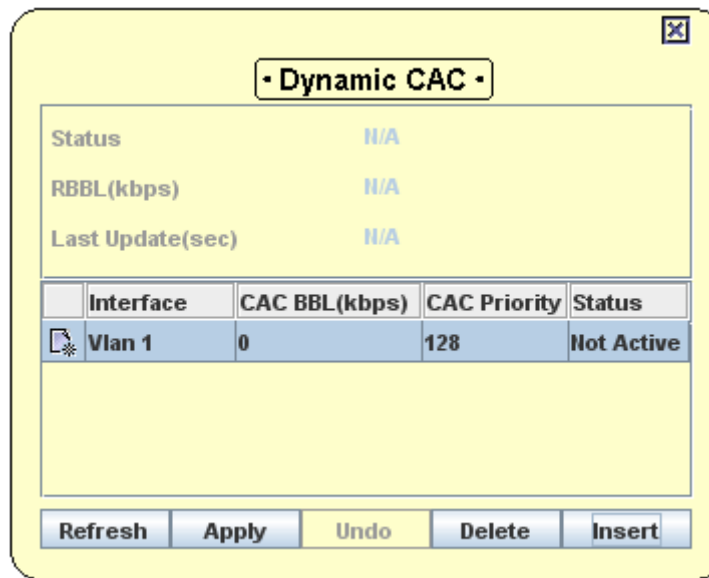
Dynamic CAC

The **Dynamic CAC** dialog box enables you to configure the Dynamic CAC function on a WAN interface. Dynamic CAC allows the Avaya G430 Device to control the traffic flow between itself and a remotely located call controller.

To configure the Dynamic CAC on a WAN interface:

1. Select **Configure > WAN > Dynamic CAC**.

Figure 43: Dynamic CAC dialog box



The screenshot shows the 'Dynamic CAC' dialog box. It has a title bar with a close button. Inside, there's a section with three labels: 'Status', 'RBBL(kbps)', and 'Last Update(sec)', each followed by 'N/A'. Below this is a table with four columns: 'Interface', 'CAC BBL(kbps)', 'CAC Priority', and 'Status'. The first row of the table is highlighted in blue and contains the values 'Vlan 1', '0', '128', and 'Not Active'. At the bottom of the dialog box, there are five buttons: 'Refresh', 'Apply', 'Undo', 'Delete', and 'Insert'.

Interface	CAC BBL(kbps)	CAC Priority	Status
Vlan 1	0	128	Not Active

To add a new interface, click **Insert**. A blank row appears in the interface list.

To edit an existing interface, double-click the row in the interface list.

To delete an interface, select the interface you want to delete and click **Delete**.

The following table provides a list of fields in the Dynamic CAC dialog box and their descriptions.

Table 47: Dynamic CAC dialog box

Field	Description
Status	<p>The status of Dynamic CAC on the WAN interface. Possible values are:</p> <ul style="list-style-type: none"> ● Active - Dynamic CAC is active on the WAN interface. ● Not Configured - Dynamic CAC is not configured (but is supported) for the WAN interface. ● Not Armed - Dynamic CAC is not armed (but is supported and configured) for the WAN interface. ● Armed Not Configured - Dynamic CAC is armed (and supported, but not configured) for the WAN interface. ● Not Supported - Dynamic CAC is not supported for the WAN interface. <p>Note: This field is read-only.</p>
RBBL (kbps)	<p>Remote Bearer Bandwidth Limit. RBBL is the amount of bandwidth available for CAC on the remote controller.</p> <p>Note: This field is read-only.</p>
Last Update (seconds)	<p>The last time the CAC values were updated (in seconds).</p> <p>Note: This field is read-only.</p>
Interface	<p>The local WAN interface supporting the Dynamic CAC. Possible values are:</p> <ul style="list-style-type: none"> ● Fast Ethernet ● Serial ● Tunnel
CAC BBL (kbps)	<p>The local interface bandwidth threshold after which CAC is activated.</p>
CAC Priority	<p>The CAC activation priority.</p>
Status	<p>Operational status of the Dynamic CAC. Possible values are:</p> <ul style="list-style-type: none"> ● Not Configured ● Active ● Not Active ● Active ECMP ● Not Supported

Chapter 9: VLANs

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

- [VLAN Configuration overview](#) - An overview of VLANs and their components.
- [Configuring VLANs](#) - 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.

VLAN Configuration overview

This section contains an overview of VLANs and how to configure them. This section includes:

- [VLANs overview](#) - A brief description of VLANs and their functions.
- [Master VLAN list](#) - A brief description of the Master VLAN List and its functions.
- [VLAN tags](#) - A brief description of VLAN tags and their functions.

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, see *VLANs* in the *Network Protocols* section of *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 available only when running the Avaya Network Manager. It is not available when running an Embedded Web Manager. To manage the master VLAN list, use the Avaya VLAN Manager. For information on the Avaya VLAN Manager, see 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.

Configuring VLANs

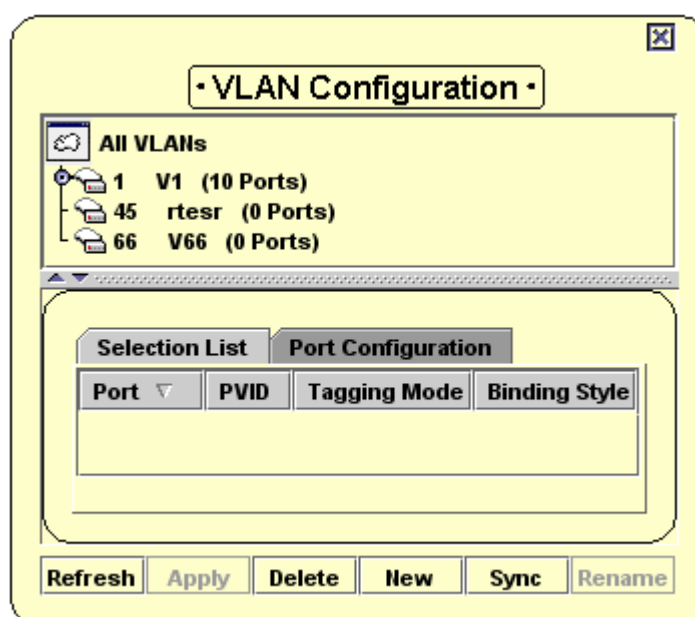
To view VLAN names, numbers, and component switch ports:

Click .

Or

Select **Configure > VLANs**. The system displays the **VLAN Configuration** dialog box.

Figure 44: 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 various 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.

VLANs

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.

The VLAN symbol includes a green tag if the VLAN is listed in the master VLAN list, and a device symbol if it exists locally on the device. If a VLAN is listed in the master VLAN list and exists locally on the device, the VLAN symbol includes a green tag and a device symbol.

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 appears 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, see [“Synchronizing VLAN names” on page 135](#).

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.

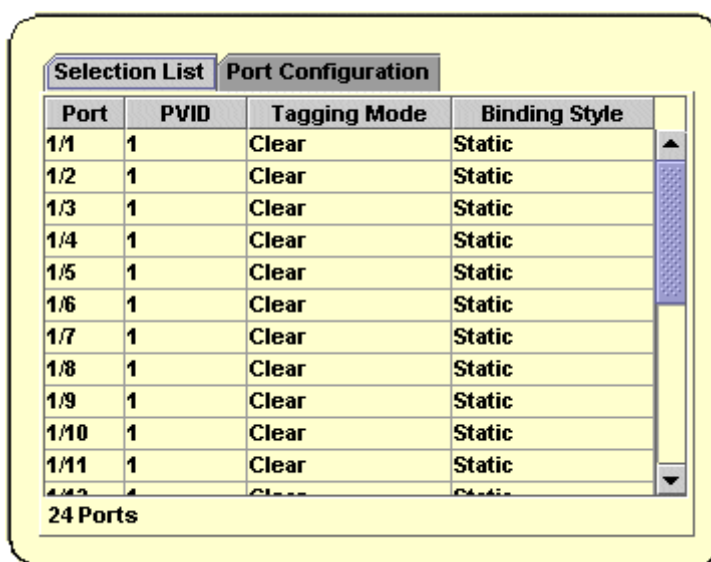
When a VLAN is selected in the VLAN Tree, member ports appear in the Chassis view with a yellow triangle and blue triangle on the port symbol, and statically bound ports appear in the Chassis view with a blue triangle on the port symbol. In addition, information about the member ports and statically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

For more information about the Selection List, see [“Selection List” on page 131](#).

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. If the Port Configuration Area is open, click **Selection List**. The system displays the Selection List.

Figure 45: Selection List



The screenshot shows a window titled 'Selection List' with a tab labeled 'Port Configuration'. Inside the window is a table with four columns: 'Port', 'PVID', 'Tagging Mode', and 'Binding Style'. The table lists 11 ports (1/1 to 1/11) with PVID 1, Tagging Mode 'Clear', and Binding Style 'Static'. A scrollbar on the right indicates more rows are present. Below the table, it says '24 Ports'.

Port	PVID	Tagging Mode	Binding Style
1/1	1	Clear	Static
1/2	1	Clear	Static
1/3	1	Clear	Static
1/4	1	Clear	Static
1/5	1	Clear	Static
1/6	1	Clear	Static
1/7	1	Clear	Static
1/8	1	Clear	Static
1/9	1	Clear	Static
1/10	1	Clear	Static
1/11	1	Clear	Static

24 Ports

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

Table 48: Selection List fields

Field	Description
Port	The Module and Port number.
PVID	The Port VLAN ID (PVID) of the ports. This is the VLAN of which the port is a member.
Tagging Mode	The tagging mode of the port. For information on tagging modes, see "Port Configuration area" on page 132 .
Binding Style	The binding style configured on the port. For information on binding styles, see "Port Configuration area" on page 132 .

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.

To view the Port Configuration Area:

Click **Port Configuration**.

Figure 46: Port Configuration area

The screenshot shows a web interface for Port Configuration. At the top, there are two tabs: 'Selection List' and 'Port Configuration', with 'Port Configuration' being the active tab. Below the tabs, there are three dropdown menus: 'PVID : 1 V1', 'Tagging Mode : Clear', and 'Binding Style : Static'. Below these is a section titled 'Static Binding VLANs' which contains a list of VLANs with checkboxes. The list includes: '0 {Generic}', '1 V1' (which is checked), '255 {Global}', and '888 {XXXXXXX}'.

The following table provides a list of the configuration parameters in the Port Configuration area and their descriptions..

Table 49: 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 field contains all VLANS known to the network and VLANs on the device.
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. <ul style="list-style-type: none">● 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.
1 of 2	

Table 49: Port Configuration area parameters (continued)

Field	Description
Binding Style	<p>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:</p> <ul style="list-style-type: none"> ● 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 Configured - 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 selected in the Static Binding VLANs list. Packets on all other VLANs are discarded.
Static Binding VLANs	<p>A list of VLANs known on the network and VLANs configured on the device. Each VLAN has an accompanying check box. Possible values are:</p> <ul style="list-style-type: none"> ● Selected - The VLAN is bound to the port being configured. ● Cleared - The VLAN is not bound to the port being configured. <p>Note:</p> <p>The settings are only used when the port is configured with the Static Binding Style.</p>
2 of 2	

Managing VLANs

You can create, rename, synchronize, and delete VLANs.

- [Creating VLANs](#)
- [Renaming VLANs](#)
- [Synchronizing VLAN names](#)
- [Deleting VLANs](#)

Creating VLANs

To create a new VLAN:

1. From the **VLAN Configuration** dialog box, click **New**.

Figure 47: Create VLAN dialog box

A screenshot of a 'New VLAN' dialog box. The dialog box has a yellow background and a black border. At the top, there is a title bar with the text '• New VLAN •'. Below the title bar, the text 'The first available VLAN ID is 2.' is displayed in blue. There are two input fields: 'VLAN ID:' and 'VLAN Name:'. The 'VLAN ID:' field is a text box with a yellow background. The 'VLAN Name:' field is a text box with a yellow background. At the bottom of the dialog box, there are two buttons: 'OK' and 'Cancel'.

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

Note:

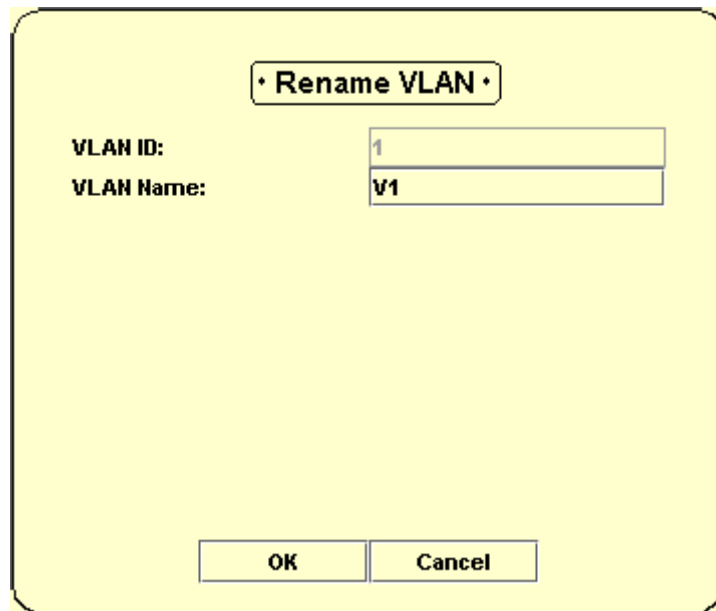
The range of valid VLAN numbers is between **1 - 4090** for the Avaya G430 Device.

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. From the **VLAN Configuration** dialog box, select the VLAN whose name you want to edit.
2. Click **Rename**. The system displays the **Rename VLAN** dialog box.

Figure 48: Rename VLAN dialog boxA screenshot of a 'Rename VLAN' dialog box. The dialog has a yellow background and a black border. At the top center is a title bar with the text '• Rename VLAN •'. Below the title bar, there are two labels: 'VLAN ID:' and 'VLAN Name:'. To the right of 'VLAN ID:' is a text input field containing the number '1'. To the right of 'VLAN Name:' is a text input field containing the text 'V1'. At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel'.

3. Edit the VLAN's name in the **VLAN Name** field.
4. Click **OK**.

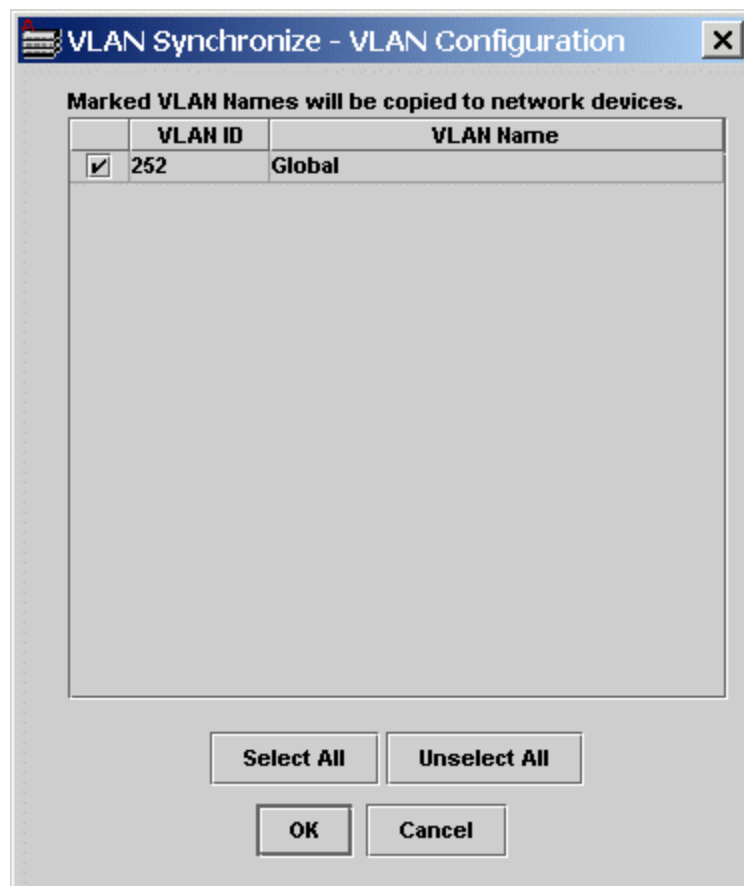
Synchronizing VLAN names

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. From the VLAN Configuration dialog box, click **Sync**. The system displays the **VLAN Synchronize** dialog box. The **VLAN Synchronize** dialog box contains a list of VLANs whose local names differ from the VLAN names in the master VLAN list. For each VLAN, the system displays the following fields:
 - **VLAN ID** - The VLAN number (ID) of the VLAN.
 - **VLAN Name** - The VLAN name in the master VLAN list.

Figure 49: VLAN Synchronize dialog box

2. Select the check boxes next to the VLANs whose names you want to synchronize.
 - To select all the VLANs in the VLAN Synchronize dialog box, click **Select All**.
 - To clear all the VLANs in the VLAN Synchronize dialog box, click **Unselect All**.
3. Click **OK**. The marked VLANs on the device are renamed with the VLAN names in the master VLAN list.

Deleting VLANs

You can delete VLANs from the Avaya G430 Device. Globally known VLANs can be deleted from the device, but not from the master VLAN list. If you delete a VLAN that is on the master VLAN list and on the device, the VLAN remains in the VLAN Tree with a green tag.

To delete a VLAN:

1. Select the VLAN you want to delete.

2. Ensure that there are no member ports associated with the VLAN by deleting all the ports under the VLAN.
3. Click **Delete**.

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

Ports can be selected from the Tree view, Chassis view, or from the 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 **Control** while selecting additional ports.
- To select all the ports on a module, click the module icon in the Tree view or Chassis view.
- To select all the ports on the device, click the device icon in the Tree view or Chassis view.
- To select all 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 the selected ports appear in the Selection List. In addition, parameters that are common to all the ports in the selection appear in the Port Configuration Area.

For details on the information provided in the Selection List, see [“Selection List” on page 131](#).

Using the Port Configuration Area

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

1. Click **Port Configuration**. The system displays the Port Configuration area.
2. Select the ports you want to configure in the Tree view, Chassis view, or VLAN Tree. The settings that are common to all the selected ports appear in the fields in the Port Configuration area. For information on selecting ports, see [“Selecting ports” on page 137](#).
3. Change the settings in the Port Configuration area using the fields and check boxes. For information on the settings in the Port Configuration Area, see [“Port Configuration area” on page 132](#).

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.

Configuring VLANs using drag-and-drop

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

1. Select the ports you want to configure from the Tree view, Chassis view, or VLAN Tree. For information on selecting ports, see [“Selecting ports” on page 137](#).
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. Dragging static binding icons are ignored. The PVIDs of these ports do not change.

Updating the device

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

For more information on user interface, see [“Using dialog boxes and tables” on page 32](#).

Chapter 10: Port Mirroring

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

- [Port Mirroring overview](#) - An overview of port mirroring.
- [Configuring Port Mirroring](#) - Instructions on adding, editing, and deleting a port mirroring pair.
- [The Port Mirroring wizard](#) - Detailed descriptions of the screens in the Port Mirroring wizard.

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, see *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.

Configuring Port Mirroring

This section explains how to configure Port Mirroring on the Avaya G430 Device.

To configure Port Mirroring:

Click .

Or

Select **Configure > Port Mirroring**. The system displays the Port Mirroring wizard.

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:

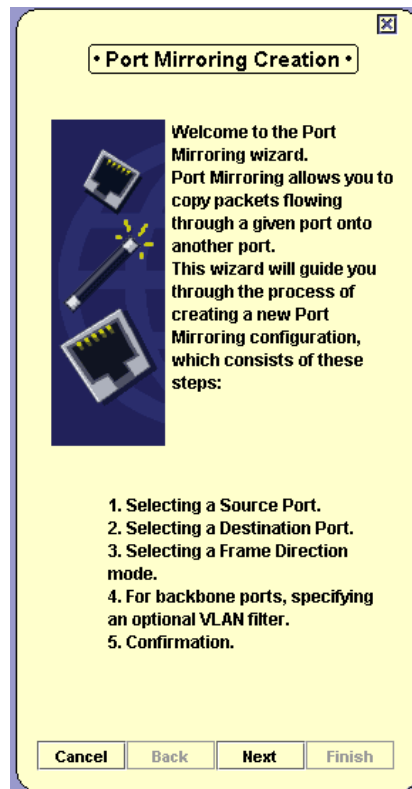
- [Port Mirroring wizard - Create Welcome](#)
- [Port Mirroring wizard - Edit/Delete Welcome](#)
- [Port Mirroring wizard - Source Port Selection](#)
- [Port Mirroring wizard - Destination Port Selection](#)
- [Port Mirroring wizard - Frames Direction Selection](#)
- [Port Mirroring wizard - Confirmation](#)

If Port Mirroring is not currently active on the device, the Port Mirroring wizard starts with the Create Welcome screen. If Port Mirroring is currently active on the device, the Port Mirroring Wizard starts with the Edit/Delete Welcome screen.

Port Mirroring wizard - Create Welcome

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

Figure 50: Port Mirroring wizard - Create Welcome

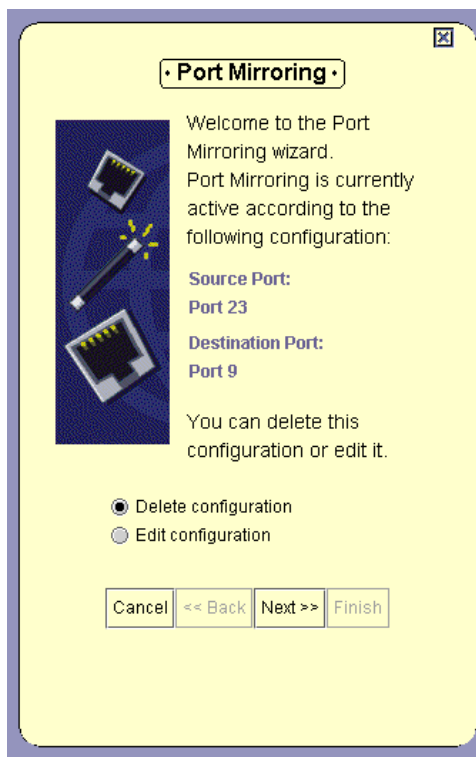


To continue, click **Next**. The Port Mirroring Wizard continues with the [Port Mirroring wizard - Edit/Delete Welcome](#) screen.

Port Mirroring wizard - Edit/Delete Welcome

The wizard offers the choice of deleting or editing the existing Port Mirroring configuration.

Figure 51: Port Mirroring wizard - Edit/Delete Welcome screen



To delete the existing Port Mirroring configuration:

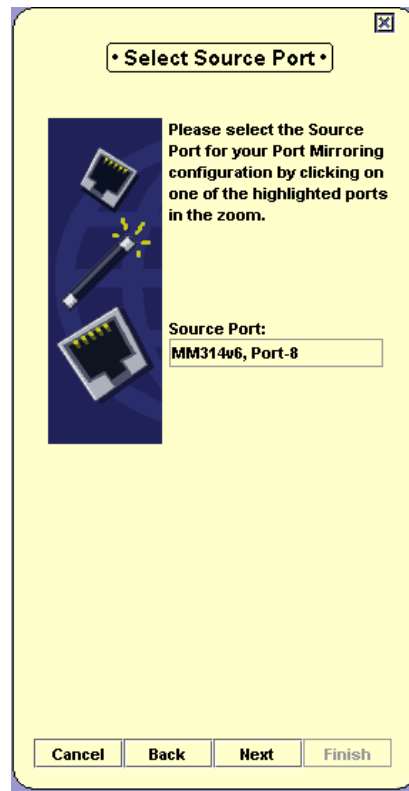
1. Select the **Delete configuration** option.
2. Click **Next**. The Port Mirroring wizard continues with the [Port Mirroring wizard - Confirmation](#) screen.

To edit the existing Port Monitoring configuration:

1. Select the **Edit configuration** option.
2. Click **Next**. The Port Mirroring Wizard continues with the [Port Mirroring wizard - Source Port Selection](#) screen. The current configuration is reflected in the wizard's screens.

Port Mirroring wizard - Source Port Selection

The Source Port Selection screen of the Port Mirroring wizard helps you select a source port for the Port Mirroring pair. Ports that are selected as sources appear white in the Chassis view.

Figure 52: Port Mirroring wizard - Source Port Selection screen

To select a source for the Port Mirroring pair, select a highlighted port in the Chassis view. The selected port appears blue in the Chassis view and Tree view and is listed in the **Source Port** field in the wizard.

After selecting the source for the Port Mirroring, click **Next**. The Port Mirroring wizard continues with the [Port Mirroring wizard - Destination Port Selection](#) screen.

Port Mirroring wizard - Destination Port Selection

The Destination Port Selection screen of the Port Mirroring wizard helps you select a destination port for the Port Mirroring pair. Ports that can be selected as destinations appear white in the Chassis view.

Figure 53: Port Mirroring wizard - Destination Port Selection screen



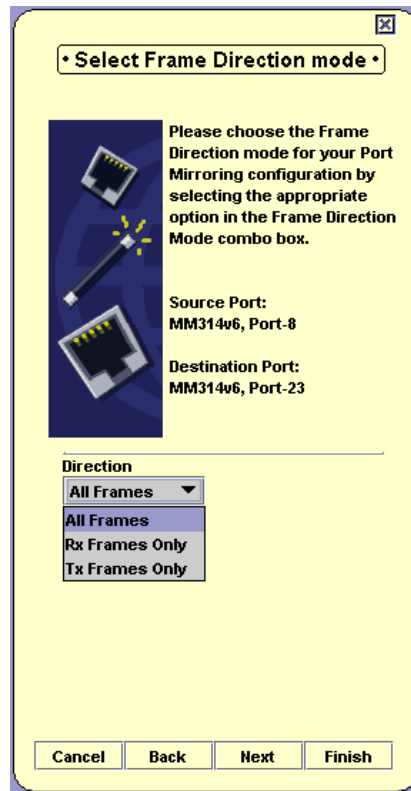
To select a destination for the Port Mirroring pair, select a port in the Chassis view. The selected port appears cyan in the Chassis view and Tree view and is listed in the **Destination Port** field in the wizard.

After selecting the destination for the Port Mirroring pair, click **Next**. The Port Mirroring wizard continues with the [Port Mirroring wizard - Frames Direction Selection](#) screen.

Port Mirroring wizard - Frames Direction Selection

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 the traffic going through the source port, or only the traffic received by the source port.

Figure 54: Port Mirroring wizard - Frames Direction Selection screen



To configure the frames that are copied to the destination port, select an option from the **Frames Direction Mode** field. Possible options are:

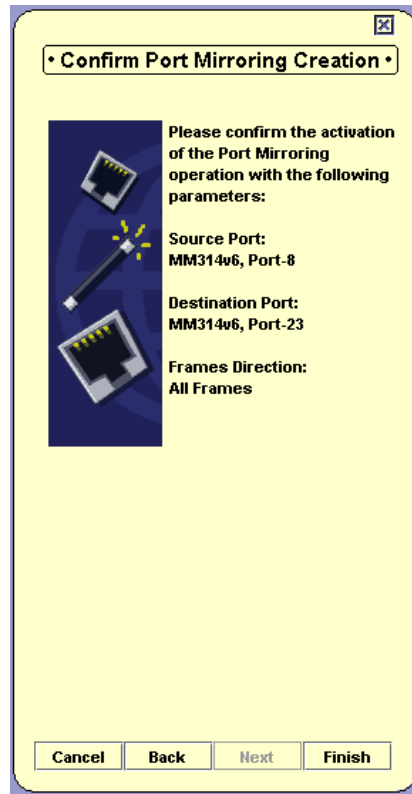
- **All Frames** - All the traffic going through the source port is copied to the destination port.
- **Rx Frames Only** - Traffic received by the source port is copied to the destination port.
- **Tx Frames Only** - Traffic transmitted by the source port is copied to the destination port.

After selecting the traffic to be copied, click **Next**. The Port Mirroring wizard continues with the [Port Mirroring wizard - Confirmation](#) screen.

Port Mirroring wizard - Confirmation

The Port Mirroring wizard displays a summary of the Port Mirroring information entered in the previous screens. The Port Mirroring configuration is not yet uploaded to the device.

Figure 55: Port Mirroring wizard - Confirmation screen



To make 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**.

Chapter 11: Port RMON

This chapter explains the port RMON options of the Avaya G430 Device.

To view Port RMON information, you must be in the Port RMON mode.

To switch to the Port RMON mode:

Click .

Or

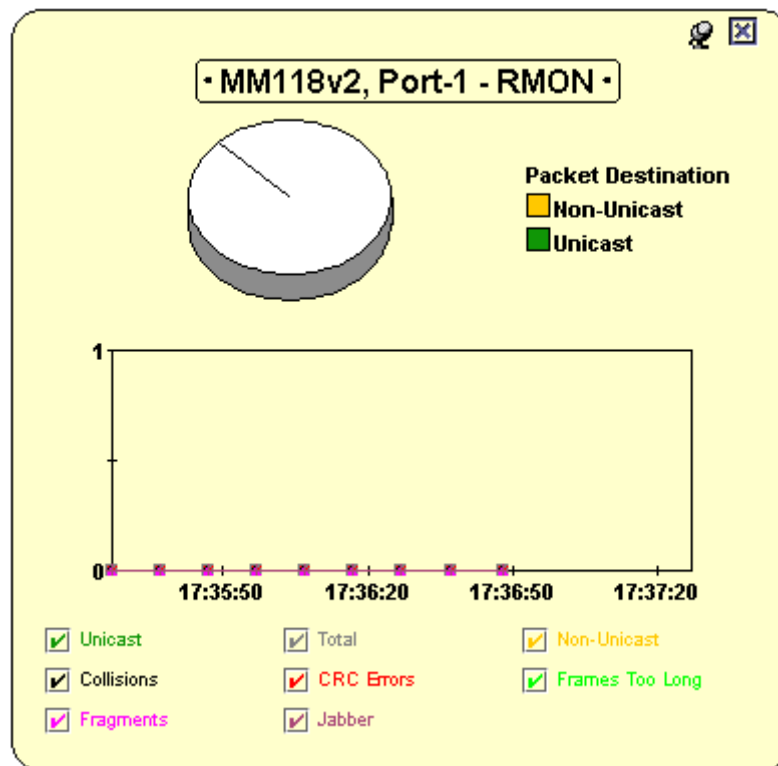
Select **View > Port RMON**.

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

Displaying the Port RMON Window

To display the Port RMON window, select a port in the Chassis or Tree view. The system displays the Port RMON window.

Figure 56: 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. At the bottom of the window is a list of traffic types.

The Pie Chart

The pie chart shows the relative amount of Unicast and Non-Unicast traffic on a selected port. 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 and 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 the statistics. After two seconds, an information box opens 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 the traffic on the port from the time the application was opened until the present time.

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 is 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 check box next to it. Only traffic types whose check boxes are selected are displayed in the Port RMON graph.

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

Table 50: Traffic Types

Field	Description
Unicast	Total number of good packets received that are directed to a unicast address.
Multicast	Total number of good packets directed to a multicast address.
Broadcast	Total number of good packets directed to a broadcast address.
Total	Total number of packets of valid frame length that are received on the port.
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.
Over Size	Total number of Ethernet packets received at this port whose octet count is more than the maximum standard packet length.
Fragments	Total number of Ethernet packets received at this port whose octet count is less than the minimum standard packet length.
Jabber	Total number of Ethernet packets received at this port that are too long and these include CRC errors.
Collisions	Total number of Ethernet collisions in which the port is involved.

Chapter 12: Switch Connected Addresses

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

- [Switch Connected Addresses overview](#) - An overview of the Switch Connected Addresses feature.
- [Viewing the Switch Connected Addresses window](#) - Instructions on accessing the Switch Connected Addresses window, and a description of the Switch Connected Addresses window.

Switch Connected Addresses overview

The Switch Connected Addresses feature allows you to see the devices that are connected to the ports on the Avaya G430 Device. Keeping track of this network information increases the efficiency and security, and assists 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.

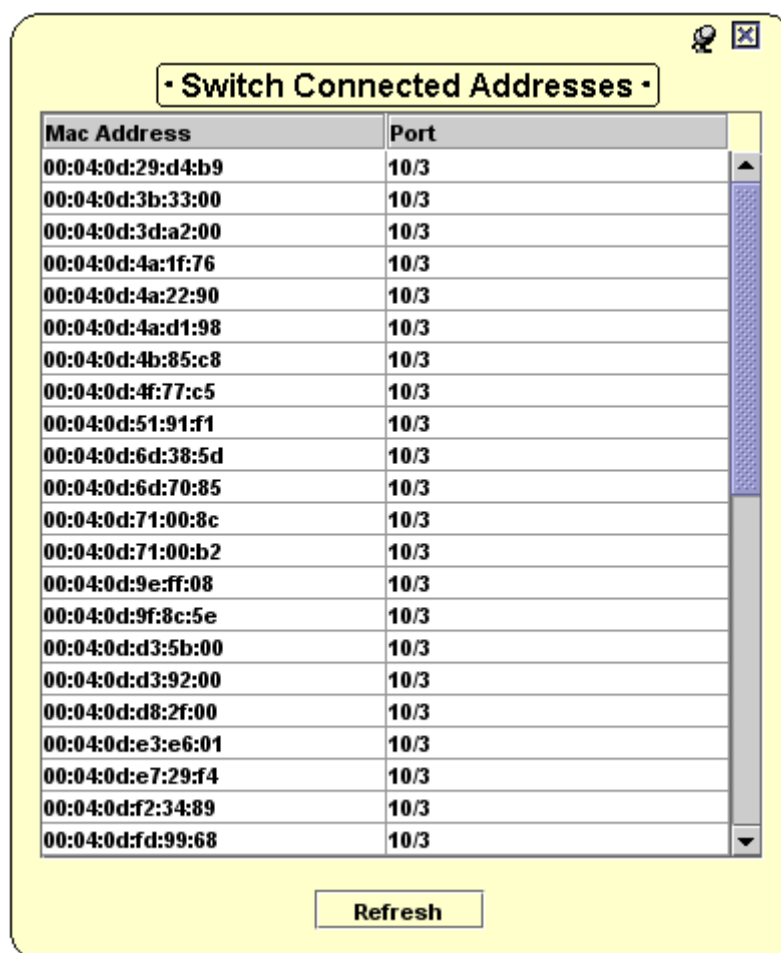
To view the list of connected stations:

Click .

Or

Select **View > Switch Connected Addresses**.

Figure 57: Switch Connected Addresses window



Mac Address	Port
00:04:0d:29:d4:b9	10/3
00:04:0d:3b:33:00	10/3
00:04:0d:3d:a2:00	10/3
00:04:0d:4a:1f:76	10/3
00:04:0d:4a:22:90	10/3
00:04:0d:4a:d1:98	10/3
00:04:0d:4b:85:c8	10/3
00:04:0d:4f:77:c5	10/3
00:04:0d:51:91:f1	10/3
00:04:0d:6d:38:5d	10/3
00:04:0d:6d:70:85	10/3
00:04:0d:71:00:8c	10/3
00:04:0d:71:00:b2	10/3
00:04:0d:9e:ff:08	10/3
00:04:0d:9f:8c:5e	10/3
00:04:0d:d3:5b:00	10/3
00:04:0d:d3:92:00	10/3
00:04:0d:d8:2f:00	10/3
00:04:0d:e3:e6:01	10/3
00:04:0d:e7:29:f4	10/3
00:04:0d:f2:34:89	10/3
00:04:0d:fd:99:68	10/3

Refresh

All the connections to the Avaya G430 Device are listed with their respective ports in the Switch Connected Addresses window. The rows of the Switch Connected Addresses window comprise of 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.

To refresh the information in the Switch Connected Addresses window, click **Refresh**.

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 the column heading of the field by which the list is sorted.

For more information on user interface, see [“Using dialog boxes and tables” on page 32](#).

Chapter 13: Port Redundancy

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

- [Overview of Port Redundancy](#) - An overview of port redundancy.
- [Configuring Port Redundancy](#) - Instructions on accessing the Port Redundancy dialog box, and a description of the Port Redundancy dialog box.
- [Adding a Port Redundancy](#) - Instructions on configuring a new port redundancy.
- [Port Redundancy wizard](#) - Detailed descriptions of the screens in the Port Redundancy Wizard.
- [Deleting Port Redundancies](#) - Instructions on deleting port redundancies.
- [Updating the device](#) - Instructions on updating the device with the changes made to the Port Redundancy dialog box.

Overview of Port Redundancy

Port Redundancy enables you to define a redundancy relationship between any two ports in a device. One port is defined as the primary port and the other as the secondary port. In case the primary port link fails, the secondary port takes over. This connection between the two ports is called a Port Redundancy.

Note:

To edit Port Redundancy information, you must delete the Port Redundancy, and create a new one.

For more information on Port Redundancy, see *Redundancy* in *The Reference Guide*.

Configuring Port Redundancy

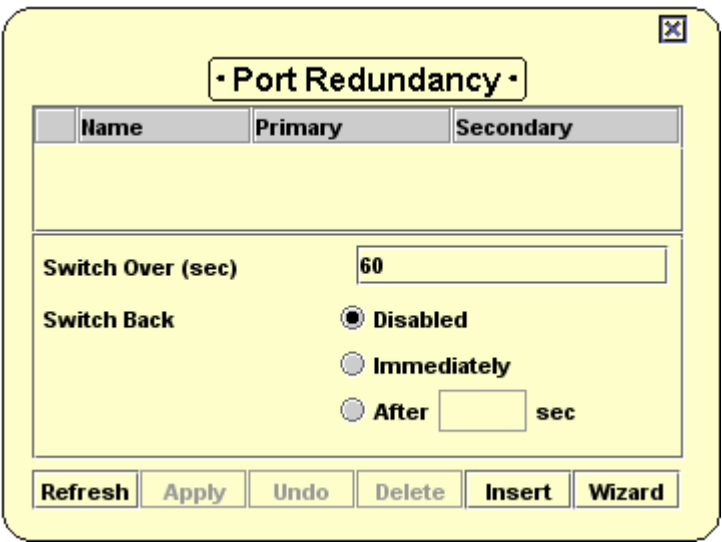
To view the Port Redundancy dialog box:

Click .

Or

Select **Configure > Port Redundancy**.

Figure 58: Port Redundancy dialog box

The image shows a software dialog box titled "Port Redundancy". It features a table with three columns: "Name", "Primary", and "Secondary". Below the table, there are configuration options: "Switch Over (sec)" with a text input field containing "60", and "Switch Back" with three radio button options: "Disabled" (which is selected), "Immediately", and "After" followed by a text input field and the unit "sec". At the bottom of the dialog, there is a row of buttons: "Refresh", "Apply", "Undo", "Delete", "Insert", and "Wizard".

The **Port Redundancy** dialog box provides a list of all the port redundancies configured on the switch, with their respective primary and secondary ports along with the device's port redundancy configuration.

The following table provides a list of the fields in the **Port Redundancy** dialog box and their descriptions.

Table 51: Port Redundancy fields

Field	Description
Name	The name of the port redundancy.
Primary	The primary port of the port redundancy pair.
Secondary	The secondary port of the port redundancy pair.
Switch Over (seconds)	The minimum time for switching between the ports in a port redundancy pair.
1 of 2	

Table 51: Port Redundancy fields (continued)

Field	Description
Switch Back	<p>The amount of time after the primary port link is re-established, after which the primary port takes over from the secondary port. Possible values include:</p> <ul style="list-style-type: none"> ● Disabled - The primary port does not take over from the secondary port. ● Immediately - The primary port takes over from the secondary port as soon as the primary port link is re-established. ● After x sec - The primary port takes over from the secondary port x seconds after the primary port link is re-established.
2 of 2	

To configure the device's port redundancy configuration:

1. Enter an amount in the **Switch Over** field to determine the initial switching time between the ports in a port redundancy pair.
2. Select one of the options in the **Switch Back** field.
3. If you select **After x sec**, enter the number of seconds for the switch back in the **After x sec** field.
4. Update the device. For more information on updating the device, see ["Updating the device" on page 162](#).

Adding a Port Redundancy

To add a new Port Redundancy:

1. From the **Port Redundancy** dialog box, click **Wizard**. The Port Redundancy wizard starts. For more information, see ["Port Redundancy wizard" on page 156](#).

Or

From the **Port Redundancy** dialog box, click **Insert**. A row is added to the **Port Redundancy** dialog box.

2. Enter a name for the Port Redundancy in the **Name** field.
3. Select a port from the Tree view or the Chassis view and drag it to the **Primary Port** field. The port number name appears in the **Primary Port** field.
4. Select a port from the Tree view or the Chassis view and drag it to the **Secondary Port** field. The port number name appears in the **Secondary Port** field.

Port Redundancy

5. Update the device. For more information on updating the device, see [“Updating the device” on page 162](#).

Note:

A port cannot participate in more than one redundancy scheme.

Port Redundancy wizard

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

The Port Redundancy wizard consists of the following screens:

- [Port Redundancy wizard - Welcome](#)
- [Port Redundancy wizard - Primary Port Selection](#)
- [Port Redundancy wizard - Secondary Port Selection](#)
- [Port Redundancy wizard - Name and Type](#)
- [Port Redundancy wizard - Confirmation](#)

Port Redundancy wizard - Welcome

The Port Redundancy wizard provides a simple, step-by-step method for creating a Port Redundancy.

Figure 59: Port Redundancy wizard - Welcome screen

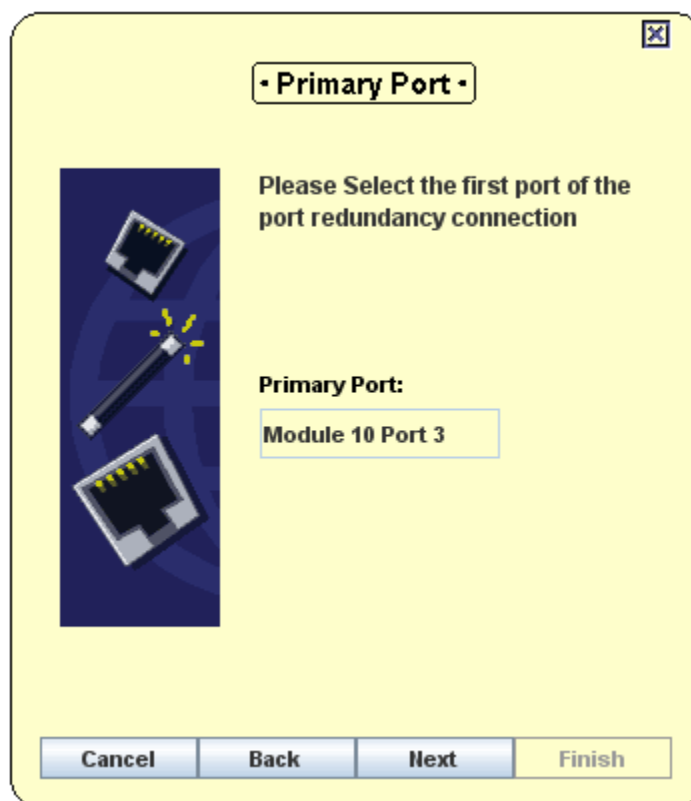


To continue, click **Next**. The Port Redundancy wizard continues with the [Port Redundancy wizard - Primary Port Selection](#) screen.

Port Redundancy wizard - Primary Port Selection

The Primary Port Selection screen of the Port Redundancy wizard helps you select a primary port for the Port Redundancy. Ports which can be selected as primary ports appear in white in the Chassis view.

Figure 60: Port Redundancy wizard - Primary Port Selection screen



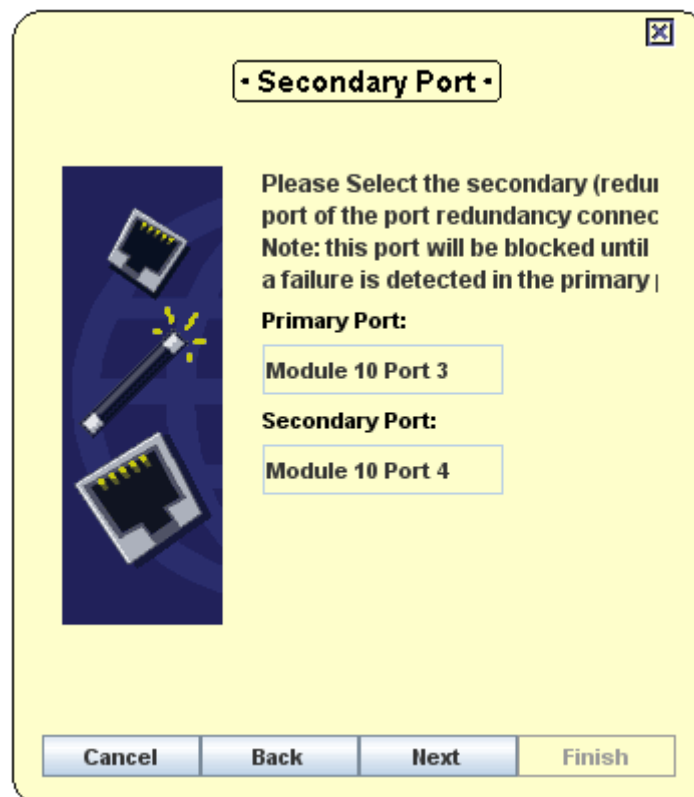
To select a primary port for the Port Redundancy, click a port in the Chassis view. The selected port appears blue in the Chassis view and Tree view, and is listed in the **Primary Port** field in the wizard.

After selecting the primary port for the Port Redundancy, click **Next**. The Port Redundancy wizard continues with the [Port Redundancy wizard - Secondary Port Selection](#) screen.

Port Redundancy wizard - Secondary Port Selection

The Secondary Port Selection screen of the Port Redundancy wizard allows you to select a secondary port for the Port Redundancy. Ports that can be selected as secondary ports appear white in the Chassis view.

Figure 61: Port Redundancy wizard - Secondary Port Selection screen



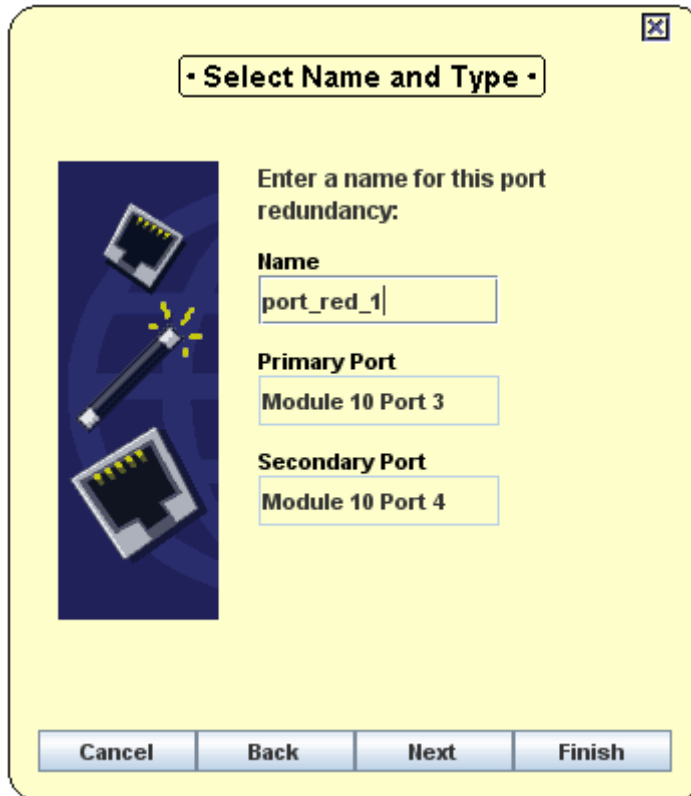
To select a secondary port for the Port Redundancy, click a port in the Chassis view. The selected port appears cyan in the Chassis view and Tree view, and is listed in the **Secondary Port** field in the wizard.

After selecting the secondary port for the Port Redundancy, click **Next**. The Port Redundancy wizard continues with the [Port Redundancy wizard - Name and Type](#) screen.

Port Redundancy wizard - Name and Type

The Port Redundancy Name and Type screen of the Port Redundancy wizard allows you to assign a name for the Port Redundancy.

Figure 62: Port Redundancy wizard - Name and Type screen



- Select Name and Type -

Enter a name for this port redundancy:

Name
port_red_1

Primary Port
Module 10 Port 3

Secondary Port
Module 10 Port 4

Cancel Back Next Finish

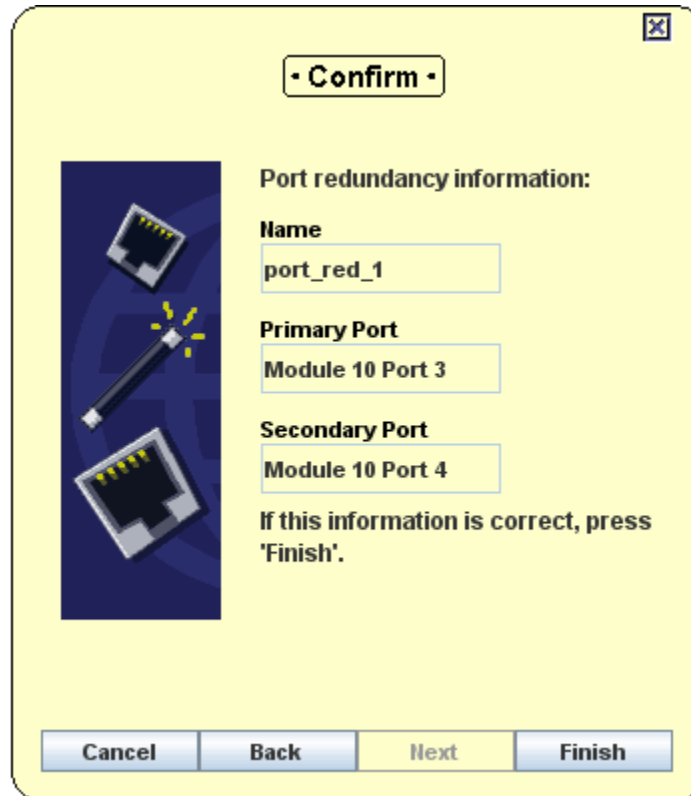
To assign a name to the Port Redundancy, enter the name for the Port Redundancy in the **Name** field.

After selecting a name and a type for the Port Redundancy, click **Next**. The Port Redundancy wizard continues with the [Port Redundancy wizard - Confirmation](#) screen.

Port Redundancy wizard - Confirmation

The Port Redundancy wizard displays a summary of the Port Redundancy information entered using the previous screens. The Port Redundancy is not yet created.

Figure 63: Port Redundancy wizard - Confirmation screen

The image shows a confirmation dialog box titled '- Confirm -'. On the left is a graphic of two network ports connected by a cable. On the right, under the heading 'Port redundancy information:', there are three text boxes: 'Name' with the value 'port_red_1', 'Primary Port' with the value 'Module 10 Port 3', and 'Secondary Port' with the value 'Module 10 Port 4'. Below these boxes is the instruction 'If this information is correct, press 'Finish''. At the bottom are four buttons: 'Cancel', 'Back', 'Next', and 'Finish'.

To make changes to the summary information:

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

To create the Port Redundancy, click **Finish**. The Port Redundancy information is uploaded to the device, and the **Port Redundancy** dialog box is refreshed.

Deleting Port Redundancies

To delete an existing Port Redundancy:

1. Select a Port Redundancy from the **Port Redundancy** dialog box.

To select more than one Port Redundancy, press **Control** while clicking additional Port Redundancies.

2. Click **Delete**. The selected Port Redundancies are marked with the  symbol.

Updating the device

To update the device with all the changes made to the **Port Redundancy** dialog box, click **Apply**.

To discard all the changes made to the **Port Redundancy** dialog box, click **Refresh**.

For more information on user interface, see [“Using dialog boxes and tables” on page 32](#).

For more information on tables, see [“Managing tables” on page 23](#).

Chapter 14: Trap Managers Configuration

This chapter provides the information and instructions for configuring trap managers for the Avaya G430 Device. It includes the following sections:

- [Trap Manager overview](#) - An overview of trap managers.
- [Configuring Trap Managers](#) - Instructions on accessing the device's Trap Managers Table, and a description of the Trap Managers Table.
- [Editing the Trap Managers Table](#) - Instructions on how to edit the Trap Managers Table.

Trap Manager overview

In the event of a fault or an unusual occurrence, the Avaya G430 Device sends traps to one or more Network Management Stations (NMS). To enable this feature, you must configure the Avaya G430 Device with a list of the managers' workstations. Traps are then sent to the stations listed in the Managers table.

Note:

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

Using the Trap Managers Table you can also configure the traps that are sent. Selecting the check box for a trap enables the manager to receive the trap. Managers receive only traps that are selected.

Configuring Trap Managers

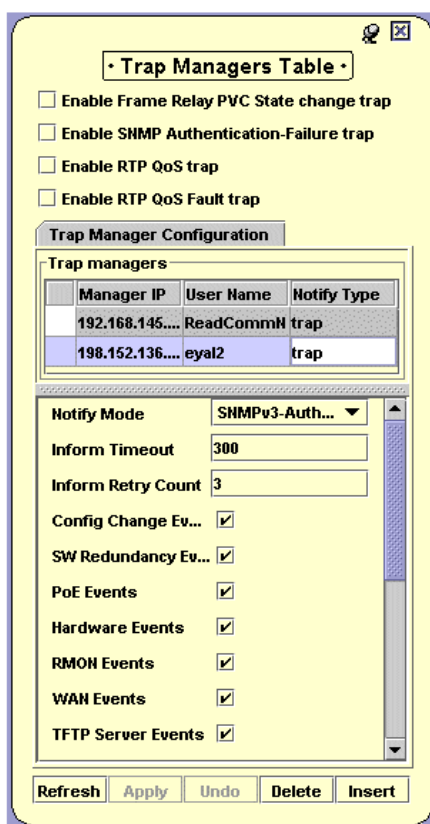
To view the Trap Managers table for the device:

Click  .

Or

Select **Configure > Trap Managers**.

Figure 64: Device Trap Managers Table



The following table describes the information displayed in the Device Trap Managers Table.

Table 52: Device Trap Managers Table

Item	Description
Enable Frame Relay PVC State change trap	When selected, enables Frame Relay PVC State Change trap.
1 of 3	

Table 52: Device Trap Managers Table (continued)

Item	Description
Enable SNMP Authentication-Failure trap	When selected, enables SNMP Authentication-Failure trap.
Enable RTP QoS trap	When selected, enables RTP QoS trap.
Enable RTP QoS Fault trap	When selected, enables RTP QoS Fault trap.
Manager IP	IP address of the management station that receives the traps.
User Name	The SNMPv3 user authentication name.
Notify Type	The type of notification. Possible values are: <ul style="list-style-type: none"> • Trap • Event
Notify Mode	The notification mode. Possible values are: <ul style="list-style-type: none"> • SNMPv1 • SNMPv3
Inform Timeout	The number of seconds for an event message to connect to the manager before failing.
Inform Retry Count	The number of failed event attempts before an event is discarded.
Config Change Events	When selected, configuration change events are sent to the manager.
SW Redundancy Event	When selected, software redundancy events are sent to the manager.
PoE Events	When selected, PoE events are sent to the manager.
Hardware events	When selected, hardware events are sent to the manager.
RMON Events	When selected, RMON events are sent to the manager.
DHCP Client Events	When selected, DHCP client events are sent to the manager.
FileSys Events	When selected, Avaya Load MIB events such as download and upload success/failure/start, are sent to the manager.
DHCP Server Events	When selected, DHCP server events are sent to the manager.
TFTP Events	When selected, TFTP events are sent to the manager.
WAN Events	When selected, WAN events are sent to the manager.
Media Gateway Events	When selected, Media Gateway events are sent to the manager.
Security Events	When selected, security events are sent to the manager, including 802.1x and MSS notifications.
2 of 3	

Table 52: Device Trap Managers Table (continued)

Item	Description
TFTP Server Events	When selected, TFTP Server events are sent to the manager.
RADIUS Events	When selected, RADIUS authentication events are sent to the manager.
PoE Events	When selected, Power over Ethernet events are sent to the manager.
RTP Events	When selected, RTP events are sent to the manager.
L3 Events	When selected, Layer 3 events are sent to the manager.
Link Events	When selected, link events are sent to the manager.
Policy Events	When selected, policy events are sent to the manager.
Eth Port Fault Events	When selected, Ethernet port fault events are sent to the manager.
Generic Events	When selected, generic events are sent to the manager.
3 of 3	

The first row in the Device Trap Managers Table is reserved for the Dynamic Trap Manager entry. The Dynamic Trap Manager is discovered automatically and the IP address is read-only. The entry row for the Dynamic Trap Manager is highlighted in grey.

For information on adding and removing trap managers and editing their trap reporting statuses, see [“Editing the Trap Managers Table” on page 166](#).

Editing the Trap Managers Table

You can add and remove managers from the Trap Managers Table.

To add managers to the table:

1. Click **Insert**.
2. Enter the IP address 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.

Chapter 15: Routing Manager

This chapter provides an introduction to the Avaya G430 Routing Manager. It includes the following sections:

- [The Routing Manager user interface](#) - An introduction to the Avaya G430 Routing Manager user interface.
- [Editing tables](#) - An explanation on editing the Avaya G430 Routing Manager table.
- [Saving table information in a file](#) - Instructions on saving the information in a table to a text file.
- [Saving configuration changes](#) - An explanation on applying and saving configuration changes to routers.
- [Resetting a router](#) - Instructions on resetting routers.
- [Using the Avaya G430 Routing Manager help](#) - An explanation of the options for accessing the online help in the Avaya G430 Routing Manager.

The Routing Manager user interface

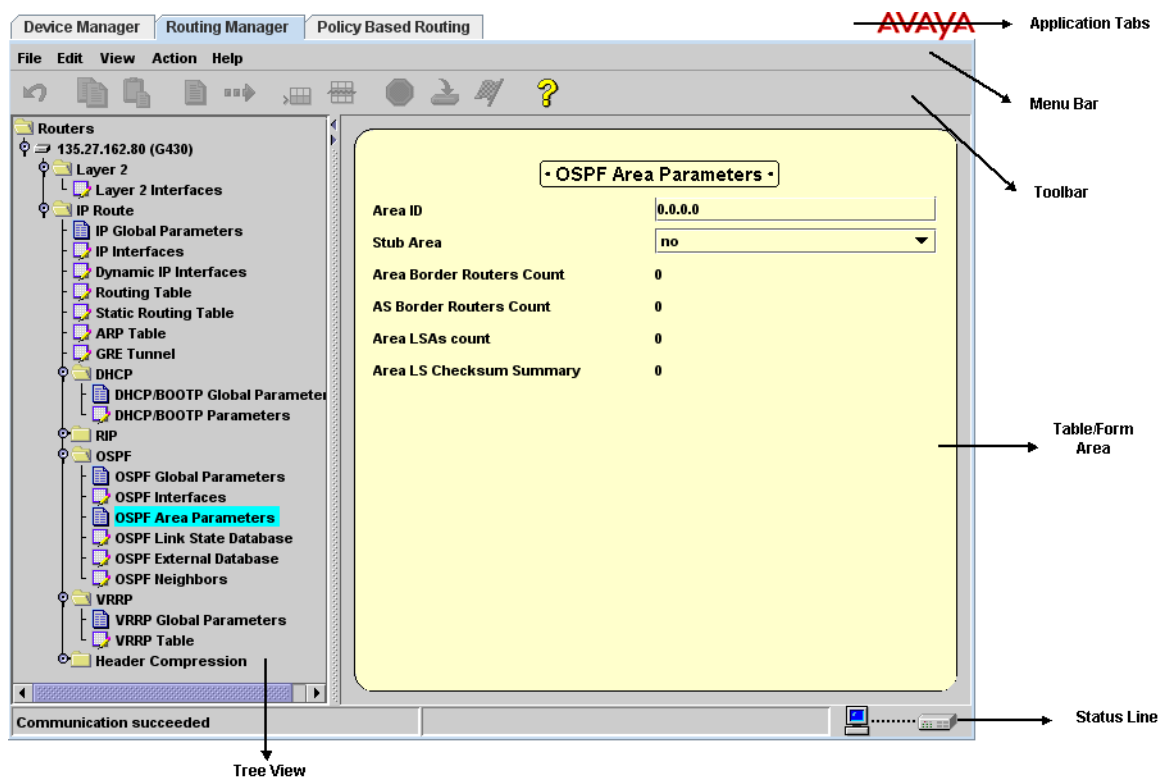
The user interface consists of the following elements:

- [Toolbar](#) - A toolbar providing shortcuts to the main Routing Manager functions.
- [Tree view](#) - A resizable window containing a representation of the configuration windows of the Avaya G430 Routing Configuration.
- [Table/Form Area](#) - A resizable window where all tables and forms are displayed.

For information on other parts of the user interface, see [“The user interface” on page 22](#).

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

Figure 65: Avaya G430 Routing Manager user interface




To resize the main areas of the user interface, the Tree view, the Table Area, and the Table/Form Area, use the splitter bars and their arrows.

Toolbar

The Toolbar provides shortcuts to the main Routing Manager functions.











The following table describes the buttons on the Application toolbar and gives the equivalent menu options.

Table 53: Application toolbar

Button	Description	Menu Item
	Undoes changes made to the table or form currently displayed.	Edit > Undo

1 of 2

Table 53: Application toolbar (continued)

Button	Description	Menu Item
	Copies the selected information to the clipboard.	Edit > Copy
	Pastes information from the clipboard into the selected table row.	Edit > Paste
	Toggles the display of a form corresponding to the current table.	View > Form
	Toggles the display of additional table parameters.	View > More
	Adds a row to the table.	Edit > Insert Row
	Deletes the selected table row.	Edit > Delete Row
	Stops loading information into the current table.	Action > Stop
	Sends the configuration information to the device.	Action > Apply
	Opens a dialog box which enables you to specify the starting point in the display of a table.	Action > Start Point
	Opens the online help for context-sensitive information.	Help > Context Sensitive Help
2 of 2		

Tree view

The Tree view shows the applicable configuration windows for the Avaya G430 Device's routing function.

To expand the view of the element when it is contracted, or to contract the view when it is expanded in the tree:

Double-click the element.

Or

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

Table/Form Area

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

To view additional parameters in the table:

Click .

Or

Open Select **View > More**.

To hide additional parameters in the table:

Click .

Or

Select **View > More**.

To toggle the display of forms associated with table rows:

1. Select a table row.



2. Click .

Or

Select **View > Form**.

Editing tables

The Avaya Routing Manager user interface enables you to create, modify, and delete table entries in selected windows. Information can be added directly into the table, or in a form associated with the table.

To undo all the changes made to a table, click . When all the changes are finalized, click  to update the router.


Creating new table entries

To create a new table entry:

1. Click .


Or

Select **Edit > Insert Row**.

2. Enter data in the fields as required.
3. Click  to update the router.


Modifying table entries

To modify data in table entries:

1. Select the table entry you want to modify by clicking it.
2. Click a field.
3. Modify the value of the selected parameters.
4. After editing the table, click  to update the router.

Deleting table entries

To delete a table entry:

1. Select the table entry you want to delete by clicking it.
2. Click .

Or

Select **Edit > Delete Row**.

3. Click  to update the router.

Saving table information in a file

Information in tables can be saved to text files.

To save the information in the current table to a text file:


1. Select **File > Save**. The system displays the **File Save** dialog box.
2. Use the browser to select a directory.
3. Enter a filename in the **File name** field.
4. Click **Save**.

Saving configuration changes

There are two levels of applying routing configuration changes to the router:

- [Running changes](#) - Changes are applied to the router, but are not saved.
- [Committed changes](#) - Changes are saved to the router.

Running changes

After finalizing all the changes to a dialog box or table, the changes must be sent to the router. To send the changes to the router, click . The configuration changes are applied to the router.

The changes remain in effect until the router is reset. When the router is reset, it is configured with the last saved configuration. All changes that are applied but not saved are lost.

Committed changes

To make configuration changes permanent, the changes must be committed (saved) to the router. To commit the configuration to the router, select **File > Commit**.

Resetting a router

To reset a router:

1. Click the router's icon in the Tree view.
2. Select **Action > Reset**.
3. Click **Yes**.

Using the Avaya G430 Routing Manager help

This section explains how to use the online help in the Avaya G430 Routing Manager. The online help can be opened to the contents page or directly to a topic of interest.


Note:

When running the Avaya G430 Manager through web management, online help is only available if you install the online help on your network and configure the device with the location of the help files.

Opening the Help to the contents page

To open the help to the contents page, select **Help > Help Contents**.

Opening the Help to a topic of interest

To open the help directly to a topic of interest, click . The system displays the topic currently selected from the online help.

Chapter 16: Layer 2

The Layer 2 folder provides access to the following window:

- [Layer 2 Interfaces](#)

Layer 2 Interfaces

To display the layer 2 interfaces:

Select **Layer 2 > Interfaces**.

Figure 66: Layer 2 Interfaces window

	Interface Name	Interface Description	MAC Address	Peer Address	Admin Status	Oper Status
●	FastEthernet 10/2		00:07:3B:E4:67:F4		<input checked="" type="checkbox"/>	Disable
●	Vlan 1		00:07:3B:E4:67:F1		<input checked="" type="checkbox"/>	Enable
●	Vlan 45		00:07:3B:E4:67:F1		<input checked="" type="checkbox"/>	Enable
●	Vlan 66		00:07:3B:E4:67:F1		<input checked="" type="checkbox"/>	Enable
●	Dialer 1		N/A	0.0.0.0	<input checked="" type="checkbox"/>	Disable

The following parameters are displayed:

Table 54: Layer 2 Interfaces window parameters

Field	Description
Interface Name	The name of this Layer 2 interface.
Interface Description	Description of this Layer 2 interface.
MAC Address	The MAC address of this Layer 2 interface.
Peer Address	The peer address of this Layer 2 interface.
Admin Status	The administrative status of this Layer 2 interface.
Oper Status	The operational status of this Layer 2 interface.

All fields except for **Interface Description** in the Layer 2 Interfaces window are read-only.

Chapter 17: Policy Based Routing Manager

This chapter provides an introduction to the Avaya G430 Policy Based Routing Manager. It includes the following sections:

- [The Policy Based Routing Manager user interface](#) - An introduction to the Avaya G430 Policy Based Routing Manager user interface.
- [The Application Editor tool](#) - An explanation on launching the Application Editor tool.
- [Saving configuration changes](#) - An explanation on saving the changes to the Policy Based Routing configuration.
- [Using the Avaya G430 Policy Based Routing Manager help](#) - An explanation of the options for accessing online help in the Avaya G430 Routing Manager.

The Policy Based Routing Manager user interface

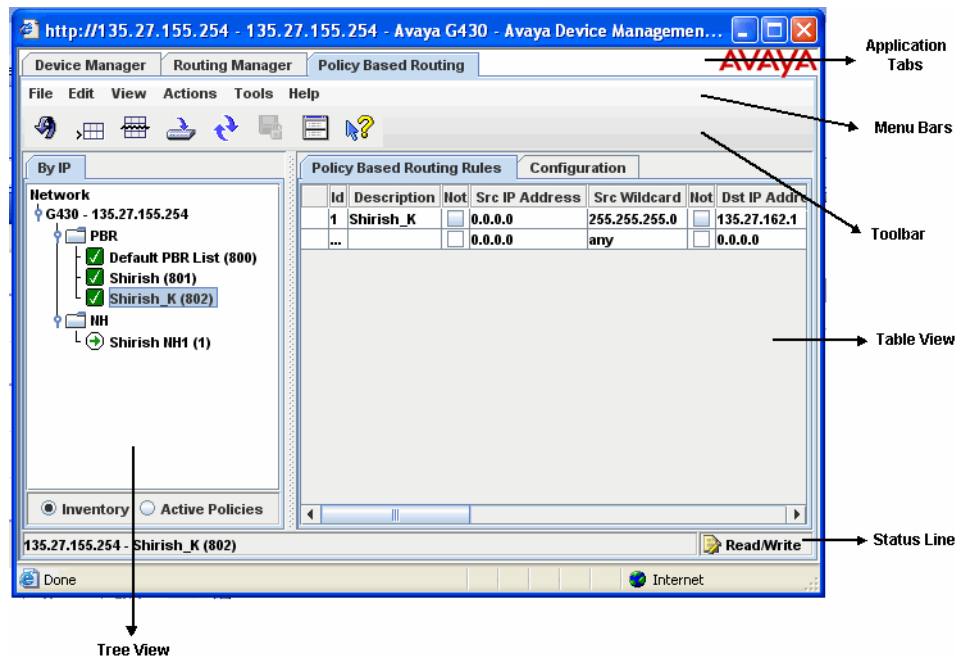
The user interface consists of the following elements:

- [Toolbar](#) - A toolbar providing shortcuts to the main Routing Manager functions.
- [Tree view](#) - A resizable window containing a representation of the configuration windows of the Avaya G430 Routing Configuration.
- [Table view](#) - A resizable window where all the tables and forms are displayed.

For information on other parts of the user interface, see [“The user interface” on page 22](#).

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

Figure 67: Avaya G430 Policy Based Routing Manager user interface



To resize the main areas of the user interface, the Tree view, and the Table view, use the splitter bars and their arrows.

Toolbar

The Toolbar provides shortcuts to the main Policy Based Routing Manager functions.

The following table describes the buttons on the Application toolbar and gives the equivalent menu options.

Table 55: Application toolbar








Button	Description	Menu Item
	Clears applied changes and reverts to the last saved configuration.	Edit > Revert
	Adds a row to the table.	Edit > Add
	Deletes the selected row of the table.	Edit > Delete
	Sends the configuration to the device without saving.	
	Refreshes the information in the Table view.	View > Refresh

Table 55: Application toolbar (continued)

Button	Description	Menu Item
	Sends the configuration to the device and saves the configuration.	File > Commit
	Opens the online help for context-sensitive information.	Help > Help On

Tree view

The Tree view shows the applicable configuration windows for the Avaya G430 Device's Policy Based Routing function.

To expand the view of an element when it is contracted, or to contract the view when it is expanded in the tree:

Double-click the element.

Or

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

Table view

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

The Application Editor tool

The Application Editor tool enables you to specify application protocols by selecting an application name that represents the protocol and the port number information. For more information on using the Applications editor tool, see [“Applications Editor Tool” on page 239](#).


Saving configuration changes

There are two levels of applying routing configuration changes to the router:

- [Applied changes](#) - Changes are applied to the router, but are not saved.

- [Committed changes](#) - Changes are saved to the router.

Applied changes

After finalizing all the changes to a dialog box or a table, the changes must be sent to the router. To send the changes to the router, click . The configuration changes are applied to the router.

The changes remain in effect until the router is reset. When the router is reset, it is configured with the last saved configuration. All applied changes that are not saved are lost.

Committed changes

To make configuration changes permanent, the changes must be committed (saved) to the router. To commit the configuration to the router, select **File > Commit**.

Using the Avaya G430 Policy Based Routing Manager help

This section explains how to use the online help in the Avaya G430 Policy Based Routing Manager. The online help can be opened to the contents page or directly to a topic of interest.


Note:

When running the Avaya G430 Manager through web management, online help is available only if you install the online help on your network and configure the device with the location of the help files.

Opening the Help to the Contents Page

To open the help to the contents page, select **Help > Help Contents**.

Opening the Help to a topic of interest

To open the help directly to a topic of interest, click . The system displays the currently selected topic of the online help.

Chapter 18: IP Route

The IP Route folder provides access to the following windows:

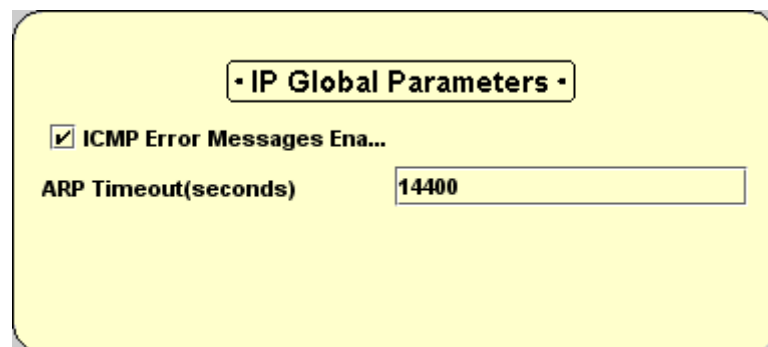
- [Displaying IP Global Parameters](#)
- [Configuring IP interfaces](#)
- [Viewing the Routing Table](#)
- [Viewing the ARP Table](#)
- [Configuring GRE tunneling](#)
- [DHCP](#)
- [RIP](#)
- [OSPF](#)
- [VRRP](#)
- [Header Compression](#)

Displaying IP Global Parameters

To display and update the IP global parameters:

Select **IP Route > IP Global Parameters**.

Figure 68: IP Global Parameters window



The following parameters are displayed:

Table 56: IP Global Parameters

Field	Description
ICMP Error Messages Enable	If selected, ICMP error messages are sent. If not selected, ICMP error messages are not sent.
ARP Timeout (seconds)	The number of seconds between ARP requests concerning entries in the ARP table. After this period, the entry is deleted from the table.

Configuring IP interfaces

IP interfaces represent the logical connections of the device to the IP nets or subnets attached to it. Each IP interface corresponds to one net or subnet.

You can either create a static IP interface or an unnumbered IP interface. When you create a new IP interface, RIP and OSPF interfaces are automatically created and assigned the enable status. When you delete an IP interface, the device deletes the associated RIP and OSPF interfaces.

Note:

An unnumbered IP interface can be configured on point-to-point interfaces only.
An unnumbered IP interface supports all the parameters of a static PPP IP interface except for **Broadcast address**, which cannot be configured on the unnumbered IP interface.

To create entries in the IP interface table, first specify whether the interface is static or unnumbered using the **Type** field (the default value is static). Then configure the following fields:

- If you are configuring a static interface, configure the **IP Address**, **IP Netmask**, and **Layer 2 Interface Name** fields.
- If you are configuring an unnumbered interface, configure the **Layer 2 Interface Name** and **Reference Layer 2 Interface Name** fields. You need not configure **IP address** and **IP Netmask** fields.

To define and display the IP interfaces:

Select **IP Route > IP Interfaces**.

Figure 69: IP Interfaces window





	IP Interface Name	Type	IP Address	Reference IP Address	IP Netmask	Layer 2 Interface Name	Reference Layer 2 Interface Name	Status	Oper Status
●	Vlan 1	Static	135.27.162.80	N/A	255.255.255.0	Vlan 1	N/A	✓	✓

The following parameters are displayed:

Table 57: IP Interface Table parameters

Field	Description
IP Interface Name	The name assigned to the selected IP interface.
IP Address	The IP address assigned to the device on this subnet.
Reference IP Address	The IP address borrowed for an unnumbered IP interface. If the IP address is not unnumbered this field returns a value of N/A .
IP NetMask	The IP network mask of the attached net or subnet.
Layer 2 Interface name	<p>The name of the Layer 2 interface with which this subnet is associated. Multiple subnets may be associated with a single VLAN, so multiple IP interfaces may be associated with the same IP Name.</p> <p>Note:</p> <p>For unnumbered IP interfaces, this field shows only point-to-point interfaces such as GRE tunnel, Serial Interface, and Dialer.</p>
Reference Layer 2 Interface Name	<p>An 'alias' name for the lower layer interface used to borrow an unnumbered IP address. To designate the interface as unnumbered, enter a reference interface name. If the IP address is numbered this field returns a value of N/A.</p> <p>Note:</p> <p>An unnumbered IP interface cannot point to another unnumbered IP interface.</p>
Type	<p>The type of IP address assignment on the interface. Possible values are:</p> <ul style="list-style-type: none"> ● Static - The address is assigned by user configuration. ● DHCP/IPCP - The address is assigned remotely by a DHCP server or by an IPCP session. The DHCP/IPCP values are read-only; they can be changed in the Dynamic IP Interfaces table (see "Viewing the Dynamic IP Interfaces Table" on page 185). <p>Unnumbered - The interface is unnumbered and has no IP address.</p>
Status	The status of the IP interface. If selected, the IP interface is enabled.
Oper Status	The operational status of the IP interface.
1 of 2	

Table 57: IP Interface Table parameters (continued)

Field	Description
Directed Broadcast	<p>When enabled, the router forwards directed broadcasts to an attached network.</p> <p>Note:</p> <p>This field is only available when additional parameters are selected. To select additional parameters, click  on the Routing Manager Application Toolbar.</p>
Proxy ARP	<p>When enabled, the router responds to ARP requests received on a Layer 2 interface, for a device reachable on a different Layer 2 interface. The response is the Mac address of the router interface.</p> <p>Note:</p> <p>This field is only available when additional parameters are selected. To select additional parameters, click  on the Routing Manager Application Toolbar.</p>
Netbios Rebroadcast	<p>The status of Netbios rebroadcast service on the interface. Possible values are:</p> <ul style="list-style-type: none"> ● Both - Netbios messages are rebroadcasted both to and from this interface. ● Disable - Netbios messages are not rebroadcasted to or from this interface. <p>Note:</p> <p>This field is only available when additional parameters are selected. To select additional parameters, click  on the Routing Manager Application Toolbar.</p>
ICMP Redirect Status	<p>The status of ICMP Redirect service on the interface. Possible values are:</p> <ul style="list-style-type: none"> ● Enable - Redirect messages are sent if the router is forced to resend a packet through the same interface from which it is received. ● Disable - Redirect messages are not sent. <p>Note:</p> <p>This field is only available when additional parameters are selected. To select additional parameters, click  on the Routing Manager Application Toolbar.</p>
Broadcast Address	<p>Define the broadcast address value. Possible values are:</p> <ul style="list-style-type: none"> ● Zero Fill - defines the broadcast address as zero. For example, 192.92.0.0. ● One Fill - defines the broadcast address as one. For example, 192.92.255.255.
2 of 2	

You can create, modify, and delete IP interfaces. For more information on editing tables, see [“Editing tables” on page 170](#).

Note:

IP Address, **IP NetMask**, **Layer 2 Interface Name**, and **Status** must be defined before creating an IP interface.

Note:

The list of VLANs allocated in the system are displayed in the **Layer 2 Interface Name** field.

Note:

IP Address for unnumbered interfaces or for interfaces receiving their IP address from a DHCP server or IPCP session cannot be modified.

There are certain constraints when configuring static IP or unnumbered interfaces. After clicking **Apply** in the IP Interfaces window, the software checks your configuration and displays error messages if applicable. The following table lists the possible errors and their descriptions:

Table 58: Error Messages

Error Text	Description
The Reference Layer 2 interface cannot be used because it is configured with IP unnumbered interface.	Reference Layer 2 Interface points to an IP unnumbered interface.
There is already another IP unnumbered interface on the layer 2 interface.	Layer 2 interface is already configured as an IP unnumbered interface, and you attempt to configure Layer 2 interface with a static IP.
There is already another IP static interface on the layer 2 interface.	Layer 2 interface is already configured with a static IP, and you attempt to configure Layer 2 interface as an IP unnumbered interface.
The Reference Layer 2 Interface has no Valid IP address.	Reference Layer 2 interface is not configured, and you attempt to add an IP unnumbered interface.

Viewing the Dynamic IP Interfaces Table

This table allows the configuration of ICMP-redirect only. You cannot add or delete rows in the table.

To display the dynamic IP interfaces:

Select **IP Route > Dynamic IP Interfaces**.

Figure 70: Dynamic IP Interfaces table

	IP Interface Name	IP Address	IP Netmask	Layer 2 Interface Name	Type	Oper Status	Redirects
●	FastEthernet 10/2.0	0.0.0.0	255.255.255.255	FastEthernet 10/2	DHCP	<input type="checkbox"/>	<input checked="" type="checkbox"/>

The following parameters are displayed:

Table 59: Dynamic IP Interfaces table parameters

Field	Description
IP Interface Name	The name assigned to the selected IP interface.
IP Address	The IP address of this interface. This address is received from a remote peer during the PPP-IPCP session, or from a DHCP server using a DHCP client.
IP NetMask	The IP network mask of the attached net or subnet.
Layer 2 Interface name	The name of the Layer 2 interface with which this subnet is associated.
Type	The type of IP address assignment on the interface. Possible values are: <ul style="list-style-type: none"> ● DHCP - a dynamic IP interface created by activating the DHCP client on the interface and getting an IP address from the DHCP server. ● Negotiated - a dynamic IP interface created by activating PPP-IPCP on the interface and getting an IP address.
Oper Status	The operational status of the IP interface.
Redirects	The status of the ICMP Redirect service on the interface. Possible values are: <ul style="list-style-type: none"> ● Enable - Redirect messages are sent if the router is forced to resend a packet through the same interface from which it is received. ● Disable - Redirect messages are not sent.

Viewing the Routing Table

To display and update the Routing Table:

Select **IP Route > Routing Table**.

Static routes are displayed as read-only in the Routing Table. To configure or create static routes, see [“Viewing the Static Routing Table” on page 189](#).

Figure 71: Routing Table

	Destination	Netmask	Next Hop	Layer 2 Interface name	Protocol	Redistribute	Cost	Permanent	Status
●	0.0.0.0	0.0.0.0	149.49.78.1	FastEthernet 10/2	static	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	low
●	1.1.1.0	255.255.255.0	0.0.0.0	Vlan 1	local		1	<input type="checkbox"/>	high
●	2.2.2.0	255.255.255.0	0.0.0.0	Vlan 1	local		1	<input type="checkbox"/>	high
●	3.3.3.0	255.255.255.0	Null		static	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	low
●	149.49.78.0	255.255.255.0	0.0.0.0	FastEthernet 10/2	local		1	<input type="checkbox"/>	high

The following parameters are displayed:

Table 60: Routing Table parameters

Field	Description
Destination	The destination network IP address of this route. An IP address of 0.0.0.0 denotes a default router.
Netmask	The destination network mask of this route.
1 of 2	

Table 60: Routing Table parameters (continued)

Field	Description
Next Hop	<p>The address of the next router of this route, through which the destination of this route is reached.</p> <p>Note:</p> <p>If the static route is defined over the WAN Fast Ethernet interface configured as a DHCP client, then this field displays the IP address (DHCP), provided the DHCP client has a default route; otherwise, it displays the Unassigned (DHCP).</p>
Layer 2 Interface Name	The logical name of the local interface through which the next hop of this route is reached.
Protocol	<p>The protocol through which the route is learned. The following protocols can be specified:</p> <ul style="list-style-type: none"> • Static - The route is manually configured to this device. • Local - The route represents a directly attached net or subnet and corresponds to one of the IP interfaces configured to this device. • RIP - The entry is learned from the RIP protocol. • OSPF - The entry is learned from the OSPF protocol.
Redistribute	If selected, static entries are advertised by RIP and OSPF. If not selected, static entries are not advertised.
Cost	Number of hops to the destination network, or the cost of the route for OSPF routes.
Permanent	<p>The permanence status of the route. Possible statuses are:</p> <ul style="list-style-type: none"> • selected - The route is not disabled when a link on the route is down. • Cleared - The route is disabled when a link on the route is down.
Static Preference	<p>The preference of this route. Possible values are:</p> <ul style="list-style-type: none"> • Low - Dynamic routes are preferred on this static route. • High - This static route is preferred on dynamic routes.
Route Type	The type of route.
Route Age	The number of seconds since this route was last updated or otherwise determined to be correct.
2 of 2	

You can create, modify, or delete Routing Table static entries. For more information on editing tables, see [“Editing tables” on page 170](#).

You can limit the table entries displayed.

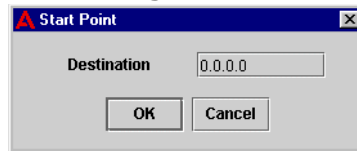
To start the display of entries from a specified interface and IP address:

1. Click .

Or

Select **Action > Start Point**. The system displays the Start Point dialog box.

Figure 72: Routing Table Start Point Dialog Box



2. Enter an IP address in the **Destination** field.
3. Click **OK**. The Routing Table displays entries starting with the specified IP address.

To view all the entries in the Routing Table:

Click .

Or

Select **View > Refresh**.

Viewing the Static Routing Table

To display and update the Static Routing Table:

Select **IP Route > Static Routing Table**. The system displays the Static Routing Table window.

Figure 73: Static Routing Table

Destination	Netmask	Next Hop	Layer 2 Interface name	Redistribute	Cost	Permanent	Static Preference	Route Type	Active
0.0.0.0	0.0.0.0	149.49.78.1	FastEthernet 10/2	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	low	Regular	Yes
58.0.0.0	255.255.255.0	149.49.78.18	FastEthernet 10/2	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	low	Regular	Yes
58.3.0.0	255.255.0.0	149.49.78.12	FastEthernet 10/2	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	low	Regular	Yes

The following parameters are displayed:

Table 61: Static Routing Table parameters

Field	Description
Destination	The destination network IP address of this route. An IP address of 0.0.0.0 denotes a default router.
1 of 2	

Table 61: Static Routing Table parameters (continued)

Field	Description
Netmask	The destination network mask of this route.
Next Hop	<p>The address of the next router of this route, through which the destination of this route is reached.</p> <p>Note: If the static route is over the WAN Fast Ethernet interface configured as a DHCP client, then this field displays the IP address (DHCP), provided the DHCP client has a default route; otherwise, it displays the Unassigned (DHCP).</p> <p>Note: You must specify Route Type before configuring Next Hop.</p>
Layer 2 Interface Name	<p>The logical name of the local interface through which the next hop of this route is reached.</p> <p>Note: You must specify Route Type before configuring Layer 2 Interface Name.</p>
Redistribute	If selected, static entries are advertised by RIP and OSPF. If not selected, static entries are not advertised.
Cost	Number of hops to the destination network, or the cost of the route for OSPF routes.
Permanent	<p>The permanence status of the route. Possible statuses are:</p> <ul style="list-style-type: none"> ● Selected - The route is not disabled when a link on the route is down. ● Cleared - The route is disabled when a link on the route is down.
Static Preference	<p>The preference of this route. Possible values are:</p> <ul style="list-style-type: none"> ● Low - Dynamic routes are preferred on this static route. ● High - This static route is preferred on dynamic routes.
Route Type	<p>The type of static route. Possible values are:</p> <ul style="list-style-type: none"> ● through - through the interface static route. ● Discard - using a route which discards traffic. ● DHCP - using the DHCP client next hop. ● Regular - the regular static route.
Active	<p>The status of the route. Possible values are:</p> <ul style="list-style-type: none"> ● Yes - the route is active and affects the traffic. ● No - the route is not active and does not affect the traffic.
2 of 2	

Note:

When editing an existing row, the following fields cannot be changed:

Destination, Netmask, Next Hop, Layer 2 Interface Name, and Static Preference. To change these fields, you must create a new row and change those fields as desired. After changing, delete the original row. All the other fields can be edited in an existing row.

When adding Static Routing Table entries on an Avaya G430 Device, you can configure the next hop method in the Form view. Available next hop methods include:

- **Next Hop** - Select the **Next Hop** option, and enter the IP address of the next hop.
- **Layer 2 Interface Name** - Select the **Layer 2 Interface Name** option, and select an interface from the field.
- **Discard** - Select the **Discard** option.

Viewing the ARP Table

To display and update the ARP Table parameters:

Select **IP Route > ARP Table**.

Figure 74: ARP Table window

	IP Address	MAC Address	Layer 2 Interface name	Status
●	135.27.162.1	00:04:96:18:F2:F0	Vlan 1	Dynamic
●	135.27.162.81	00:04:0D:4A:14:1B	Vlan 1	Dynamic
●	135.27.162.170	00:18:8B:84:50:8D	Vlan 1	Dynamic

The following parameters are displayed:

Table 62: ARP parameters

Field	Description
IP Address	The IP address of the station.
MAC Address	The MAC address of the station.
Layer 2 Interface name	The name of the interface.

Table 62: ARP parameters (continued)

Field	Description
Status	<p>The status of the interface. Possible status values are:</p> <ul style="list-style-type: none"> ● Dynamic - The entry is learned from the ARP protocol. If the station entry is not active for a pre-determined time, the entry is deleted from the table. ● Static - The entry has been configured by the network management station, and is permanent. ● Invalid - The entry in the table is invalid.

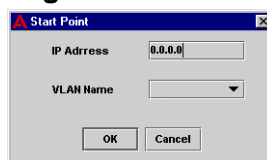
You can create or delete ARP table entries. For more information on editing tables, see [“Editing tables” on page 170](#).

You can limit the table entries displayed. To start the display of entries from a specified interface and IP address:

1. Click .

Or

Select **Action > Start Point**. The system displays the Start Point dialog box.

Figure 75: ARP Table Start Point dialog box

2. Enter an IP address in the **IP Address** field.
3. Select an interface from the **If Name** field.
4. Click **OK**. The ARP Table displays entries starting with the specified IP address and interface.

To view all the entries in the ARP Table:

Click .

Or

Select **View > Refresh**.

Configuring GRE tunneling

GRE tunneling is used to reserve a path between two specific IP addresses on a network, which enables you to reserve bandwidth, set security policy, or set Quality of Service parameters between the two configured devices.

To create or modify an IP tunnel:

Select **IP Route > GRE Tunnel**. The system displays the GRE Tunnel Table.

Figure 76: GRE Tunnel Table

Tunnel No...	Enca...	Local IP	Remote...	DSCP	Interface MT...	Path MTU Dis...	Tunnel MT...	Hop Li...	Verify Ch...	Key Mo...	Key	Aging Ti...	KeepAl...	KeepAl...
1 1	GRE	1.1.1.4	1.1.1.5	No Ch...	1476	<input checked="" type="checkbox"/>	0	255	<input type="checkbox"/>	<input type="checkbox"/>	0	Disable	255	0
2 2	GRE	0.0.0.0	0.0.0.0	No Ch...	0	<input checked="" type="checkbox"/>	0	255	<input type="checkbox"/>	<input type="checkbox"/>	0	Disable	3	10
3 3	GRE	0.0.0.0	0.0.0.0	No Ch...	0	<input checked="" type="checkbox"/>	0	255	<input type="checkbox"/>	<input type="checkbox"/>	0	Disable	3	10
4 4	GRE	0.0.0.0	0.0.0.0	No Ch...	0	<input checked="" type="checkbox"/>	0	255	<input type="checkbox"/>	<input type="checkbox"/>	0	10	3	10

The following parameters are displayed:

Table 63: GRE Tunnel parameters

Field	Description
Interface Name	Name of the Tunnel interface.
Tunnel No.	The index number of the Tunnel interface. Possible values: 1-50 Note: Tunnel numbers must be unique.
Encapsulation Method	The encapsulation method used for differentiating tunnel traffic from other traffic on a physical interface. Value is always GRE .
Local IP	The IP address of the local endpoint of the tunnel. Note: The local IP and remote IP must be different.
1 of 3	

Table 63: GRE Tunnel parameters (continued)

Field	Description
Remote IP	The IP address of the remote endpoint of the tunnel. Note: The local IP and remote IP must be different.
DSCP	The offset to the DSCP value in the encapsulation header, which is used to show the difference between encapsulated traffic and regular traffic on a physical interface. Possible values are: <ul style="list-style-type: none"> • No Change • An integer between 0 - 63
Interface MTU	The current Maximum Transmission Unit for the physical interface through which tunnel packets are sent. Note: This field is read-only.
Path MTU Discovery	When selected, the device actively polls the next hop device for MTU value.
Tunnel MTU	The Maximum Transmission Unit for the tunnel. Note: This field is read-only. Note: This field is only active when Path MTU Discovery is active.
Hop Limit	Maximum number of intervening devices between two endpoints of an IP tunnel.
Verify Checksum	When selected, the Avaya G430 Device verifies the checksum value in IP headers of packets traveling over the tunnel.
Key Mode	When selected, a shared key is used for encrypting traffic over an IP tunnel.
Key	The shared key for encrypting traffic over an IP tunnel.
Aging Timer	The number of minutes Path MTU Discovery is aged. Default: 10 . A value of 0 indicates Aging Timer is disabled. Note: Aging Timer can only be changed if Path MTU Discovery is set.
2 of 3	

Table 63: GRE Tunnel parameters (continued)

Field	Description
Keep Alive Retries	The number of Keep Alive requests sent before an interface becomes inactive. Default: 3 Note: Keep Alive Retries can only be changed if Keep Alive Rate is set.
Keep Alive Rate	The rate, in seconds, at which Keep Alive packets are sent. Default: 10 . A value of 0 indicates Keep Alive is disabled.
3 of 3	

You can create or delete GRE tunnel table entries. For more information on editing tables, see [“Editing tables” on page 170](#).

DHCP

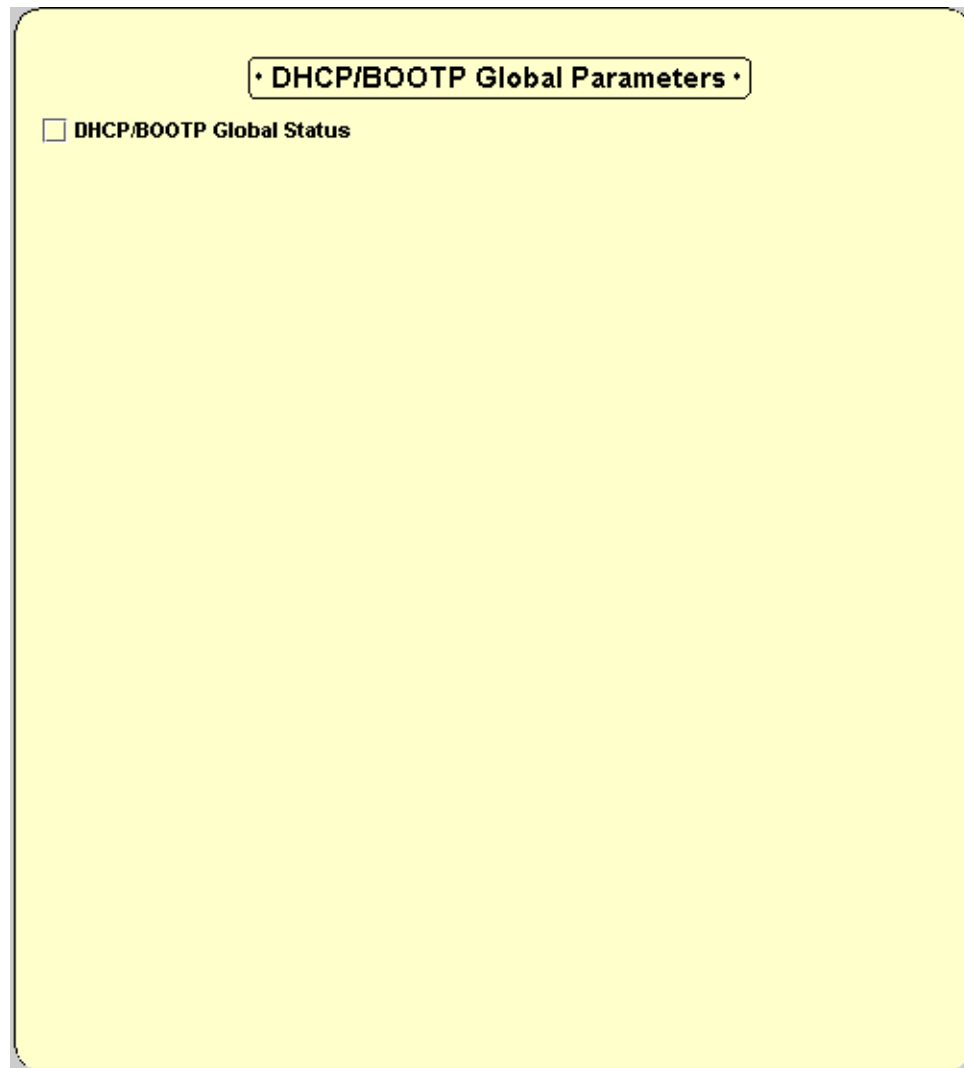
The **DHCP** folder provides access to the following windows:

- [Viewing DHCP/BOOTP Global Parameters](#)
- [Configuring the DHCP/BOOTP parameters](#)

Viewing DHCP/BOOTP Global Parameters

To display and update the DHCP/BOOTP global parameters:

Select **IP Route > DHCP > DHCP/BOOTP Global Parameters**.

Figure 77: DHCP/BOOTP Global Parameters window

The following parameter is displayed:

Table 64: DHCP/BOOTP Global Parameter

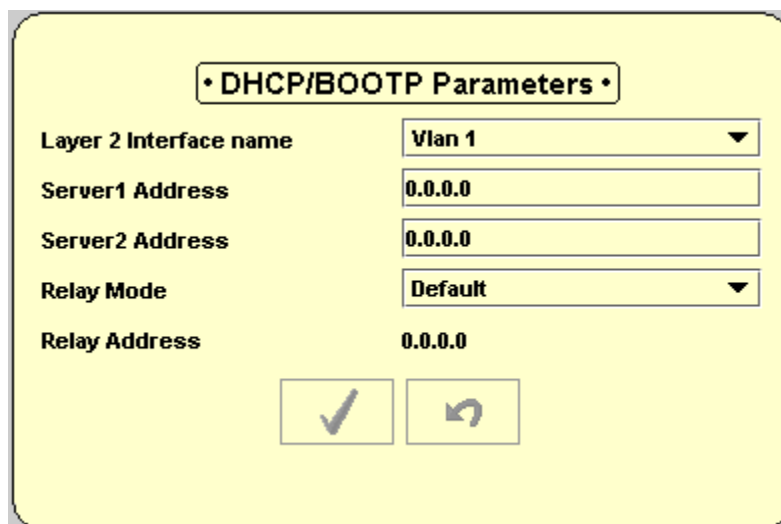
Field	Description
DHCP/BOOTP Global Status	If the DHCP/BOOTP Global Status check box is selected, DHCP/BOOTP is enabled according to the DHCP/BOOTP configuration of each interface. If it is not selected, DHCP/BOOTP relays over all the interfaces are disabled.

Configuring the DHCP/BOOTP parameters

To display and update the DHCP/BOOTP parameters:

Select **IP Route > DHCP > DHCP/BOOTP Parameters**.

Figure 78: DHCP/BOOTP Parameters window



The following parameters are displayed:

Table 65: DHCP/BOOTP Parameters

Field	Description
Layer 2 Interface name	The interface name upon which the clients are located.
Server1 Address	The IP address of the first of the two possible DHCP servers for the interface.
Server2 Address	The IP address of the second of the two possible DHCP servers for the interface.

Table 65: DHCP/BOOTP Parameters (continued)

Field	Description
Relay Mode	<p>The method by which the DHCP relay chooses an IP address to include in the DHCP request.</p> <p>When relaying a DHCP/BOOTP request, the relay has to write its own IP address into the relayed DHCP request. This address is used by the DHCP server to determine the subnet from which the client's IP address has been allocated. When the router has multiple IP addresses on the same VLAN, any of these addresses can be used when relaying DHCP requests.</p> <p>The Mode field controls the behavior of the DHCP relay in choosing the IP address to write into the DHCP request. Possible modes are:</p> <ul style="list-style-type: none"> • Default - The router chooses one of the addresses itself. The address chosen will be the lowest IP address on that VLAN. • Specific - The router is configured with a single IP address to be used with all the relayed requests arriving on the VLAN. This address must be one of the router's IP addresses on the specified VLAN. It must be entered in the Relay Address field.
Relay Address	One of the router's IP addresses on the VLAN. This is used for all relayed requests, if Mode is set to Specific .

Note:

The available values of **Layer 2 Interface Name** do not include the Layer 2 interface on which the dynamic IP addresses are defined.

You can create, modify, or delete DHCP/BOOTP parameters. For more information on editing tables, see [“Editing tables” on page 170](#).

RIP

The **RIP** folder provides access to the following windows:

- [Viewing RIP Global Parameters](#)
- [Configuring RIP Interfaces](#)

Viewing RIP Global Parameters

To display and update RIP global parameters:

Select **IP Route > RIP > RIP Global Parameters**.

Figure 79: RIP Global Parameters window

• RIP Global Parameters •

☐ **RIP Global Status**

☐ **Redistribute OSPF into RIP**

☐ **Redistribute Static into RIP**

Update interval (seconds)

Route invalidate timeout (seconds)

The following parameters are displayed:

Table 66: RIP Global Parameters

Field	Description
RIP Global Status	The status of RIP on the device. If selected, RIP is enabled. If this check box is not selected, RIP is disabled on all interfaces, regardless of the settings in the RIP Interfaces window.
Redistribute OSPF into RIP	Controls redistribution of routes from OSPF to RIP. If selected, all routes learned through OSPF are advertised into RIP.
Redistribute Static into RIP	Controls redistribution of static routes to RIP. If selected, the static routes inserted into the IP Routing Table are advertised into RIP, according to the "Leak Route" definition for each static route.
Update Interval (seconds)	The amount of time between each RIP periodic update.
Route invalidate timeout (seconds)	The amount of time after which a route becomes invalid in the routing table.

You can modify RIP Global Parameters by selecting the check boxes as desired.

Configuring RIP Interfaces

To define and display RIP interfaces:

Select **IP Route > RIP > RIP Interfaces**.

Figure 80: RIP Interfaces window

	IP Interface Name	IP Address	Reference IP Address	State	Status	RIP Version	Send Receive Mode	Cost
●	Vlan 22.4	22.21.4.1	N/A	Inactive	<input type="checkbox"/>	Rip1	talk-listen	1
●	Vlan 22.1	22.22.1.1	N/A	Inactive	<input type="checkbox"/>	Rip1	talk-listen	1
●	Vlan 3.0	33.1.1.1	N/A	Inactive	<input type="checkbox"/>	Rip1	talk-listen	1
●	Vlan 3.5	33.5.1.1	N/A	Inactive	<input type="checkbox"/>	Rip1	talk-listen	1
●	FastEthernet 10/2	149.49.78.138	N/A	Inactive	<input type="checkbox"/>	Rip1	talk-listen	1

The following parameters are displayed:

Table 67: RIP Interface Parameters

Field	Description
Interface Name	The name assigned to the selected IP interface.
IP Address	The IP address of the interface. If the IP address is unnumbered, this field returns a value of N/A .
Reference IP Address	The IP address borrowed for an unnumbered interface. A value of 0.0.0.0 indicates either that the IP address is not valid, or that the IP interface is borrowing the IP address from a dynamic IP interface whose IP address is not allocated yet. If the IP address is numbered, this field returns a value of N/A .
State	The operational status of the RIP interface. Possible statuses are active and inactive.
Status	The administrative status of the RIP interface. If selected, the RIP interface status is enabled. If this check box is not selected, it is disabled.
RIP Version	The router can be configured to operate either RIP version 1 or RIP version 2 on each IP interface. The configuration of the RIP version must be consistent on each subnet. That is, all routers should be configured with the same RIP version on their interface to the subnet. When possible, homogeneous configuration of the RIP version in the network is recommended. <ul style="list-style-type: none"> ● Rip1 - The router runs regular RIP on that interface, following the RIP version 1 subnet aggregation rules. That is, it advertises an aggregate route for the net as opposed to advertising subnet routes across the network boundary. ● Rip2 - The router runs RIP version 2 on that interface. RIP version 2 advertisements are sent as multicast rather than broadcast. No route aggregation is done in RIP version 2. RIP version 2 allows for Variable Length Subnets Masks (VLSM), meaning that subnets of the same net may have masks of different lengths, and may be of different sizes.
1 of 2	

Table 67: RIP Interface Parameters (continued)

Field	Description
Send Receive Mode	What the device sends on this interface. Values are: <ul style="list-style-type: none"> • Talk-listen - RIP updates contain the entire routing table. • Talkdefault-listen - RIP updates contain only a single entry. This advertises the router as the default router. • Listen-only - No RIP updates are sent.
Cost	The cost of using this interface. RIP chooses the route with the lowest total cost (metric) for each destination.
Default Route Metric	The metric of the default route entry in RIP updates originates on this interface, if configured to SendDefaultOnly .
Default Route Mode	The default route mode. Possible values are: Talk-listen : accepts default route entries in RIP messages received from other routes on this interface. Talk-only : does not accept default route entries in RIP messages received from other routes on this interface.
Split Horizon	The methods for handling routes from this interface when sending updates to this interface. Possible methods are: <ul style="list-style-type: none"> • Poisoned Reverse - The routes are advertised to this interface as unreachable. • Split Horizon - The routes are not advertised to this interface at all. • None - The routes are advertised to this interface as is.
Auth Type	Authentication Type. Possible methods are: <ul style="list-style-type: none"> • None • Simple
Auth Key	The password for this interface. This is only used if the Auth Type is set to Simple-password . The password may contain up to 16 characters. It may be configured here, but not viewed.
2 of 2	

Note:

If you select the **listen-only** or **talk-listen** mode, you can not update the **Default Route Metric** field.

You can modify RIP interfaces. For more information on editing tables, see [“Editing tables” on page 170](#).

OSPF

The **OSPF** folder provides access to the following windows:

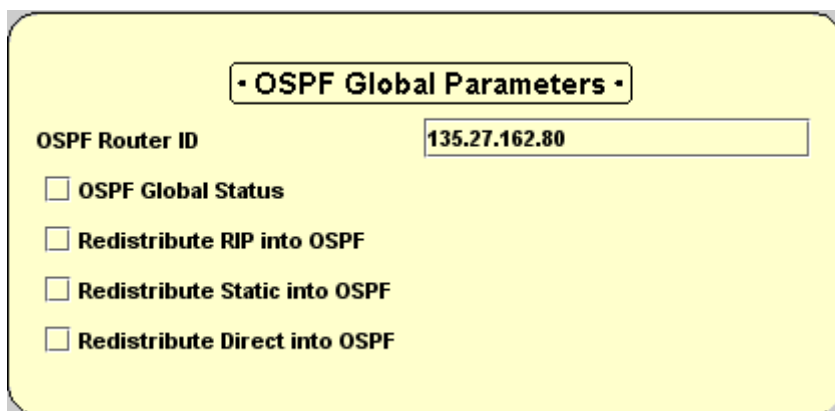
- [Viewing OSPF Global Parameters](#)
- [Configuring OSPF Interfaces](#)
- [Configuring OSPF Area Parameters](#)
- [Viewing the OSPF Link State Database](#)
- [Viewing the OSPF External Database](#)
- [Viewing OSPF Neighbors](#)

Viewing OSPF Global Parameters

To define and display OSPF Global parameters:

Select **IP Route > OSPF > OSPF Global Parameters**.

Figure 81: OSPF Global Parameters window



The following parameters are displayed:

Table 68: OSPF Global Parameters

Field	Description
OSPF Router ID	The ID number of the router. The router ID must be unique. By default, the router ID equals one of the router's IP addresses.
1 of 2	

Table 68: OSPF Global Parameters (continued)

Field	Description
OSPF Global Status	The administrative status of OSPF in the router. If not selected, OSPF is not active on any interface, regardless of the settings in the OSPF Interfaces window.
Redistribute RIP into OSPF	Controls redistribution of routes from RIP to OSPF. If selected, all routes learned through RIP are advertised into OSPF as external routes.
Redistribute Static into OSPF	Controls redistribution of static routes into OSPF. If selected, routes are advertised into OSPF as external routes, according to the "Leak Route" definition for each static route.
Redistribute Direct into OSPF	Controls redistribution of direct routes which are external to OSPF. If selected, local subnets on which OSPF is disabled are advertised into OSPF as external routes.
2 of 2	

You can modify OSPF Global Parameters.

Note:

After updating the **Router ID** field, the system displays a warning message which says that the operation might cause the OSPF database to reset.

Configuring OSPF Interfaces

To define and display OSPF interfaces:

Select **IP Route > OSPF > OSPF Interfaces**.

Figure 82: OSPF Interfaces Window

IP Interface Name	IP Address	Reference IP Address	Type	State	Status	Designated Router	Backup Designated Router
› Vlan 22.4	22.21.4.1	N/A	broadcast	down	<input type="checkbox"/>	0.0.0.0	0.0.0.0
› Vlan 22.1	22.22.1.1	N/A	broadcast	down	<input type="checkbox"/>	0.0.0.0	0.0.0.0
› Vlan 3.0	33.1.1.1	N/A	broadcast	down	<input type="checkbox"/>	0.0.0.0	0.0.0.0
› Vlan 3.5	33.5.1.1	N/A	broadcast	down	<input type="checkbox"/>	0.0.0.0	0.0.0.0
› FastEthernet 10/2	149.49.78.138	N/A	broadcast	down	<input type="checkbox"/>	0.0.0.0	0.0.0.0

The following parameters are displayed:

Table 69: OSPF Interfaces

Field	Description
IP Interface Name	The name assigned to the selected IP interface.
IP Address	The IP address of this OSPF interface. For an unnumbered IP interface, this field returns a value of N/A .
Reference IP Address	The IP address borrowed for an unnumbered interface. A value of 0.0.0.0 indicates either that the IP address is not valid, or that the IP interface is borrowing the IP address from a dynamic IP interface whose IP address is not yet allocated. If the IP address is unnumbered, this field returns a value of N/A .
Type	The type of interface. Possible values are: <ul style="list-style-type: none"> ● Point To Point ● Point To Multipoint ● Broadcast
State	The interface state of the OSPF interface: <ul style="list-style-type: none"> ● Down - OSPF is not active on the interface. ● Waiting - The identity of the designated router for this subnet is not yet determined. ● Designated Router - This router is the Designated Router on this subnet. ● Backup Designated Router - This router is the Backup Designated Router. ● Other Designated Router - Another router is the Designated Router on this subnet.
Status	If selected, this denotes that the interface may form neighbor relationships, and that the interface is advertised as an internal route to OSPF. If this is not selected, the interface is external to OSPF.
Designated Router	The IP Address of the designated router.
Backup Designated Router	The IP Address of the backup designated router.
Priority	The priority of this router to become the designated router on this interface. A value of zero indicates that this router is not eligible to become the designated router on the current network. If more than one router has the same priority, then the router ID is used.
Cost	The cost of using this interface. OSPF chooses the route with the lowest total cost (metric) for each destination.
Hello Interval	The period of time (in seconds) between Hello packets. All routers attached to a common network must have the same Hello Interval.
1 of 2	

Table 69: OSPF Interfaces (continued)

Field	Description
Dead Interval	The period of time (in seconds) that a router's Hello packets have not been seen before the router's neighbors declare the router down. All routers attached to a common network must have the same Dead interval.
Auth Type	Authentication Type. Possible methods are: <ul style="list-style-type: none"> • None • Simple-password • MD5 - Auth Type cannot be set to MD5 from the Avaya G430 Manager. If MD5 authentication is configured from the CLI, you can view the existing Auth Type, or change Auth Type to None or Simple-password.
Auth Key	The password for this interface. This is used only if the Auth Type is set to Simple-password . The password may contain up to 8 characters. It can be configured here, but not viewed.
2 of 2	

You can modify OSPF interfaces. For more information on editing tables, see ["Editing tables" on page 170](#).

Configuring OSPF Area Parameters

To define and display OSPF Area Parameters:

Select **IP Route > OSPF > OSPF Area Parameters**.

Figure 83: OSPF Area Parameters window

• OSPF Area Parameters •	
Area ID	0.0.0.0
Stub Area	no
Area Border Routers Count	0
AS Border Routers Count	0
Area LSAs count	0
Area LS Checksum Summary	0

The following parameters are displayed:

Table 70: OSPF Area Parameters

Field	Description
Area ID	A unique number identifying the OSPF area to which this router belongs. Area ID 0.0.0.0 is used for the OSPF backbone.
Stub Area	If selected, external link-state advertisements are not imported into the area.
Area Border Routers Count	The number of routers designated as OSPF Area Border Routers for the area chosen.
AS Border Routers Count	The number of routers designated as OSPF Autonomous System Border Routers for the area chosen.
Area LSAs Count	The number of Link-State Advertisements for the area chosen.
Area LS Checksum Summary	Summary of the Link-State Checksums for the area chosen.

You can modify OSPF Area parameters.

Viewing the OSPF Link State Database

To display the OSPF Link State Database:

Select **IP Route > OSPF > OSPF Link State Database**.

Figure 84: OSPF Link State Database window

SA Type	LSA ID	Router ID	Sequence No.	LSA Age	Checksum
Link	1.1.1.1	1.1.1.1	0x800002D0	1126	0x93F3

The following parameters are displayed:

Table 71: OSPF Link State Database window

Field	Description
LSA Type	The type and format of the Link-State advertisement; for example, Router links and Network links.
LSA ID	Identifies the part of the routing domain that is described by the advertisement. The LSA ID can either be a router ID or an IP address.
Router ID	Identifies the originating router in the autonomous system.
1 of 2	

Table 71: OSPF Link State Database window (continued)

Field	Description
Sequence No.	The sequence number of the Link-State advertisement. Use this parameter to detect old and duplicate Link-State advertisements. The larger the sequence number, the more recent the advertisement. Note that the sequence number is usually negative.
LSA Age	The age of the Link-State advertisement (in seconds).
Checksum	This parameter is a checksum of the complete contents of the advertisement, not including the Age value.
2 of 2	

The parameters in the OSPF Link State Database window are read-only.

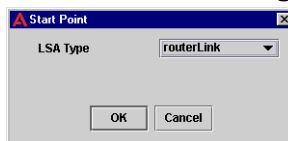
You can limit the table entries displayed. To start the display of entries from a specified interface and IP address:

1. Click .

Or

Select **Action > Start Point**. The system displays the Start Point dialog box.

Figure 85: OSPF Link State Database Start Point Dialog Box



2. Select an LSA Type from the **LSA Type** field.
3. Click Start. The OSPF Link State Database displays entries starting with the specified LSA Type.

To view all the entries in the OSPF Link State Database:

- Click .

Or

Select **View > Refresh**.

Viewing the OSPF External Database

To display the OSPF External Database window:

Select **IP Route > OSPF > OSPF External Database**.

Figure 86: OSPF External Database window

	LSA Type	LSA ID	Router ID	Sequence No.	LSA Age	Checksum
--	----------	--------	-----------	--------------	---------	----------

The following parameters are displayed:

Table 72: OSPF External Database Window

Field	Description
LSA Type	The type and format of the Link-State advertisement; for example, Router links and Network links.
LSA ID	Identifies the part of the routing domain that is described by the advertisement. The LSA ID can be either a router ID or an IP address.
Router ID	Identifies the originating router in the autonomous system.
Sequence No.	The sequence number of the Link-State advertisement. Use this parameter to detect old and duplicate Link-State advertisements. The larger the sequence number, the more recent the advertisement. Note that the sequence number is usually negative.
LSA Age	The age of the Link-State advertisement (in seconds).
Checksum	This parameter is a checksum of the complete contents of the advertisement, not including the Age value.

The parameters in the OSPF External Database window are read-only.

Viewing OSPF Neighbors

To display the OSPF Neighbors window:

Select **IP Route > OSPF > OSPF Neighbors**.

Figure 87: OSPF Neighbors window

Neighbor Address	Router ID	Neighbor State

The following parameters are displayed:

Table 73: OSPF Neighbors Parameters

Field	Description
Neighbor Address	The IP address of this neighbor.
Router ID	The unique OSPF identifier for the neighboring router.
Neighbor State	The state of relationship with this neighbor: <ul style="list-style-type: none"> • Down • Attempt • Init • Two Way • Exchange Start • Exchange • Loading • Full
Priority	The priority of the path between the router and its neighbor for determining path calculations.
Retransmit QLength	The size of the queue for retransmission packets.

The parameters in the OSPF Neighbors Table window are read-only.

VRRP

The **VRRP** folder provides access to the following windows:

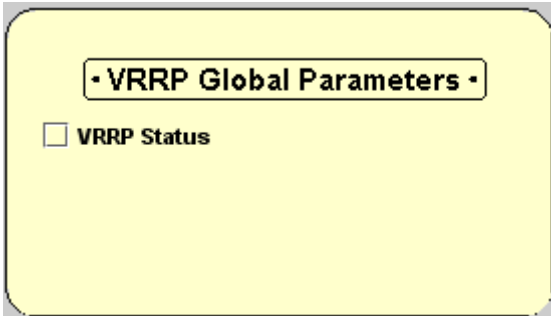
- [Viewing VRRP Global Parameters](#)
- [Viewing the VRRP Table](#)

Viewing VRRP Global Parameters

VRRP (Virtual Router Redundancy Protocol) provides a method for configuring a redundancy between routers. A Master Router is selected for each Virtual Router. Backup routers function normally, while checking the Master Router. If the Master Router fails, the backup routers handle traffic directed to the Master Router.

To define and display the VRRP global parameters:
Select **IP Route > VRRP > VRRP Global Parameters**.

Figure 88: VRRP Global Parameter window



The following parameter is displayed:

Table 74: VRRP Global Parameter

Field	Description
VRRP Status	When the VRRP global parameter check box is selected, VRRP is operational on the router. If the check box is not selected, VRRP is not operational on the router.

You can modify the VRRP Global Parameter.

Viewing the VRRP Table

To define and display the VRRP table:
Select **IP Route > VRRP > VRRP Table**.

Figure 89: VRRP Table

Layer 2 In	VRID	IP Address	State	Master IP	Priority	Virtual Route	Advertise Inter	MAC A	Primary I	Pr
------------	------	------------	-------	-----------	----------	---------------	-----------------	-------	-----------	----

The following parameters are displayed:


Table 75: VRRP Table Parameters

Field	Description
Layer 2 Interface Name	The name of the selected interface.
1 of 2	

Table 75: VRRP Table Parameters (continued)


Field	Description
VRID	A number which, along with an interface index (ifIndex), serves to uniquely identify a virtual router on a given VRRP router. A set of one or more associated addresses is assigned to a VRID.
IP Address	The IP address associated with this virtual router. If more than one IP address is associated with this virtual router, Click for Details appears in the IP Address field. Clicking the field opens the Form view showing all IP addresses associated with this virtual router. The IP addresses must be on a local subnet on the VLAN.
State	The state of the virtual router. Possible states are: <ul style="list-style-type: none"> ● Initialize - The virtual router is not functional. ● Backup - The virtual router is monitoring the availability of the master router. ● Master - The virtual router is forwarding packets with IP addresses associated with this virtual router.
Master IP Address	The IP address of the physical router currently acting as the Virtual Router's Master Router.
Priority	This object specifies the priority to be used for the virtual router master election process. Higher values imply higher priority. A priority of '0', although not settable, is sent by the master router to indicate that this router has ceased to participate in VRRP and a backup virtual router should transition to become a new master. A priority of 255 is used for the router that owns the associated IP address(es).
Virtual Route Up Time	The time when the virtual router's state changes from initialized to backup or master . The time is expressed in ticks (1/60 of a second).
Advertise Interval	The interval of state advertisements from the primary interface to the backup interface.
MAC Address	MAC address of the VRRP interface.
Primary Interface	Logical name of the primary interface.
Preempt Mode	If Preempt is set, the interface becomes primary whenever it is active.
Auth Type	Authentication Type. Possible methods are: <ul style="list-style-type: none"> ● None ● Simple
Auth Key	The password for this interface. This is only used if the Auth Type is set to Simple-password . The password may contain up to 8 characters. It can be configured here, but not viewed.
2 of 2	

To associate IP addresses with a selected virtual router:

1. Select a virtual router in the VRRP table.
2. Ensure that the Form view is visible.
3. Enter the IP address to associate with the selected router in the textbox under the **IP Addresses** field in the Form view.
4. Click .

The IP address is associated with the virtual router.

To disassociate IP addresses from a selected virtual router:

1. Select a virtual router in the VRRP table.
2. Ensure that the Form view is visible.
3. Select the IP address from the **IP Addresses** field in the Form view.
4. Click . The IP address is no longer associated with the virtual router.

You can modify VRRP parameters. For more information on editing tables, see [“Editing tables” on page 170](#).

Header Compression

The **Header Compression** folder provides access to the following windows:

- [Configuring cRTP Interfaces](#)
- [Configuring TCP Header Compression Interfaces](#)

Note:

All header compression methods apply to point-to-point interfaces only.

Configuring cRTP Interfaces

The Avaya G430 Device supports RTP compression. You can configure cRTP (Compressed RTP) parameters for each PPP interface.

To define and display CRTP Interfaces:

Select **IP Route > Header Compression> cRTP Interfaces**.

Figure 90: cRTP Interfaces window

Interface name	RTP Header Compression	Format	Max RTP ...	Actual RTP c...	Min Port	Max Port	Max Period	Max Time	Compressio
	<input type="checkbox"/>	N/A	16	0	2048	65535	256	5	0

The following parameters are displayed:

Table 76: cRTP Interface Table parameters

Field	Description
Layer 2 Interface Name	The name of the selected interface.
RTP Header Compression	The status of the RTP header compression on this interface. Possible values are: <ul style="list-style-type: none"> ● Enabled - RTP header compression is enabled on the interface. ● Disabled - RTP header compression is disabled on the interface.
Format	The IP header compression format. Possible values are: <ul style="list-style-type: none"> ● IPHC - header compression is active. ● N/A - header compression is not active.
Max RTP Connection	The maximum number of context identifiers for RTP connections on this interface. 0 implies that no RTP headers are compressed.
Actual RTP Connections	The actual number of context identifiers for RTP connections on this interface.
Min Port	The minimal UDP destination port number to be considered as RTP traffic.
Max Port	The maximal UDP destination port number to be considered as RTP traffic.
Max Period	The maximum number of compressed packets that can be sent between full headers.
Max Time	The maximum number of seconds between full headers.
Compression Ratio	The average ratio between the compressed header size and the original header size on this interface. This value is expressed as a percentage.
Mode	Whether RTP Header compression is compliant with IETF or Non-IETF format. This field is relevant for Frame Relay interfaces only. For other interfaces this field returns a value of N/A .

You can modify cRTP parameters on PPP interfaces. For more information on editing tables, see [“Editing tables” on page 170](#).

Configuring TCP Header Compression Interfaces

The Avaya G430 Device supports TCP header compression, enabling compression of all TCP traffic. You can configure TCP header compression parameters for each PPP interface.

To define and display TCP header compression Interfaces:

Select **IP Route > Header Compression> TCP Header Compression Interfaces**.

Figure 91: TCP Header Compression Interfaces window

	Layer 2 Interface name	TCP Header Compression	Format	Max TCP ...	Actual TCP ...	Compression Ratio
●	Dialer 1	<input type="checkbox"/>	N/A	16	0	0

The following parameters are displayed:

Table 77: TCP Header Compression Interfaces Table parameters

Field	Description
Layer 2 Interface Name	The name of the selected interface.
TCP Header Compression	The status of the TCP header compression on this interface. Possible statuses include: <ul style="list-style-type: none"> ● Enabled - TCP header compression is enabled on the interface. ● Disabled - TCP header compression is disabled on the interface.
Format	The header compression format. Possible values are: <ul style="list-style-type: none"> ● IPHC - IP header compression ● VJ - Van Jacobson compression
Max TCP Connection	The maximum number of context identifiers for TCP connections on this interface. 0 implies that no TCP headers are compressed.
Actual TCP Connections	The actual number of context identifiers for TCP connections on this interface.
Compression Ratio	The average ratio between the compressed header size and the original header size on this interface. This value is expressed as a percentage.

For PPP and Frame Relay interfaces, available header compression values are as follows:

Table 78: Available Compression Values for PPP and Frame Relay Interfaces

Interface Type	Available Compression Values
PPP	<ul style="list-style-type: none">● IPHC - TCP/RTP/UDP headers, or● VJ - TCP headers only
Frame Relay (IETF)	<ul style="list-style-type: none">● IPHC - TCP/RTP/UDP headers
Frame Relay (Non-IETF)	<ul style="list-style-type: none">● IPHC - RTP headers only, and/or● VJ - TCP headers only

Chapter 19: Policy Based Routing

This chapter describes the Policy Based Routing function in the Avaya G430 Manager and how to use it to add, modify, and delete policies and rules. It includes the following sections:

- [Policy Based Routing overview](#) - An overview of the different views in Avaya G430 Policy Based Routing.
- [Using the Tree view](#) - A detailed description of the Tree view including information on navigation between the different levels of the tree.
- [Using the Table view](#) - A detailed description of the Table view including a description of the table fields, instructions on adding, modifying, and deleting policies and rules, and a description of the different tabs and options.
- [Using Address Wildcards](#) - A description of address wildcards, and instructions on how to use them in Avaya G430 Policy Based Routing.
- [Using the IP Simulate function](#) - A description of the IP Simulate function, and instructions on activating and using the IP Simulate function to simulate the effect of rules on information packets.

Policy Based Routing overview

Policy Based Routing allows implementation of routing policies that selectively cause packets to take different paths. For example, in cases where the Avaya G430 Device has two WAN interfaces - Serial and xDSL - you can specify which voice packets be sent over the Serial link, and data packets over xDSL. Thus, it is only the voice packets which require high QoS that are sent over the more expensive Serial link.

The Avaya Policy Based Routing has two main views. These views provide you with information about the network, and enable you to manage policies and rules.

The Avaya Policy Based Routing's two main views are:

- **The Tree view** - Provides a hierarchical view of the device types in the network, the IP addresses of the devices in the network, the modules in the devices, and the existing policies. See ["Using the Tree view" on page 220](#).
- **The Table view** - Provides information about the contents of the elements in the Tree view. You can add, modify, and delete policies, composite actions, and rules in the Table view. See ["Using the Table view" on page 220](#).

Using the Tree view

This section provides an explanation of the Tree view hierarchy and how to use it.

You can select between the following Tree views using the Option buttons at the bottom of the Tree view:

- **Inventory** - Displays all the policy lists associated with each device, whether the lists are active or not.
- **Active Policies** - Displays only the active policy lists associated with each device.

The levels in the Tree view are:

- **Device** - IP addresses of devices. When a device is selected, the Policy Enforcement Points and Policy List tabs appear in the Table view.
- **Lists** - When a list is selected in the Tree view, the Policy Based Routing Rules (for Policy Based Routing lists), Next Hop (for Next Hop lists) and Configuration (for both types of lists) tabs appear in the Table view. The list name appears in the tree with the list ID in parentheses.

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

Double-click the element you want to expand or contract.

Or

Click the handle next to the element.

Using the Table view

The Table view provides the following tables on individual tabs, depending on the entity selected in the Tree view:

- [Policy Based Routing list](#) - Appears on a tab labeled Policy Lists.
- [Policy Based Routing Rules list](#) - Appears on a tab labeled Policy Based Routing.
- [Policy Enforcement Points](#) - Appears on a tab labeled Policy Enforcement Points.
- [Next Hop list](#) - Appears on a tab labeled Next Hop.
- [Configuration](#) - Appears on a tab labeled Configuration.



Policy Based Routing list

The Policy list provides a list of policies created for a selected module, and displays information about each of the policies. This section provides a description of the Policy list, and discusses the following topics:

- [Adding Policies](#)
- [Deleting Policies](#)




To view a Policy list, select a module in the Tree view. The system displays the Table view of the module's Policy list.

Figure 92: Policy list

Name	Type	Active	Validity
Shirish NH1	NHL	<input checked="" type="checkbox"/>	
Default PBR List	PBR	<input type="checkbox"/>	
Shirish	PBR	<input type="checkbox"/>	
Shirish_K	PBR	<input type="checkbox"/>	

The following table lists the fields in the Policy list and their descriptions:

Table 79: Policy list fields

Field	Description
Name	The user-defined policy name. The user-defined name appears in the Tree view as the policy name. You can change the policy name by clicking the table cell and typing the new name.
Type	The type of list. Possible values are: <ul style="list-style-type: none"> • PBR • NH
Active	Whether the policy is active or not on the module. Possible statuses include: <ul style="list-style-type: none"> • Active - The policy is currently active. • Not Active - The policy is not currently active.
Validity	The status of the policy. Possible statuses are: <ul style="list-style-type: none"> •  Valid - The policy is valid and can be used as the active policy. •  Partially Valid - Some of the policy rules which comprise this list are invalid. However, the policy can still be activated on the module. •  Invalid - At least one mandatory rule in the policy is not valid. An invalid policy cannot be made active on a module.


Adding Policies

To add a policy:

1. Click .

Or

Select **File > New List** and choose a list type. The system displays a new policy in the policy list.

2. Define the user defined fields in the Policy List. For more information on Policy fields, see [“Policy Based Routing list” on page 221](#).
3. Click . The module is updated with the new policy, and the table is refreshed.
4. Add rules to the new policy. For more information on adding rules, see [“Adding rules” on page 226](#).

Note:




Commit changes to the module to ensure that all the changes are permanently saved.

Deleting Policies

To delete a policy:

1. Select the policy you want to delete.

To select more than one policy, press **Shift** while selecting additional policies.

2. Click . An  appears next to the policy.
3. Click . The policy is deleted from the module, and the Table view is refreshed.

Note:

Commit changes to the module to ensure that all the changes are permanently saved.

Note:

You cannot delete the active policy.

Policy Based Routing Rules list

The Policy Based Routing Rules list allows you to add, modify, move, and delete rules in a policy. Since rules are applied to packets in the order they appear in the table, the order of rules in the table is important. This section provides a description of the Rules list, and discusses the following topics:

- [Adding rules](#)

- [Modifying rules](#)
- [Copying rules](#)
- [Moving rules](#)
- [Deleting rules](#)

To view the Rules list, select the policy in the Tree view whose rules you wish to view, and then select the **Policy Based Routing Rules** tab in the Table view. If the Rules list is not in the active policy, the Rules list opens in the Table view.

If the selected Policy Based Routing Rules list is in the active policy, the Policy Based Routing Rules list appears as read-only. To edit an active Rules list, activate a different policy on that interface and direction, and deactivate the policy with the Rules list you wish to edit.

Figure 93: Policy Based Routing Rules list

d	Description	Not	Src IP Address	Src Wildcard	Not	Dst IP Address	Dst Wildcard	Fragment	Not	Protocol	Not	DSCP Filter	No
..		<input type="checkbox"/>	0.0.0.0	any	<input type="checkbox"/>	0.0.0.0	any	<input type="checkbox"/>	<input type="checkbox"/>	IP	<input type="checkbox"/>	any	<input type="checkbox"/>

The following table lists the fields in the Rules list and their descriptions:





Table 80: Policy Based Routing Rules list fields

Field	Description
ID	Index number of the rule in the Policy Based Routing Rules List.
Description	Description of the rule. You cannot configure this field for default rules.
Not	Logical not. The rule is disabled and bypassed.
Src IP Address	Source Address. The source address of the packet matched by this rule.
Src Wildcard	Source Address Wildcard. A wildcard that can modify the definition of the specified source address. You can change the Source Address Wildcard using the field or by entering a user defined wildcard. Possible SrcAddWild values include: <ul style="list-style-type: none"> • Host • Any • User Defined For more information about using wildcards, see “Using Address Wildcards” on page 234 .
Not	Logical not. This enables all addresses except for the address listed in the Dst IP Address field.
Dst IP Address	Destination Address. The destination address of the packets matched by this rule.
1 of 3	

Table 80: Policy Based Routing Rules list fields (continued)

Field	Description
Dst Wildcard	<p>Destination Address Wildcard. A wildcard that can modify the definition of the destination address to which this rule applies.</p> <p>You can change the Destination Address Wildcard using the field or by entering a user defined wildcard. Possible DestAddrWild values include:</p> <ul style="list-style-type: none"> • Host • Any • User Defined <p>For more information about using wildcards, see “Using Address Wildcards” on page 234.</p>
Fragment	<p>When enabled, the IP rule applies only to packets that are non-initial fragments, and does not apply to initial fragments or non-fragments.</p> <p>When enabled, the Src Application and Dst Application fields return a value of N/A.</p>
Not	Logical not. This enables all protocols except for the protocol listed in the following Protocol field.
Protocol	<p>Protocol. The protocol of the packets to which this rule applies. Possible values include:</p> <ul style="list-style-type: none"> • AH • ESP • GRE • ICMP • IGMP • IPComp • IP-in-IP • OSPF • PIM • RSVP • SpectraLink • TCP • UDP • VRRP • IP
Not	Logical not. This enables all the traffic except the traffic affected by the following DSCP filter, to flow normally.
DSCP Filter	DSCP Filter. The DSCP filter applied to the traffic to which this rule applies.
Not	Logical not. This enables all applications except for the application listed in the following Src Application field.
2 of 3	

Table 80: Policy Based Routing Rules list fields (continued)

Field	Description
Src Application	Source Application. The source application protocol of the packets to which this rule applies. Select an application from the field. Note: Specifying a source application disables the Fragment check box.
Not	Logical not. This enables all applications except for the application listed in the following Dst Application field.
Dst Application	Destination Application. The destination application protocol of the packets to which this rule applies. Select an application from the field. Note: Specifying a destination application disables the Fragment check box.
Not	Logical not. This enables all ICMP codes and types except for the ICMP codes and types listed in the following ICMP code/type field.
ICMP code/type	ICMP code or type. Relevant when ICMP protocol is selected in the Protocol field.
Next-Hop	The policy to apply to the packet - either a specified Next-Hop list or Destination Based Routing. Possible values are: <ul style="list-style-type: none"> ● NH1 - Next-Hop list 1 ● NH2 - Next-Hop list 2 ● ● NH20 - Next-Hop list 20 ● DBR - Destination Based Routing
Validity	The validity of the rule. Possible values are: <ul style="list-style-type: none"> ●  Applicable - The rule is valid and can be applied to packets. ●  Best Effort - The rule may or may not be applied to packets. ●  Not Applicable - The rule contains invalid values or it conflicts with other rules. ●  Unknown - The rule status is unknown. The rule status is unknown if changes have been made but not applied.
3 of 3	


Adding rules

To add a new rule to a policy:

1. Click .

Or

Select **Edit > Add**. The new rule appears in the Rules List.


2. Define the fields in the table cells. For more information on the Rules fields see [“Policy Based Routing Rules list” on page 222](#).
3. Click . The policy is updated with the added rule, and the Table view is refreshed.

Note:

A mandatory, but invalid rule is highlighted in red.

Modifying rules

To modify a rule:

1. Click the rule you want to modify.
2. Define the fields in the table cells. For more information on the Rules fields see [“Policy Based Routing Rules list” on page 222](#).
3. Click .


Note:

Modifying a rule may invalidate other rules.

Copying rules

You can copy a rule to a different position in the Rules List or to a different policy.

To copy a rule:

1. Select the rule from the Rules List.
To select more than one rule, press **Shift** while selecting additional rules.
2. Select **Edit > Copy**. The selected rule is buffered to the clipboard.
3. If you want to copy the rule to a different policy, select the policy to which you want to paste the copied rule.
4. Select the rule above which you want to paste the copied rule.
5. Select **Edit > Paste**. The rule is pasted above the selected rule.
6. Click . The policy is updated with the copied rule, and the Table view is refreshed.


Note:

If no rule is selected, the copied rule is added to the bottom of the table.

Moving rules

You can move a rule's position in a policy or move it from one policy to another.

To move a rule:




1. Select a rule from the Rules List.
To select more than one rule, press **Shift** while selecting additional rules.
2. Select **Edit > Cut**. The selected rule is buffered on the clipboard.
3. To copy the rule to a different policy, select the policy to which you want to paste the copied rule.
4. Select the rule above which you want to move the rule.
5. Select **Edit > Paste**. The rule is inserted into the policy above the highlighted rule.
6. Click .

Note:

If no rule is selected, the copied rule is added to the bottom of the table.

Deleting rules

To delete a rule:

1. Select a rule from the Rules List.
To select more than one rule, press **Shift** while selecting additional rules.
2. Click . The rule is marked for deletion, and a  appears next to the rule.
3. Click .

Note:

Commit changes to the module to ensure that all changes are permanently saved.

Next Hop list

You can define up to 20 Next Hop lists, with 20 entries each. Each item in a list specifies an IP Address or Interface to route the packet to. If an item is down (interface down), the packet is routed according to the next item, and so on, until the end of the list. If all the items are down, the packet is routed according to Destination Based Routing.

The Next Hop tab enables you to add, modify, move, and delete entries in the Next Hop table of a Next Hop list. This section provides a description of the Next Hop table.

Note:

The following interfaces are supported as next hops:

- WAN Fast Ethernet, if it is configured either with encapsulation PPPoE or with no encapsulation but running DHCP client.
- Dialer
- Tunnel
- Null0 (discard the packets)
- Serial

Figure 94: Next Hop table

Id	Type	IP Address	Interface	Status
1	Null0	0.0.0.0	Null0	up

The following table provides a list of fields in the Next Hop Table:

Table 81: Next Hop fields

Fields	Description
Id	Index of the Next Hop entry.
Type	The type of the Next Hop entry. Possible values are: <ul style="list-style-type: none">• Interface• IP Address
IP Address	IP address of the Next Hop.
Interface	Interface of the Next Hop.
Status	Operational status of the Next Hop.


Adding routes

To add a new Next Hop route to a Next Hop routing table:

1. Click .

Or

Select **Edit > Add**.


2. Define the fields in the table cells. For more information on the route's fields see ["Next Hop list" on page 227](#).
3. Click .

Note:

A mandatory, but invalid route is highlighted in red.

Modifying routes

To modify a route:

1. Click the route you want to modify.
2. Define the route's fields in the table cells. For more information on the route's fields see ["Next Hop list" on page 227](#).
3. Click .


Note:

Modifying a route may invalidate other routes.

Copying routes

You can copy a route to a different position in the Next Hop table or to a different list.

To copy a route:

1. Select the route from the Next Hop List.
To select more than one route, press **Shift** while selecting additional routes.
2. Select **Edit > Copy**. The selected route is buffered to the clipboard.
3. If you want to copy the route to a different policy, select the table to which you want to paste the copied route.
4. Select the route above which you want to paste the copied route.
5. Select **Edit > Paste**. The route is pasted above the selected route.
6. Click .

Note:

If a route is not selected, the copied route is added to the bottom of the table.


Moving routes

You can move a route's position in a table or move it from one table to another.

To move a route:

1. Select a route from the Next Hop List.
To select more than one route, press **Shift** while selecting additional routes.
2. Select **Edit > Cut**. The selected route is buffered on the clipboard.
3. If you want to copy the route to a different table, select the table to which you want to paste the copied route.
4. Select the route above which you want to move the route.

Policy Based Routing



5. Select **Edit > Paste**. The route is inserted into the table above the highlighted route.
6. Click .

Note:

If a route is not selected, the route that is moved is added to the bottom of the table.

Deleting routes

To delete a route:

1. Select a route from the Next Hop table.
To select more than one route, press **Shift** while selecting additional routes.
2. Click . The route is marked for deletion, and a **X** appears next to the route.
3. Click .

Note:

Commit changes to the module to ensure that all the changes are permanently saved.

Policy Enforcement Points

The Policy Enforcement Points (PEPs) table allows you to add, modify, move, and delete policies to an interface. This section provides a description of the Policy Enforcement Points list.

Figure 95: Policy Enforcement Points table

Interface	Active PBR
FastEthernet 10/2	<none>
Vlan 1	<none>
Vlan 45	<none>
Vlan 66	<none>
Dialer 1	<none>

The Policy Enforcement Points table allows you to apply PBR lists to specific interfaces in the Avaya G430 Policy Based Routing. The following interfaces are supported:

- Vlan
- Wan Fast Ethernet
- Tunnel
- Dialer
- Loopback

- Serial

The following table provides a list of fields in the Policy Enforcement Points Table:

Table 82: Policy Enforcement Points Fields

Fields	Description
Interface	The interface name and description.
Active PBR	The Policy Based Route active on this interface.

To modify a Policy Enforcement Points table, select policies for interfaces using the pull-down list in the **Active PBR** field.

Configuration

The Configuration tabs perform the following function:

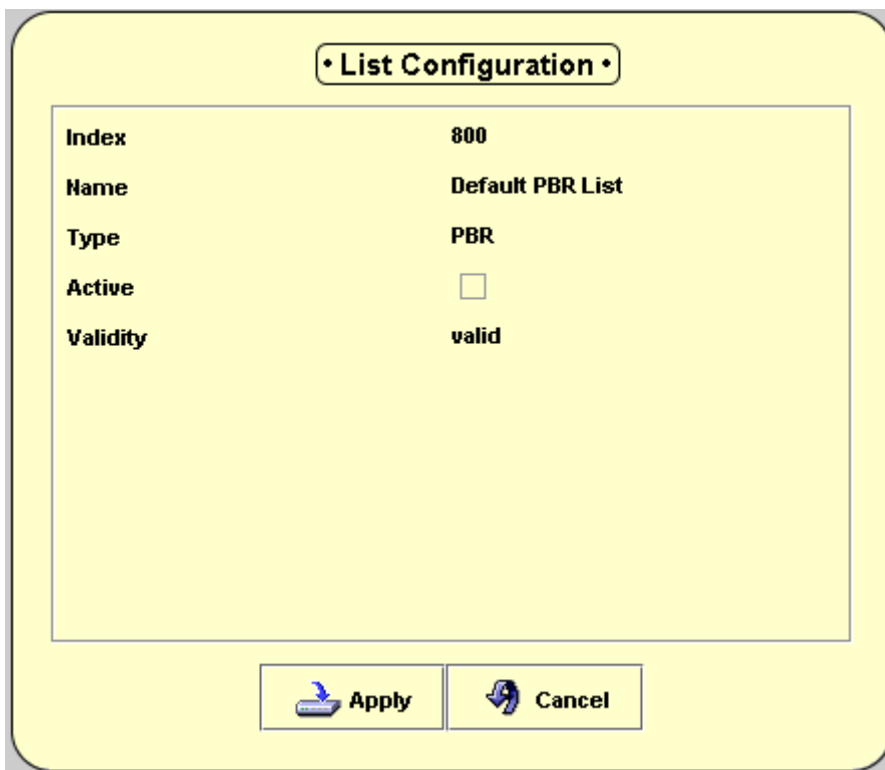
- [Policy Based Routing List Configuration](#) - The system displays this tab in the Table view when a Policy Based Routing list is selected. It enables viewing the Policy Based Routing list's configuration attributes, and changing its name.
- [Next Hop List Configuration](#) - The system displays this tab in the Table view when a Next Hop list is selected, and enables viewing the Next Hop list's configuration attributes, and changing its name.

Policy Based Routing List Configuration

To view the Policy Based Routing List Configuration form:

1. Select the policy list whose configuration form you wish to view from the Tree view.
2. Select the **Configuration** tab in the Table view.

Figure 96: Policy Based Routing List Configuration dialog box



The dialog box is titled "• List Configuration •". It contains a table with the following fields:

Index	800
Name	Default PBR List
Type	PBR
Active	<input type="checkbox"/>
Validity	valid

At the bottom of the dialog box are two buttons: "Apply" and "Cancel".

Note:

Only the **Name** field is configurable in the **Policy Based Routing List Configuration** Dialog Box.

The following table lists the fields in the Policy Based Routing List Configuration form and their descriptions:

Table 83: Policy Based Routing List Configuration fields

Field	Description
Index	The identification number of the policy list.
Name	The user defined policy name that appears in the Tree view as the policy name.
Type	The type of policy list. Possible values include: <ul style="list-style-type: none"> ● PBR - For a Policy Based Routing policy, this field always returns a value of PBR. ● NH - For a Next Hop policy, this field always returns a value of NH.
Active	Whether a policy is active or not on the module. Possible statuses include: <ul style="list-style-type: none"> ● Active - The policy is currently active. ● Not Active - The policy is currently not active.

Table 83: Policy Based Routing List Configuration fields (continued)

Field	Description
Validity	Determination of whether this list is valid.

After changing any of the fields, click **Apply** to implement the changes or **Cancel** to revert to the previous values.

Next Hop List Configuration

To view the Next Hop List Configuration form:

1. Select the policy list whose configuration form you wish to view from the Tree view.
2. Select the **Configuration** tab in the Table view.

Figure 97: Next Hop List Configuration dialog box

The dialog box is titled "• List Configuration •". It contains the following fields:

Index	1
Name	NH1
Type	NHL
Active	<input checked="" type="checkbox"/>
Validity	valid

At the bottom of the dialog are two buttons: "Apply" and "Cancel".

Note:

Only the **Name** field is configurable in the **Next Hop List Configuration** dialog box.

The following table lists the fields in the Next Hop Configuration form and their descriptions:

Table 84: Next Hop List Configuration fields

Field	Description
Index	The identification number of the policy list.
Name	The user defined policy name that appears in the Tree view as the policy name.
Type	The type of policy list. Possible values include: <ul style="list-style-type: none">● PBR - For a Policy Based Routing policy, this field always returns a value of PBR.● NH - For a Next Hop policy, this field always returns a value of NH.
Active	Whether the policy is active or not on the module. Possible statuses include: <ul style="list-style-type: none">● Active - The policy is currently active.● Not Active - The policy is currently not active.
Validity	Determination of whether this list is valid.

Using Address Wildcards

Wildcards are used to mask all or part of a source or destination IP address. Using wildcards, you can create filters for IP addresses. A wildcard can also be used to mask specific bits of an IP address. This mask is used to specify bits that are used and bits that are ignored.

If you specify **Host**, the wildcard is set to 0.0.0.0 and the entire address is used. If you specify **Any**, the wildcard is set to 255.255.255.255 and the IP address is ignored. You can also specify a custom wildcard to mask a part of the IP address.

Examples:

- If the source IP address is 149.36.184.189 and the wildcard is 255.0.255.255, the rule applies to all the packets, where the second byte of the IP address is 36. The 255 in the first, third, and fourth bytes allow any value in the corresponding bytes of the source address to match this rule.
- If the destination address is 149.36.184.189 and the destination wildcard is 255.255.127.0, the rule applies only to the traffic directed to IP addresses whose third byte is between 128-255 and whose fourth byte is 189.

Using the IP Simulate function

This section provides instructions on activating and using the IP Simulate function to simulate the effect of rules on information packets. It discusses the following topics:

- [IP Simulate overview](#) - An overview of the IP Simulate function.
- [Using IP Simulate](#) - Instructions on using the IP Simulate function to simulate the actions of a policy on defined packets.

IP Simulate overview

The IP Simulate function allows you to view the results of a policy on a simulated packet.

The IP Simulate function tests a simulated packet against the rules in a policy. The rules are applied to the simulated packets in the order they appear in the Rules List, and the resulting operation is reported in the **Result** field of the **IP Simulate** dialog box.

The rule that matches the packet is highlighted in the Rules List. This enables you to view the outcome of a policy before activating it. It also eases the editing of rules in a policy to provide the desired results.

Note:

IP Simulate only operates on saved policies. Ensure that changes to the policy are applied before testing the packets.

Note:

IP Simulate can be used only when a specific Rules List is selected in the Tree view.

Using IP Simulate

To analyze the results of a policy on simulated packets:

1. Select a policy.

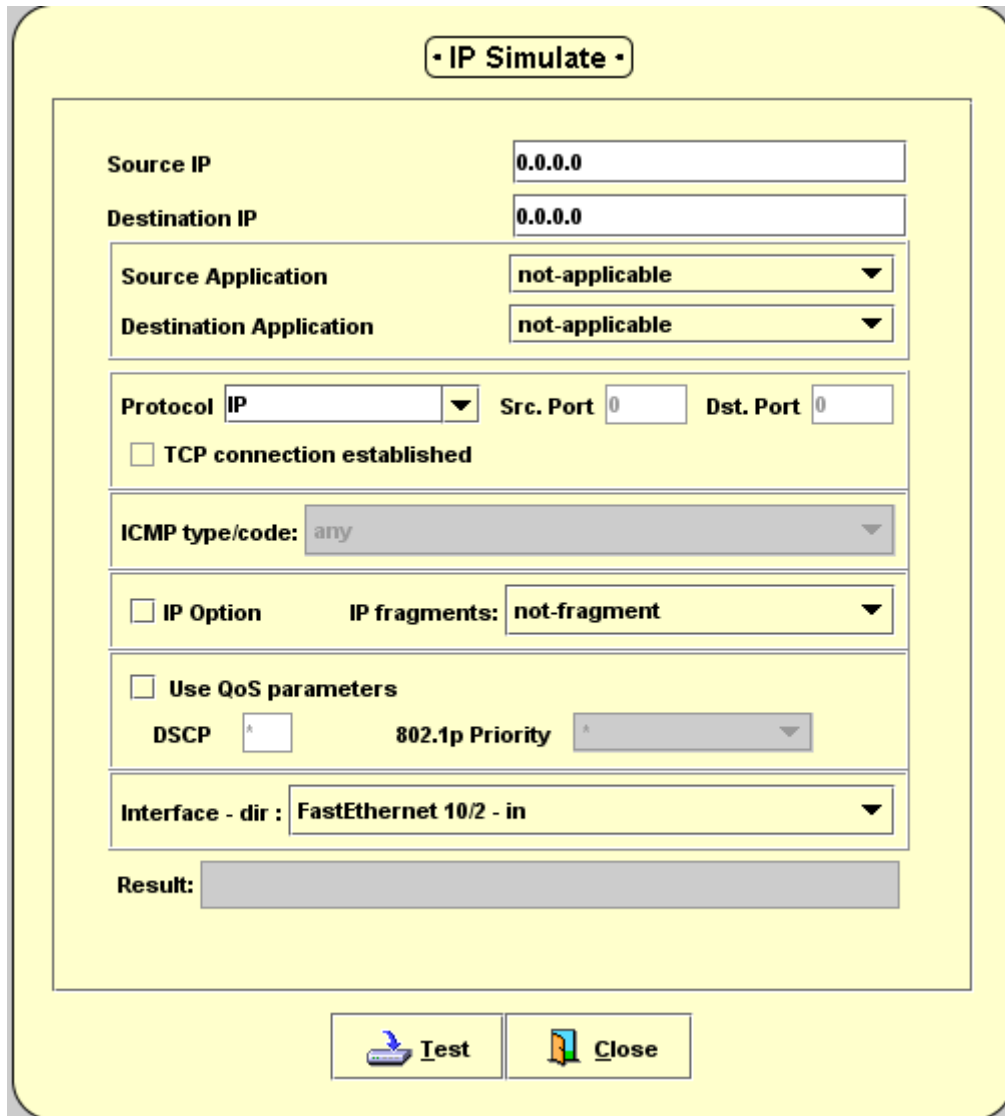
Policy Based Routing

2. Click .

Or

Select **Actions > Simulate**. The system displays the **IP Simulate** dialog box in the Form view area.

Figure 98: IP Simulate



The IP Simulate dialog box is a yellow-bordered window with a title bar that says "• IP Simulate •". It contains several input fields and checkboxes for configuring a simulated packet. The fields are arranged in a vertical stack. At the bottom, there are two buttons: "Test" (with a blue arrow icon) and "Close" (with a red X icon).

Field	Value
Source IP	0.0.0.0
Destination IP	0.0.0.0
Source Application	not-applicable
Destination Application	not-applicable
Protocol	IP
Src. Port	0
Dst. Port	0
TCP connection established	<input type="checkbox"/>
ICMP type/code:	any
IP Option	<input type="checkbox"/>
IP fragments:	not-fragment
Use QoS parameters	<input type="checkbox"/>
DSCP	A
802.1p Priority	A
Interface - dir :	FastEthernet 10/2 - in
Result:	

3. Define a simulated packet using the fields in the **IP Simulate** dialog box. For more information on the fields in IP Simulate, see the following table.
4. Click **Test**. The effect of the policy on the simulated packet appears in the **Result** field and the matching rule is highlighted in the Rules Table.

The following table provides a list of fields in IP Simulate and their descriptions:

Table 85: IP Simulate fields

Field	Description
Source IP	The IP address of the device from which the simulated packet originates.
Destination IP	The IP address of the device to which the simulated packet is addressed.
Source Application	The application from which the simulated packet is sent. Select an application from the drop-down list or select custom and define the Protocol and Port fields.
Destination Application	The application to which the simulated packet is sent. Select an application from the pull-down list or select custom and define the Protocol and Port fields.
Protocol	The number of the application protocol. The number can range between 0-255. <ul style="list-style-type: none"> ● TCP - The protocol number is 6. ● UDP - The protocol number is 17.
Src. Port	A specific application source. When combined with the protocol number, this identifies the application from which the packet is sent.
Dst. Port	A specific application destination. When combined with the protocol number, this identifies the application to which the packet is sent.
TCP connection established	The type of session to which the rule applies. If selected, the simulated packet is from an established session. An established session occurs when the packets entering the module respond to a previously established communications session. If this is not selected, the simulated packet is not from an established session.
ICMP type/code	Type of ICMP packet to be used in this simulation. For possible values, see Appendix C: "ICMP Packet Types & Codes" on page 255 .
IP Option	Enables setting of IP Fragmentation options.
IP fragments	Options for IP packet fragmentation. Possible values are: <ul style="list-style-type: none"> ● Not fragmented ● First packet fragmented ● Packet fragmented non-I4
1 of 2	

Table 85: IP Simulate fields (continued)

Field	Description
Use QoS parameters	<p>Enables QoS parameters for forwarding the packet. The possible options are:</p> <ul style="list-style-type: none"> ● Selected ● Cleared <p>If the Use QoS Parameters box is selected, the IP simulate function uses the values in the DSCP and 802.1p fields for determining the action to be taken on the simulated packet. The DSCP and 802.1p fields must contain valid values.</p> <p>If the Use QoS Parameters is cleared, the IP simulate function ignores the DSCP and 802.1p fields.</p> <p>Note:</p> <p style="padding-left: 40px;">This field does not appear if the simulation is based on an ACL.</p>
DSCP	The value of the DSCP tag on the simulated packet. Valid values are between 0-63. The value of * indicates that this field should be ignored. This value affects the forwarding priority of the packet when the operation to be taken on the packet is permit .
802.1p Priority	The value of the CoS tag on the simulated packet. The tag value of CoS runs from 0-7. The value of * indicates that this field should be ignored. This value affects the forwarding priority of the packet when the operation to be taken on the packet is permit .
Interface - dir	The interface and direction on an X330WAN expansion module for which the rule applies. Select an interface and direction from the drop-down list.
Result	The operation that is carried out on the simulated packet, if the selected policy is active.
2 of 2	

Chapter 20: Applications Editor Tool

This chapter provides instructions on using the Application Editor Tool and customizing the application protocols. It contains the following sections:

- [Applications Editor overview](#) - An overview of the Applications Editor.
- [Using the Applications Editor](#) - Detailed instructions on using the Applications Editor including adding, modifying, and deleting application protocols, and creating ASCII reports.
- [Reports](#) - Detailed instructions on creating an ASCII report of the application protocols listed in the Applications Editor.

Applications Editor overview

The Avaya G430 Policy Based Routing allows you to specify application protocols by selecting an application name that represents a protocol and its port number information. The mapping of the application name to the information it represents is managed by the Applications Editor.

Using the Applications Editor you can add, modify, and delete custom application protocols. Default application protocols cannot be modified or deleted. You can also create ASCII reports of the applications listed in the Applications Editor.

Using the Applications Editor

This section provides a description of the Applications Editor, and discusses the following topics:

- [Adding Application Protocols](#)
- [Modifying an Application Protocol](#)
- [Deleting an Application Protocol](#)
- [Applying Changes](#)

To open the Applications Editor:

Select **Tools > Applications Editor**.

Figure 99: Applications Editor

Name	Type	Min Port	Max Port	Notes
any	A	N/A	N/A	Any applications
auth	TCP	113	113	Identification protocol determine the ide...
bgp	TCP	179	179	Border Gateway Protocol
bootpc	UDP	68	68	BOOTP client
bootps	UDP	67	67	BOOTP server - bootstrap protocol allows...
chargen-tcp	TCP	19	19	sends a character pattern back to the ori...
chargen-udp	UDP	19	19	sends a character pattern back to the ori...
daytime-udp	UDP	13	13	returns a date/time string
dns-tcp	TCP	53	53	Domain Name Service
dns-udp	UDP	53	53	Domain Name Service
echo-udp	UDP	7	7	returns whatever data is received to the ...
exec	TCP	512	512	Remote Execution
finger	TCP	79	79	User Information Protocol
ftp-all	TCP	20	21	File Transfer Protocol - Control and Data
ftp-ctrl	TCP	21	21	File Transfer Protocol - Control stream
ftp-data	TCP	20	20	File Transfer Protocol - Data stream Tran...
gopher	TCP	70	70	distributed document search and retriev...
h323gatedisc-tcp	TCP	1718	1718	
h323gatedisc-udp	UDP	1718	1718	
h323gatestat-tcp	TCP	1719	1719	
h323gatestat-udp	UDP	1719	1719	
h323hostcall-tcp	TCP	1720	1720	
h323hostcall-udp	UDP	1720	1720	
hostnames	TCP	101	101	Host name server
http-proxy	TCP	8080	8080	Default port of HTTP proxy service Defaul...
http-www	TCP	80	80	Hypertext Transfer Protocol Main web-br...
https	TCP	443	443	http protocol over TLS/SSL
hylafax	TCP	4559	4559	HylaFAX client-server
ICMP	1	N/A	N/A	Internet Control Message Protocol Debug...
IGMP	2	N/A	N/A	Internet Group Management joining/leavi...
iiop	TCP	535	535	Corba Protocol
imapv2	TCP	143	143	Interim Mail Access Protocol v2
imapv3	TCP	220	220	Interim Mail Access Protocol v3
irc	TCP	194	194	Internet Relay Chat
ircd-tcp	TCP	6667	6667	Internet Relay Chat
ircd-udp	UDP	6667	6667	Internet Relay Chat

The following table provides a list of the fields in the Application Editor and a description of each field:

Table 86: Applications Editor fields

Field	Description
Name	The name of the application protocol.

Table 86: Applications Editor fields (continued)

Field	Description
Type	The application type. Possible types are: <ul style="list-style-type: none"> • TCP • UDP • * (Other protocols)
Min Port	The low end of the range of ports for this protocol.
Max Port	The high end of the range of ports for this protocol.
Notes	A user defined description of the protocol.

Adding Application Protocols

To add a new application protocol:

1. Click .

Or

Select **Edit > Add**.

2. Define the application protocol using the fields in the table.

Modifying an Application Protocol

To modify an application protocol:

1. Select the application protocol you want to modify.
2. Edit the application protocol's fields in the table.

Deleting an Application Protocol

To delete an application protocol:

1. Select the application protocol you want to delete.

2. Click .

Or

Select **Edit > Delete**. A  appears next to the protocol.

Applying Changes

When the Avaya G430 Policy Based Routing is updated with changes in the Applications Editor table, the Rules List is updated.

Added protocols appear in the Application field, and deleted applications no longer appear in the Application field.

To update the changes in the Applications Editor table, click . The Application field in the Rules List is also updated.

Reports

You can create an ASCII report of the application protocols listed in the Applications Editor. The report is a text file with information in each column separated by tabs.

To create an ASCII report of the Applications Editor table:

1. Click .

Or

Select **File > Report**.

2. Select a directory for the report.
3. Enter a name for the report.
4. Click **Save**. The report is saved to the specified file.

Appendix A: Menus

This appendix gives the full structure of the menus in the Avaya G430 Manager.

- [Device Manager Menus](#)
- [Routing Manager Menus](#)
- [Policy Based Routing Menus](#)
- [Applications Editor Menus](#)

Device Manager Menus

This section provides the menu structure of the Avaya G430 Device Manager.

- [File Menu](#)
- [View Menu](#)
- [Configure Menu](#)
- [Actions Menu](#)
- [Tools Menu](#)
- [Help Menu](#)

File Menu

Table 87: File Menu - Device Manager

Item	Description
Exit	Exits the Avaya G430 Manager. Note: This function is not supported when running the Avaya G430 Manager in a web browser. Close the browser to exit the application.

View Menu

Table 88: View Menu - Device Manager

Item	Description
Refresh	Refreshes the display with information from the device.
Configuration	Moves to the configuration mode of the Device Manager.
Port RMON	Moves to the monitoring mode of the Device Manager.
Switch-Connected Addresses	Opens the Switch-Connected Addresses table.
Toolbars > Show Application Toolbar	Toggles the display of the application toolbar.
Toolbars > Show Get/Set Toolbar	Toggles the display of the Get/Set toolbar.

Configure Menu

Table 89: Configure Menu - Device Manager

Item	Description
Device Configuration	Displays configuration information of the device.
VLAN	Displays and enables configuration of VLANs.
1 of 2	

Table 89: Configure Menu - Device Manager (continued)

Item	Description
Port Redundancy	Displays and enables configuration of port redundancies.
Port Mirroring	Allows copying of all transmitted and received packets from one port to another.
Trap Managers	Displays managers and traps configuration information.
WAN > Backup Interfaces	Opens the Backup Interfaces table.
WAN > Dynamic CAC	Allows configuration of Dynamic CAC.
Dialer	Allows configuration of the Dialer.
Servers > DHCP Server	Allows configuration of the DHCP server.
Servers > TFTP Server	Allows configuration of the TFTP server.
CNA	Allows configuration of DNS clients through the Converged Network Analyzer application.
2 of 2	

Actions Menu

Table 90: Actions Menu - Device Manager

Item	Description
802.1X > Initialize Selected Ports	Initializes 802.1x security on the selected ports.
802.1X > Initialize All Ports	Initializes 802.1x security on all the ports on the device.
802.1X > Reauthenticate Selected Ports	Reauthenticates 802.1x security on the selected ports.
802.1X > Reauthenticate All Ports	Reauthenticates 802.1x security on all the ports on the device.
Reset Device	Resets the entire device.
Reset Media Module	Resets the selected modules.
Commit	Saves the updated configuration to the device.
Clear CAM	Clears the CAM table for the device.

Tools Menu

Table 91: Tools Menu - Device Manager

Item	Description
Administer Station/Gateway	Opens the Avaya Site Administrator on the selected station or gateway.
Administer Call Controller	Opens the Avaya Site Administrator on the selected Media Call Controller.

Help Menu

Table 92: Help Menu - Device Manager

Item	Description
Help Contents	Opens the online help contents page.
Help On	Activates online help.
About Avaya G430 Manager	Copyright information about the Avaya G430 Device Manager.

Routing Manager Menus

This section provides the menu structure of the Avaya G430 Routing Manager.

- [File Menu](#)
- [Edit Menu](#)
- [View Menu](#)
- [Action Menu](#)
- [Help Menu](#)

File Menu

Table 93: File Menu - Routing Manager

Item	Description
Save	Saves the current table to a text file.
Commit	Saves the current configuration to the router.

Edit Menu

Table 94: Edit Menu - Routing Manager

Item	Description
Undo	Undoes changes made to the table or form currently displayed.
Copy	Buffers the selected information to the clipboard.
Paste	Pastes information from the clipboard into the selected table row.
Insert Row	Adds a row to the table.
Delete Row	Deletes the selected table row.

View Menu

Table 95: View Menu - Routing Manager

Item	Description
Refresh	Refreshes the information in the current table.
Form	Toggles the display of a form corresponding to the current table.
More	Toggles the display of additional table parameters.

Action Menu

Table 96: Action Menu - Routing Manager

Item	Description
Stop	Stops loading information into the current table.
Apply	Sends the configuration information to the device.
Start Point	Opens the Start Point dialog box for specifying the starting point of entries displayed in the table.
Reset	Resets the selected router.

Help Menu

Table 97: Help Menu - Routing Manager

Item	Description
Context Sensitive Help	Activates context sensitive help.
Contents	Opens the online help contents page.
About Routing Manager	Copyright information about the Avaya G430 Routing Manager.

Policy Based Routing Menus

This section provides the menu structure of the Avaya G430 Policy Based Routing.

- [File Menu](#)
- [Edit Menu](#)
- [View Menu](#)
- [Tools Menu](#)
- [Help Menu](#)

File Menu

Table 98: File Menu - Policy Based Routing

Item	Description
New List	Creates a new policy list.
New List > PBR List	Creates a new Policy Based Routing list.
New List > NH List	Creates a new Next Hop list.
Commit	Saves the current configuration to the device.

Edit Menu

Table 99: Edit Menu - Policy Based Routing

Item	Description
Revert	Clears uncommitted changes and reverts to the last saved configuration of a list.
Add	Adds a line to a list.
Cut	Cuts a line from a list and buffers it for copying.
Copy	Copies a line from a list.
Paste	Pastes a copied line to a list.
Delete	Deletes a line from a list.
Select All	Selects all lines in a list.

View Menu

Table 100: View Menu - Policy Based Routing

Item	Description
Tooltip	Enables viewing of tooltips.
Refresh	Refreshes information in the current table.

Tools Menu

Table 101: File Menu - Policy Based Routing

Item	Description
Applications Editor	Launches the Application Editor.

Help Menu

Table 102: Help Menu - Policy Based Routing

Item	Description
Contents	Opens the online help contents page.
Help On	Activates context sensitive help.
About Avaya Policy Based Routing	Copyright information about the Avaya Policy Based Routing.

Applications Editor Menus

This section provides the menu structure for the Applications Editor tool.

- [File Menu](#)
- [Edit Menu](#)
- [Help Menu](#)

File Menu

Table 103: File Menu - Applications Editor

Item	Description
Report	Generates the selected report.
Print	Prints the current report.
Exit	Exits the Applications Editor tool.

Edit Menu

Table 104: Edit Menu - Applications Editor

Item	Description
Refresh	Refreshes the information in the current table.
Add	Adds a new entry to the current table.
Delete	Deletes an entry from the current table.

Help Menu

Table 105: Help Menu - Applications Editor

Item	Description
Help Contents	Opens the online help contents page.

Appendix B: Web Management

This appendix provides instructions for managing the Avaya G430 Devices through the Internet and contains the following sections:

- **Web Management overview** - An overview on web management.
- **Configuring the Avaya G430 Device** - Instructions on how to configure the Avaya G430 Device for the first time.

Web Management overview

Web management provides a simple method of managing the Avaya G430 Devices through the Internet. The Avaya G430 Manager software need not be installed on your computer.

Instead, a small plug-in for your web browser activates the embedded manager software. This plug-in loads automatically when you use web management.

Note:

Port RMON is not available through web management.

Online help is available only if you have installed the online help on your network and configured the Avaya G430 Device with the location of the help files.

Configuring the Avaya G430 Device

When an Avaya G430 is initially configured as a full router, it must be assigned an IP address. The IP address must be assigned using the CLI (Command Line Interface) setup screens. For information on assigning an IP address to the router module, see the *Administration for the Avaya G430 Media Gateways*.

Appendix C: ICMP Packet Types & Codes

This appendix lists the various ICMP Packet Types and Codes as used in [“Using IP Simulate” on page 235](#).

Note:

Some ICMP Packet Types have no corresponding Code.

ICMP Packet Type/Code List

Table 106: ICMP Packet Types/Codes

Description	ICMP Type	ICMP Code
Echo Reply	0	0
Unreachable	3	--
Network Unreachable	3	--
Host Unreachable	3	1
Protocol Unreachable	3	2
Port Unreachable	3	3
Fragmentation Needed but DF Bit Set	3	4
Source Route Failed	3	5
Destination Network Unknown	3	6
Destination Host Unknown	3	7
Destination Network Administratively Prohibited	3	9
Network Unreachable for TOS	3	11
Host Unreachable for TOS	3	12
Communication Administratively Prohibited by Filtering	3	13
Host Precedence Violation	3	14
Precedence Cutoff in Effect	3	15
1 of 3		

Table 106: ICMP Packet Types/Codes (continued)

Description	ICMP Type	ICMP Code
Source Quench	4	0
Redirect	5	--
Redirect for Network	5	0
Redirect for Host	5	1
Redirect for Type-of-Service and Network	5	2
Redirect for Type-of-Service and Host	5	3
Echo Request	8	0
Router Advertisement	9	0
Router Solicitation	10	0
Time Exceeded	11	--
Time-to-Live Equals 0 During Transit	11	0
Time-to-Live Equals 0 During Reassembly	11	1
Parameters Problem	12	--
Bad IP Header	12	0
Required Option Missing	12	1
Timestamp Requested	13	0
Timestamp Reply	14	0
Address Mask Request	17	0
Address Mask Reply	18	0
Traceroute	30	--
Traceroute Outbound Packet Successfully Forwarded	30	0
Traceroute No Route for Outbound Packet	30	1
Conversion Errors	31	--
Mobile Host Redirect	32	--
IPv6 Where-Are-You	33	--
IPv6 I-Am-Here	34	--
2 of 3		

Table 106: ICMP Packet Types/Codes (continued)

Description	ICMP Type	ICMP Code
Mobile Registration Request	35	--
Mobile Registration Reply	36	--
Domain Name Request	37	0
Domain Name Reply	38	0
Skip Algorithm Discovery Protocol	39	0
Security Failure	40	--
3 of 3		

Index

Numerical

802.1x	
device configuration.	43
port configuration	55

A

Adding	
application protocols	241
managers to table	166
policies.	222 , 228
Port Redundancy	155
routes	228
rules	226
table entries	171
Additional table parameters, viewing	170
Address wildcards	234
Application Protocols	
adding	241
applying changes	242
deleting a protocol	241
modifying	241
Application tabs	22
Application Toolbar	
Device Manager	26
Routing Manager	168 , 178
Application Toolbar buttons	
Routing Manager	168 , 178
Applications editor	
overview	239
using	239
Applying changes	
in tables	23
Port Redundancy	162
VLAN configuration	138
ARP Table window	191
ASCII reports	242
Avaya G430 Manager	
Application tabs	22
connected stations	151
device configuration.	35
Device Manager	25
embedded tools	85
introduction.	19
Media Gateway functions	71
modes	31
overview	19
Policy Based	219
Port Mirroring	139
Port Redundancy	153

port RMON	147
Routing Manager	167 , 177
starting	20
Status Line	22
trap managers	163
user interface	22
VLANs	127
VoIP Engine configuration	77
WAN configuration	99
welcome to Avaya G430 Manager	13
Avaya G430 Manager, PoE	67
Avaya QoS Manager	
main views	219
views overview	219
Avaya Site Administration (ASA).	76

B

Backup interface	
configuration	117
create	118
delete	118
table	117
Backup Interface Parameters screen.	123
Backup Interface Wizard	
Backup Interface Parameters screen	123
Confirmation screen	124
overview	119
Select Backup Interface screen.	122
Select Primary Interface screen	121
Welcome screen	120

C

Chassis View.	29
Application Toolbar	26
colors in	29
Get/Set Toolbar	27
selecting elements.	31
Status Line	22
CNA Schedulers, configuring	97
Committed changes	172 , 180
Configuration form	
device	231
policy list	231
Configuring	
a port's VLAN configuration	132
applying changes	172 , 180
backup interfaces	117
CNA schedulers.	97
committed changes	172 , 180
Converged Network Analyzer application	94

Index

devices	35	backup interface.	118
devices via the Internet	253	managers from table.	166
DHCP server	85	policies	222
dialer	64	Port Redundancies	162
Ethernet LAN port	99	routes	230
Ethernet WAN port	103	rules	227
external modems	61	table entries.	171
LLDP	59	VLANs	136
Media Gateway.	71	Desktop	29
Media Gateway modules	72	Destination Port Selection screen	144
media module	75	Device	
modules	46	configuration	35
Next Hop lists	227	information	35
PoE information	68	refreshing information	32
PoE modules	68	resetting	66
PoE ports	69	traps	164
Port Mirroring.	139	updating	138, 162
port security	55	Device configuration	
ports	49	802.1x tab	43
PVID.	138	Advanced tab	39
running changes	172, 180	FRU tab	41
saving changes.	172, 179, 180	General tab	36
Test Plug.	94	introduction	35
TFTP server	93	network bridging information	39
trap managers	163	STP (Spanning Tree Protocol) information	39, 41
VLAN settings for ports	138	Device configuration form	231
VLANs	133	Device Manager	
VoIP Engine	77	Application Toolbar	26
WAN.	99	Chassis View	29
Confirmation screen		Desktop	29
Backup Interface Wizard	124	Dialog Area	31
Port Mirroring Wizard	146	Get/Set Toolbar	27
Port Redundancy Wizard	161	help	33
Connected stations	151	menus	243
Contents page in Help	33, 173, 180	overview	25
Contracting		Toolbar	26
VLAN tree branch.	129	Tree View.	29
Converged Network Analyzer		user interface	25
configuring	94	DHCP	
configuring test plugs	94	DHCP/BOOTP Global Parameters window	196
scheduling test plugs	97	DHCP/BOOTP Parameters window.	198
Copying		overview	196
routes	229	DHCP configuration	
Copying rules	226	basic configuration options.	86
Create Welcome screen	141	configuring a DHCP pool.	89
Creating		configuring assignment parameters.	90
backup interface	118	creating a new DHCP pool	87
table entries	171	General DHCP Options Config tab	90
VLANs	133	General tab	86
cRTP header compression	214	introduction	85
cRTP interfaces window	214	New Pool tab	87
D		Pool Config tab	89
Deleting		DHCP Server	
application protocols	241	configuration	85
		Dialer configuration	64

Dialog Area	31
Dialog box symbols	32
Discarding Port Redundancy changes.	162
Dragging and dropping for PVID configuration	138
Dynamic CAC, configuring	125

E

Edit/Delete Welcome screen	142
Editing	
table entries	171
tables	170
the Trap Managers table	166
VLAN names	134
Embedded tools	85
Ethernet LAN port configuration	
Advanced tab.	103
General tab	100
introduction.	99
Ethernet WAN port configuration	
DHCP Client tab	110
Extended Keep Alive tab	114
General tab	105
introduction.	103
PPPoE Client tab	108
Expanding VLAN tree branch	129

F

Fields	
policy list	221
rules list	222
Folder	
DHCP	196
IP Route	181
Layer 2.	175
OSPF	203
RIP	199
VRRP	211
Form	
device configuration.	231
policy list configuration	231
Frames Direction Selection screen	145
FRU (Field Replaceable Units)	
device configuration.	41

G

General configuration	
of a module	47
of a port	50
of the device	36
Get/Set Toolbar	27
Graph	
Port RMON traffic.	148
scrolling within	149
unfreezing	149
zooming in and out	148

Guide	
organization.	13
purpose.	13

H

Header compression	
cRTP header compression	214
introduction	214
TCP header compression	216
Help	
contents page	33 , 173 , 180
Routing Manager	173 , 180
topic	33 , 173 , 180
using	33
Hiding additional table parameters.	170
How this guide is organized	13
How to	
access the VLAN Configuration dialog box	129
activate a policy	221
add policies	222 , 228
add routes to a policy	228
add rules to a policy	222 , 226
change routes.	229
change rules	226
configure backup interfaces	117
configure devices	35
configure WAN	99
copy routes	229
copy rules.	226
delete policies.	222
delete routes	230
delete rules	227
delete rules in a policy	222
modify routes	229
modify rules.	222 , 226
move routes.	229
move rules	222 , 227
open a rules list	222
scroll within the graph	149
select elements	31
select the active policy.	221
sort the list of switch connected addresses	152
unfreeze the graph	149
use address wildcards	234
use on-line help	173 , 180
use the Device Manager Application Toolbar	26
use the Get/Set Toolbar	27
use the table view	220
use the tree view	220
view a list of policies.	221
view backup interfaces.	117
zoom in and out of the graph	148

I

ICMP packet types/codes	255
-----------------------------------	---------------------

Index

Intended audience	13	Managing	
Internet management		devices via the Internet	253
configuration	253	tables.	23
overview	253	Manual	
Introduction		organization.	13
Avaya G430 Manager.	19	purpose.	13
Avaya G430 Manager User Guide	13	Master VLAN list	128
IP Global Parameters window	181	Media Gateway	
IP Interfaces window	182	Avaya Site Administration	76
IP Route		device configuration	71
ARP Table	191	G430	71
cRTP interfaces window.	214	media module configuration	75
DHCP	196	MG Config tab	72
DHCP/BOOTP Global Parameters window	196	MGC Config tab.	74
DHCP/BOOTP Parameters window	198	module configuration	72
Header compression	214	overview	71
IP Global Parameters	181	Media Gateway Controller	
IP Interfaces	182	IP settings	74
IP Tunnel	193	Media module	
OSPF	203	configuration	75
OSPF Area Parameters window	206	list of models	47
OSPF External Database window	209	Menus	
OSPF Global Parameters window	203	Device Manager.	243
OSPF Interfaces window	204	Routing Manager	247
OSPF Link State Database window	207	MG Config tab	72
OSPF Neighbors window	210	MGC Config tab	74
overview	181	Modems	
RIP	199	configuring	61
RIP Global Parameters window	199	resetting	66
RIP Interfaces window	200	Modes	
Routing Table	186 , 189	Configuration	31
TCP header compression interfaces window	216	Port RMON	31
VRRP	211	switching between.	31
VRRP Global Parameters window	211	Modifying	
VRRP Table window	212	routes	229
IP Simulate		table entries.	23 , 171
activating.	235	Module	
fields.	235	colors.	29
ICMP packet types and codes	255	configuration	46
introduction.	235	configuring PoE	68
overview	235	resetting	66
starting.	235	Module configuration	
IP Tunnel Table	193	General tab	47
		introduction	46
L		Monitoring	
Layer 2 overview.	175	performance	147
LLDP		traffic	147
Configuration	59	traffic through a specific port	139
M		Moving	
Manager		routes	229
adding and removing	166	Moving rules	227
editing	166	N	
Routing	167 , 177	Name and Type screen	160
trap	163	Next Hop List	

adding routes	228
copying routes	229
defining	227
deleting routes	230
modifying routes	229
moving routes	229
Next hop list configuration form	233
Next Hop Table	
supported interfaces	227

O

Organization of guide	13
OSPF	
Area Parameters window	206
External Database window	209
Global Parameters window	203
Interfaces window	204
Link State Database window.	207
Neighbors window	210
overview	203
Overview	
Avaya G430 Manager	19
Avaya QoS Manager Views	219
PoE	67
Port Mirroring.	139
Port Redundancy	153
switch connected addresses.	151
trap managers	163
VLAN configuration	127
VLANs	127
VoIP	77

P

PBR	
configuration	231
overview	219
Policy based routing list	221
Policy based routing rules list	222
Policy Enforcement Points (PEPs) table	230
using Tree View	220
PBR list	
adding a policy	222
deleting a policy	222
overview	221
PBR list name	231
PBR rules list	
adding a rule	226
copying a rule	226
deleting a rule	227
modifying a rule	226
moving a rule.	227
overview	222
PEPs table	230
Pie chart	148
PoE	

configuring modules	68
configuring ports	69
overview	67
viewing configuration	68
viewing information	67
Policies	
adding	222 , 228
deleting.	222
testing on simulated IP packets.	235
viewing a list of	221
Policy based routing list configuration	231
Policy based routing list, see PBR list	221
Policy based routing rules list, see PBR rules list	222
Policy Based Routing, see PBR	219
Policy Enforcement Points (PEPs) table	230
Policy list configuration form.	231
Policy list fields.	221
Port	
colors.	29
configuration	49 , 138
Configuration Area	132
configuring PoE	69
configuring security	55
Ethernet LAN configuration	99
Ethernet WAN configuration	103
PVID configuration	138
redundancy see Port Redundancy	
selecting	31
viewing PoE information	67
viewing VLAN configuration	137
VLAN settings.	137
Port configuration	
802.1x tab	55
Advanced tab	53
General tab	50
introduction	49
LLDP tab	59
Port Mirroring	
configuring	139
overview	139
Port Mirroring Wizard	
Confirmation screen	146
Create Welcome screen	141
Destination Port Selection screen	144
Edit /Delete Welcome screen.	142
Frames Direction Selection screen	145
overview	140
Source Port Selection screen	142
Port Redundancy	
adding	155
deleting.	162
overview	153
updating table.	162
viewing the Port Redundancy dialog box	154
Port Redundancy Wizard	

Index

Confirmation screen	161
Name and Type screen	160
overview	156
Primary Port Selection screen	158
Secondary Port Selection screen	159
Welcome screen	157
Port RMON	
overview	147
pie chart	148
traffic graph	148
window.	147
Power over Ethernet, see PoE	
Primary Port Selection screen	158
R	
Refreshing	
device information	32
Port Redundancy dialog box.	162
tables	23
Removing	
managers from table	166
table entries	171
Renaming VLANs	134
Reports	242
Resetting	
devices	66
modem.	66
modules	66
routers	172
Resizing	
Table Area	170 , 179
RIP	
Global Parameters window	199
Interfaces window	200
overview	199
Routes	
adding	228
changing	229
copying	229
deleting	230
modifying	229
moving.	229
Routing Manager	
help	173 , 180
introduction.	167 , 177
menus	247
resetting	172
Table Area	170 , 179
Toolbar	168 , 178
Tree View	169 , 179
user interface.	167 , 177
Routing Table window	186 , 189
Rules list fields	222
Rules, PBR	
adding	226

changing	226
copying	226
deleting	227
modifying	226
moving	227
Running Avaya G430 Manager	
from Avaya Network Management Console	20
through the Internet	20
Running changes.	172 , 180

S

Saving table information as text	171
Scrolling within the graph	149
Secondary Port Selection screen	159
Security, port.	55
Select Backup Interface screen	122
Select Primary Interface screen	121
Selecting	
elements	31
traffic to monitor.	149
Selection List.	131
Server	
embedded functions	85
Simulating IP packets.	235
Sorting the list of stations	152
Source Port Selection screen	142
Starting	
Avaya G430 Device Manager using Avaya Network Management	20
Avaya G430 Manager	20
Web management.	20
Station connections.	151
Status	
tab, VoIP	81
Status Line.	22
STP (Spanning Tree Protocol)	
device configuration	39
port configuration	53
Switch connected addresses	
overview	151
sorting list.	152
window	151
Switching views	22
Symbols in tables.	23
Synchronizing VLAN names.	135

T

Table	
adding and deleting managers	166
adding entries	171
apply changes	23 , 170
Backup Interfaces	117
Device Trap Managers.	164
editing Trap Managers.	166
Port Redundancy	154
refreshing.	23

row symbols	23
saving as text.	171
Selection List	131
undoing changes	23 , 170
using.	32
Table Area	
in Routing Manager	170 , 179
resizing	170 , 179
Table Entries	
Adding	171
Creating	171
Deleting	171
Editing	171
Modifying	171
Removing	171
Table view	
using.	220
Tabs, application.	22
Tagging packets with VLAN information	128
TCP header compression	216
TCP header compression interfaces window.	216
Test Plug	
configuring	94
scheduling	97
Testing rules to test a simulated packet	235
TFTP server	
configuring	93
Toolbar	
Device Manager Application	26
Device Manager Get/Set	27
Routing Manager	168 , 178
Toolbar buttons	
Routing Manager	168 , 178
Traffic	
Port RMON graph	148
types.	149
viewing statistics	148
Trap managers	
configuration	163
overview	163
Trap Managers table	
adding and deleting managers.	166
device	164
editing	166
Traps	
device	164
Tree View	
Device Manager	29
in Routing Manager	169 , 179
Tree view	
levels	220
using.	220
Types of traffic.	149

U

Undo changes in table	170
Unfreezing the graph	149
Updating	
changes in table.	170
Port Redundancy information	162
User interface	
Avaya G430 Manager	22
Device Manager.	25
Routing Manager	167 , 177
Using	
Applications editor.	239
Avaya G430 Manager help.	33
Chassis View	29
Device Manager Application Toolbar	26
dialog boxes	32
Get/Set Toolbar	27
on-line help	173 , 180
table view.	220
tables.	32
the tree view	220
Using address wildcards	234

V

Viewing	
additional table parameters	170
backup interfaces	117
connected stations	151
device information.	35
device traps.	164
embedded tools	85
Ethernet LAN port configuration	99
Ethernet WAN port configuration	103
module configuration	46
port configuration	49
port VLAN configuration	137
Switch Connected Addresses window	151
the Port Redundancy dialog box	154
the Port RMON window	147
traffic statistics	148
VLAN list	129
VLANs	
accessing the dialog box.	129
applying configuration changes.	138
configuration	127
creating.	133
creating, deleting, and renaming	133
deleting.	136
expanding and contracting tree.	129
managing	133
master VLAN list	128
overview	127
Port Configuration Area	132 , 138
port PVID configuration	138
port VLAN settings	137

Index

renaming	134
selecting ports	137
Selection List	131
synchronizing names	135
tags	128
tree	129
viewing configuration	129
viewing port VLAN configuration	137
VLAN tree	129

VoIP

configuring the engine	77
overview	77
QoS	79
Resources tab	78
RSVP	80
RTCP	80
status tab	81

VRRP

Global Parameters window	211
overview	211
Table window.	212

W

WAN

configuration	99
Dynamic CAC configuration	125

Web management

configuration	253
overview	253
starting.	20

Welcome screen

Backup Interface Wizard	120
Port Redundancy Wizard	157

Welcome to Avaya G430 Manager	13
---	--------------------

Window

ARP Table	191
cRTP interfaces	214
DHCP/BOOTP Global Parameters	196
DHCP/BOOTP Parameters	198
IP Global Parameters	181
IP Interfaces	182
IP Routing Table	186 , 189
IP Tunnel Table	193
OSPF Area Parameters	206
OSPF External Database	209
OSPF Global Parameters	203
OSPF Interfaces	204
OSPF Link State Database	207
OSPF Neighbors	210
Port RMON.	147
RIP Global Parameters	199
RIP Interfaces	200
Switch Connected Addresses	151
TCP header compression interfaces	216
VRRP Global Parameters	211

VRRP Table	212
Wizard	
Backup Interface	119
Port Mirroring	140
Port Redundancy	156

Z

Zooming in and out of the graph	148
---	---------------------