IP/MPLSView Web-Based Management and Monitoring Guide

Modified: 2018-07-06

Copyright © 2018, Juniper Networks, Inc.

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

IP/MPLSView Web-Based Management and Monitoring Guide
Copyright © 2018 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://www.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation . . . xvii
Documentation and Release Notes . . . xvii
Documentation Conventions . . . xvii
Documentation Feedback . . . xix
Requesting Technical Support . . . xx
Self-Help Online Tools and Resources . . . xx
Opening a Case with JTAC . . . xx

Chapter 1 Introduction . . . 23

IP/MPLSView Initial Landing Page Overview . . . 23
IP/MPLSView Main Window Overview . . . 25

Chapter 2 Network Topology Window . . . 27

IP/MPLSView Web Interface: Live Network Overview . . . 28
Network Topology Window Overview . . . 29
IP/MPLSView Main Window Tables . . . 30
Main Window Tables . . . 31
Main Window Node Table . . . 31
Main Window Link Table . . . 33
Main Window Tunnel Table . . . 36
Main Window SRLG Table . . . 38
Viewing Information About Devices and Links in the Network Topology . . . 40
Displaying Protocol Status . . . 44
Protocol Status . . . 44
Displaying Protocol Status for BGP Neighbors at Node . . . 45
Displaying Protocol Status for Tunnels at Node . . . 46
Displaying Historical Device Performance . . . 46
Historical Device Performance . . . 46
Displaying System Uptime for a Device . . . 47
Displaying Memory Usage for a Device . . . 47
Displaying Historical Network Performance . . . 48
Historical Network Performance . . . 48
Displaying Historical Network Performance for Ping . . . 49
Displaying Historical Network Performance for Advanced Ping . . . 51
Displaying Historical Network Performance for LSP Ping . . . 52
Displaying Historical Network Performance for SLAs . . . 53
Displaying Link Latency . . . 54

Chapter 3 Network Monitoring . . . 57

Nodes . . . 57
VPNs by VPN Types Using the Network Tab . . . 68
Network Dashboard . . . 73

Network Summary 74

Chapter 4 **Configuration Management 75**

Network Data 75
Network Reports 76
Understanding Network Reports 76
Displaying Network Reports 77
Integrity Check Reports 78
Hardware Inventory Reports 78
Understanding Hardware Inventory Reports 79
Displaying Hardware Inventory for Routers 80
Displaying Hardware Inventory for Line Cards 80
Displaying Hardware Inventory for Transceivers 81
Displaying Hardware Inventory for Extensive Parts List 81
Equipment View 82
Understanding the Equipment View 82
Displaying the Equipment View 84
Configuration Revision Manager 84
Understanding the Configuration Revision Manager 85
Displaying and Comparing Configuration Revisions 85
Device Library 86
Understanding the Device Library 86
Modifying a Web Image Icon 87
Modifying the CLI Template 88
Adding a New Hardware Type 89
Miscellaneous Reports 90

Chapter 5 **Fault Management: Events 93**

Live Event Browser 93
Launching the Live Event Browser 93
Acknowledging and Clearing Events 94
Creating a Group Event 95
Creating a New Query 96
Configuring the Severity Colors 97
Uploading Event Sound Clips 98
Stopping Event Sounds 99
Analyzing Events 100
Understanding Root Cause Analysis 100
Analyzing an Event 102
LSP and Related Tunnel Events for LinkDown and LinkUp 103
Correlation of Interface Index and Tunnel Index 103
Mapping the Interface Index to Interface Name 104
LSPs and Associated LSP Events 106
Displaying LSP Events During LinkDown 106
Historical Event Browser 107
Error and Discard Chart for Interface Threshold Events 110
Events Count Chart 111
Event Summary Reports 114
Event Options 116

 Copyright © 2018, Juniper Networks, Inc.

Chapter 6 Fault Management: Threshold Crossing Alerts 121
Understanding Threshold Crossing Alerts 121
Configuring Threshold Crossing Alerts 121
Threshold Editor Overview 121
Interpreting the Threshold Editor 122
Creating Threshold Crossing Alerts 124
Triggering Threshold Alarms 126
Defining Conditions and Rules 126
Displaying Threshold Crossing Alerts 130
Displaying Data Triggered Threshold Crossing Alerts 130
Displaying Interface Traffic Threshold Crossing Alerts 131
Displaying LSP Tunnel Traffic Threshold Crossing Alerts 132
Displaying Tunnel Events 134
Troubleshooting Threshold Crossing Alerts 135
Chapter 7 Performance Management 137
Understanding Live Traffic 137
Live Traffic 140
Displaying a Live Traffic Network Tunnel Chart 140
Displaying a Link Traffic Summary Report 141
Saving and Sharing a Live Traffic Report 142
Displaying a Router Ingress Interface Traffic Summary Report 143
Displaying a Router Ingress Tunnel Traffic Summary Report 144
Displaying LSP Bandwidth 145
Displaying a VPN Egress Traffic Summary Report 146
Aggregated Traffic Reports 147
Live VPN Traffic 148
Monitoring the Status of Your Network 149
Real-Time Network Status 150
Monitoring Real-Time Network Status 150
Monitoring Real-Time Status for LSPs (Tunnels) 151
Monitoring Real-Time Status for BGP Neighbors 152
Monitoring Real-Time Traffic and Device Performance 152
Real-Time Usage for Traffic and Device Performance 152
Monitoring Real-Time Usage for Link Traffic 153
Monitoring Real-Time Usage for Device Performance 154
Monitoring Any OID in Real Time 155
Real-Time Usage for Any OID 155
Monitoring Any OID Live 156
Diagnostics 157
Running the CLI 162
Running CLI Commands 163
Running CLI Commands on Multiple Devices 163
Displaying Collected Data from the Task Manager 165
Running Live Network Updates for Selected Devices 166
Diagnostic Manager 166
Understanding the Diagnostic Manager 167
Pinging from Device to Device 169
Pinging Multiple Devices from a Device 169

Copyright © 2018, Juniper Networks, Inc.

Pinging Multiple Devices from a Server . . . 171
Performing a Continuous Ping . . . 172
Running Traceroute from Device to Device . . . 172
Running Traceroute on Multiple Devices from a Device . . . 173
Pinging and Traceroute for Device Groups . . . 174
Pinging and Traceroute for a Customized Advanced Group . . . 175
Traffic Collection Manager . . . 178
Viewing Device Performance . . . 181
Viewing Network Performance . . . 185
Viewing Miscellaneous Reports and Charts . . . 187
Network Performance Data Chart Report . . . 188
Archived Reports . . . 189

Chapter 8 **Admin . . . 193**

Admin . . . 193
Understanding the Admin Menu . . . 193
Duplicating or Renaming an Existing Report Group . . . 194
Updating the GUI Login Policy . . . 195
Displaying Current Licenses . . . 196
Uploading a License . . . 196
Viewing Vendor Icons . . . 197
Viewing the User Activity Log . . . 197

Chapter 9 **Tools . . . 199**

Task Manager . . . 199
Understanding Task Manager . . . 199
Creating a New Task in Task Manager . . . 200
Managing Existing Tasks . . . 204
Performance Management Tasks Using Task Manager and Apache Spark Clusters . . . 205
Running a Task Using Spark Clusters . . . 207
MIB Browser . . . 210
Understanding the MIB Browser . . . 210
Viewing MIB Information . . . 211
Loading and Unloading MIB Subtrees . . . 211
Querying SNMP MIB Information from Network Devices . . . 212
Filtering the MIB Tree Display by Trap Numbers . . . 214
Modifying SNMP Trap Configuration Files . . . 215
Device Profiles . . . 218
Understanding Device Profiles . . . 218
Creating a New Device Profile . . . 219
Adding Devices to a Device Profile . . . 220
Modifying a Device Entry in a Profile . . . 221
Deleting an Entry in a Device Profile or a Device Profile . . . 221
Verifying Connectivity for One or More Devices in a Device Profile . . . 222
Populating a Device Profile . . . 224
Updating Device Profiles when Device Passwords are Changed . . . 228
Dual Routing Engine Support . . . 228
Inaccessible Nodes . . . 229
Syncing to the Master Profile . . . 229

 Copyright © 2018, Juniper Networks, Inc.

User Administration 230
Understanding User Administration 230
Creating User Groups and Assigning Permissions 231
Adding, Modifying, or Deleting Users 231
Defining Regions and Assigning Devices to Regions 232
Using the File Browser 233

Chapter 10 **Generating and Viewing Reports 235**

Network Reports 235
User Collected Data Report 236
Shared Reports 243
Shared Docs 244
Report Filters 244
Filtering by Device or Interface 244
Filtering for Group Sum Value 246

Copyright © 2018, Juniper Networks, Inc.

List of Figures

Chapter 1 **Introduction 23**

Figure 1: Initial Landing Page 23
Figure 2: Login Dialog Box 24
Figure 3: Main Window 24
Figure 4: Main Window 25

Chapter 2 **Network Topology Window 27**

Figure 5: IP/MPLSView Initial Landing Page 28
Figure 6: Main Window 29
Figure 7: Main Window Node Table 31
Figure 8: Node Details Window 32
Figure 9: Total Node Traffic Chart 33
Figure 10: Main Window Link Table 34
Figure 11: Link Details Window 35
Figure 12: Main Window Tunnel Table 36
Figure 13: Tunnel Details Window 37
Figure 14: Tunnel Traffic Chart 38
Figure 15: Main Window SRLG Table 39
Figure 16: Descriptive Pop-Up Window for Selected Link 40
Figure 17: Main Window Node Menu 41
Figure 18: Main Window Link Menu 41
Figure 19: Live Interface Traffic Chart 42
Figure 20: Run CLI Window for Selected Device 43
Figure 21: Traffic Chart for Selected Link 44
Figure 22: BGP Neighbors at Node 45
Figure 23: Tunnels at Node 46
Figure 24: Historical Device Performance Charts for System Uptime 47
Figure 25: Historical Device Performance Charts for Memory Usage 48
Figure 26: Select Destination Routers to Filter 50
Figure 27: Historical Device Performance Charts for Ping 50
Figure 28: Historical Device Performance Charts for Advanced Ping 51
Figure 29: Select Tunnels to Filter 52
Figure 30: Historical Device Performance Charts for LSP Ping 53
Figure 31: Historical Device Performance Charts for SLA 54
Figure 32: Historical Device Performance Charts for Link Latency 55

Chapter 3 **Network Monitoring 57**

Figure 33: Scheduling Live Network Collection Task Options 58
Figure 34: Traffic Collection Manager 59
Figure 35: Choose Collection Tables 59
Figure 36: Prepare Performance Data 60

Figure 37: Node Details 60
Figure 38: Node Interfaces 61
Figure 39: Interfaces Traffic Chart 62
Figure 40: Node Tunnels 63
Figure 41: Tunnels Traffic Chart 64
Figure 42: Node Performance 64
Figure 43: Node Actions 65
Figure 44: Sample Status Information 65
Figure 45: Execute CLI Command 66
Figure 46: Diagnostic Manager 67
Figure 47: Sample Jitter Information 68
Figure 48: VPNs by VPN Type 69
Figure 49: Detailed VPN Info 70
Figure 50: VPN Interface Traffic Chart 71
Figure 51: VPN Actions 73
Figure 52: Network Dashboard 73
Figure 53: Summary of Network Elements 74

Chapter 4 Configuration Management 75

Figure 54: Network Model Data 75
Figure 55: Network Config Data 76
Figure 56: User Collected Data 76
Figure 57: Network Summary Report 77
Figure 58: Integrity Check Reports 78
Figure 59: Hardware Inventory Reports for Devices 79
Figure 60: Hardware Inventory Report Window for Line Cards 80
Figure 61: Hardware Inventory Report Window for Transceivers 81
Figure 62: Hardware Inventory Report Window for Extensive Parts 82
Figure 63: Logical View 83
Figure 64: Tabular View 84
Figure 65: Revision Summary 85
Figure 66: Version Difference Comparison 86
Figure 67: Device Library Window 87
Figure 68: New Hardware Type 90
Figure 69: View VLANs 91
Figure 70: Tunnel Path Report 92
Figure 71: IP/Mac Address Report 92

Chapter 5 Fault Management: Events 93

Figure 72: Live Event Browser 94
Figure 73: Column Grouping Selector 96
Figure 74: Event Browser Options 98
Figure 75: Upload Sound Clip 99
Figure 76: Selection for Analyze Event 102
Figure 77: Root Cause Analysis Results 103
Figure 78: SNMP Trap Editor Trap Configuration Tab 104
Figure 79: SNMP Trap Editor Advanced Configuration Tab 105
Figure 80: SNMP Trap Editor Trap Attributes Tab 106
Figure 81: Show Impacted LSPs 107
Figure 82: Historical Event Queries and New Event Query Window 108

 Copyright © 2018, Juniper Networks, Inc.

Figure 83: Historical Event Browser Window 108
Figure 84: Error and Discard Chart 110
Figure 85: Event Count Chart Window 111
Figure 86: Event Count Chart Series 112
Figure 87: New Event Count Series Window 113
Figure 88: Select Severity Values Window 114
Figure 89: Event Dashboard 115
Figure 90: Event Summary by Severity 115
Figure 91: Event Summary by Event Type 115
Figure 92: Event Summary by Node 116
Figure 93: Edit Threshold Alarm for CPUStats 117
Figure 94: Condition and Rule Builder for CPUStats 118
Figure 95: Edit Event Subscription for Tunnel Util 119
Figure 96: Subscription Rule Builder for Tunnel Util 119

Chapter 6 Fault Management: Threshold Crossing Alerts 121

Figure 97: Threshold Editor 122
Figure 98: Threshold Editor Scope 123
Figure 99: Example Threshold Rule 124
Figure 100: Threshold Conditions and Rules Builder 126
Figure 101: Live Event View 130
Figure 102: Historical Device Performance Charts 131
Figure 103: Interface Traffic Chart 132
Figure 104: Tunnel Traffic Chart 133
Figure 105: Tunnel Events Viewer 134

Chapter 7 Performance Management 137

Figure 106: Live Traffic Window 138
Figure 107: Total Network Tunnel Traffic Chart 140
Figure 108: Link Traffic Summary Report 141
Figure 109: Save Shared Report 142
Figure 110: Router Ingress Interface Traffic Summary 143
Figure 111: Router Ingress Tunnel Traffic Summary 144
Figure 112: Tunnel Traffic Summary Report 145
Figure 113: LSP Bandwidth Chart 146
Figure 114: VPN Egress Traffic Summary Report 147
Figure 115: Live VPN Traffic 149
Figure 116: Live Status to Monitor Menu 150
Figure 117: Live Tunnel Status Window with Filtered Display 151
Figure 118: Live Tunnel Status Window with Filtered Display 151
Figure 119: Live BGP Neighbor Status Window 152
Figure 120: Parameter to Monitor Menu 153
Figure 121: Link Traffic Chart 154
Figure 122: Live Device Performance Chart Window 155
Figure 123: Inputs for Monitor Any OID Window 156
Figure 124: Monitor Any OID Chart Window from Template 157
Figure 125: Run CLI Window for Selected Device 158
Figure 126: Run CLI from Actions Tab of Node Info Pane 159
Figure 127: Ping Multiple Routers 160
Figure 128: Traceroute Output 162

Copyright © 2018, Juniper Networks, Inc.

Figure 129: Run CLI Window 164
Figure 130: Command Execution History and Output 164
Figure 131: Command Output Collected by Task Manager 165
Figure 132: Collection for Live Update 166
Figure 133: Diagnostic Manager Window 167
Figure 134: Ping Multiple Devices from Device 170
Figure 135: Example Traceroute Output for Device to Device 173
Figure 136: Diagnostic Device Group Window 175
Figure 137: Diagnostics Custom Group 176
Figure 138: Customized Advanced Group 177
Figure 139: Traffic Collection Manager and Router Groups 179
Figure 140: Choose Collection Tables 180
Figure 141: Traffic Collection Manager Collection Status 180
Figure 142: Traffic Collection Manager Profile Connectivity Test 181
Figure 143: CPU Load Report 182
Figure 144: CPU Load Chart 183
Figure 145: System Uptime Report 183
Figure 146: CPU Temperature Report 184
Figure 147: CPU Usage Report 184
Figure 148: Memory Usage Report 185
Figure 149: Ping Report 185
Figure 150: LSP Ping Report 186
Figure 151: SLA Report 186
Figure 152: Link Latency Report 187
Figure 153: Example of Archived Reports 191

Chapter 8 **Admin 193**

Figure 154: Administration Window for Removing Stale Tunnels 194
Figure 155: Administration Window for Creating a Duplicate Report Group 195
Figure 156: Administration Window for Updating the GUI Login Policy 195
Figure 157: Display Licenses 196
Figure 158: Upload License File 196
Figure 159: Vendor Icons 197
Figure 160: Viewing the User Activity Log 198

Chapter 9 **Tools 199**

Figure 161: Task Manager 200
Figure 162: Creating a New Task 201
Figure 163: Selecting the Devices for Collection 202
Figure 164: Scheduling the Task 203
Figure 165: Chained Scheduling Live Network Collection Task 204
Figure 166: Managing an Existing Task 205
Figure 167: New Task - Select Task Name and Task 207
Figure 168: New Task - Select Devices and Options for Collection 208
Figure 169: New Task - Schedule Task and Enable Spark 209
Figure 170: Task Status Results 210
Figure 171: MIB Browser with MIB Details 211
Figure 172: Gear Icon in MIB Browser 211
Figure 173: Server File Browser 212
Figure 174: MIB Browser Access Device Tab 213

 Copyright © 2018, Juniper Networks, Inc.

Figure 175: MIB Browser Retrieving All OIDs 214
Figure 176: MIB Browser Filtering by Trap Numbers 215
Figure 177: Modify SNMP Trap Config for bgpEstablished 215
Figure 178: SNMP Trap Editor Trap Configuration Tab 216
Figure 179: SNMP Trap Editor Advanced Configuration Tab 217
Figure 180: SNMP Trap Editor Trap Attributes Tab 218
Figure 181: Device Profiles Window 220
Figure 182: Modifying a Device Entry in a Profile 221
Figure 183: Profile Connectivity Window 222
Figure 184: Add New Device Access Parameters Window 225
Figure 185: Add New Device SNMP Parameters Window 227
Figure 186: User Administration User Groups 231
Figure 187: User Administration Modify User 232
Figure 188: User Administration Region Definitions 233
Figure 189: Server File Browser 234

Chapter 10 **Generating and Viewing Reports 235**

Figure 190: Node Discovery Report (Web Version) 236
Figure 191: User Collected Data Report 237
Figure 192: Report Details 237
Figure 193: Sample User Collected Data Report 239
Figure 194: Share Report Button 244
Figure 195: Shared Reports Page 244
Figure 196: Shared Documents 244
Figure 197: Filter by Device 245
Figure 198: Filter by Interface 246
Figure 199: Group Sum Value 247

Copyright © 2018, Juniper Networks, Inc.

Copyright © 2018, Juniper Networks, Inc.

List of Tables

About the Documentation xvii

Table 1: Notice Icons xviii
Table 2: Text and Syntax Conventions xviii

Chapter 1 Introduction 23

Table 3: Main Window Drop-down Menus 25

Chapter 2 Network Topology Window 27

Table 4: Main Window Node Table Columns 31
Table 5: Main Window Link Table Columns 34
Table 6: Main Window Tunnel Table Columns 36
Table 7: Main Window SRLG Table Columns 39
Table 8: Protocol Status Options 45
Table 9: Historical Device Performance Options 46
Table 10: Task Manager Tasks for Historical Network Performance 49

Chapter 3 Network Monitoring 57

Table 11: Node Details Tab Descriptions 60
Table 12: Node Interfaces Tab Descriptions 61
Table 13: Detailed Interface Information Descriptions 62
Table 14: Tunnels Information Descriptions 63
Table 15: Detailed Tunnel Information Descriptions 64
Table 16: Detailed Node VPN Types 69
Table 17: Detailed PE Node Information 70
Table 18: Interfaces 70
Table 19: Tunnels 72
Table 20: Actions 72

Chapter 4 Configuration Management 75

Table 21: Equipment View Descriptions 83
Table 22: CLI Template Keywords 88
Table 23: Text File Descriptions 89

Chapter 5 Fault Management: Events 93

Table 24: Historical Event Browser Table Columns 109

Chapter 6 Fault Management: Threshold Crossing Alerts 121

Table 25: Additional Examples 129

Chapter 7 Performance Management 137

Table 26: Default Color Codings 160
Table 27: Ping Results 161
Table 28: Multiple Ping Results 171

Table 29: IP/MPLSView Collection Tasks and Associated Archived Reports 190

Chapter 9 **Tools 199**

Table 30: Access Parameters in Add New Device Window 225
Table 31: SNMP Parameters in Add New Device Window 227

Chapter 10 **Generating and Viewing Reports 235**

Table 32: User Collected Data Report Settings 238
Table 33: Aggregate Method Report Results 239
Table 34: Aggregate Method Report Two-Hour Results 240
Table 35: Aggregate Method Report New-Value Results 240
Table 36: Aggregate Method Report Y Percentile Results 240
Table 37: Data Points to Time Intervals 242

 Copyright © 2018, Juniper Networks, Inc.

About the Documentation

- Documentation and Release Notes on page xvii
- Documentation Conventions on page xvii
- Documentation Feedback on page xix
- Requesting Technical Support on page xx

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

Documentation Conventions

Table 1 on page xviii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xviii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*

Copyright © 2018, Juniper Networks, Inc.

Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		static {
		route default {
		nexthop *address*;
		retain;
		}
		}
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at https://www.juniper.net/documentation/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/documentation/feedback/.

- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at https://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

Copyright © 2018, Juniper Networks, Inc.

For international or direct-dial options in countries without toll-free numbers, see https://www.juniper.net/support/requesting-support.html.

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 1

Introduction

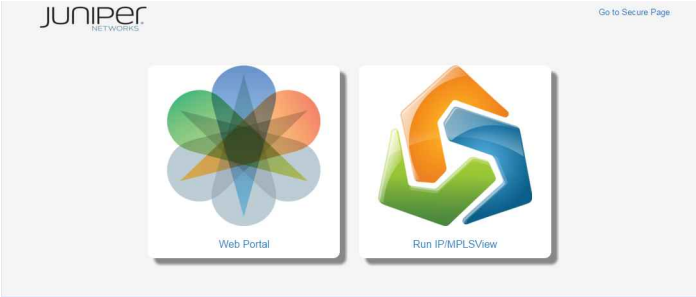
- IP/MPLSView Initial Landing Page Overview on page 23
- IP/MPLSView Main Window Overview on page 25

IP/MPLSView Initial Landing Page Overview

To access the IP/MPLSView user interface, type the host external IP address, followed by port number 8091 or 8443 in the address bar of your browser, for example, **http://192.168.153.29:8091**.

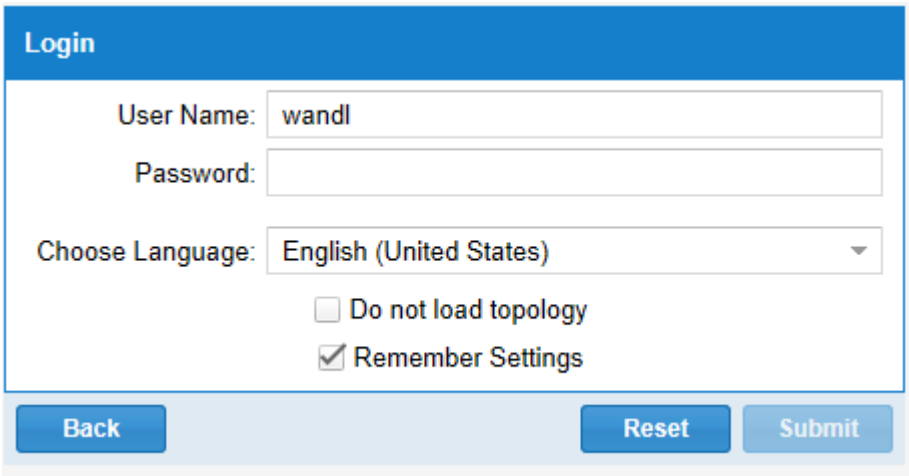
The initial landing page for IP/MPLSView is displayed. Figure 1 on page 23 shows the initial landing page.

Figure 1: Initial Landing Page



From the initial landing page, click **Web Portal**. The Login dialog box is displayed. Figure 2 on page 24 shows the Login dialog box.

Figure 2: Login Dialog Box

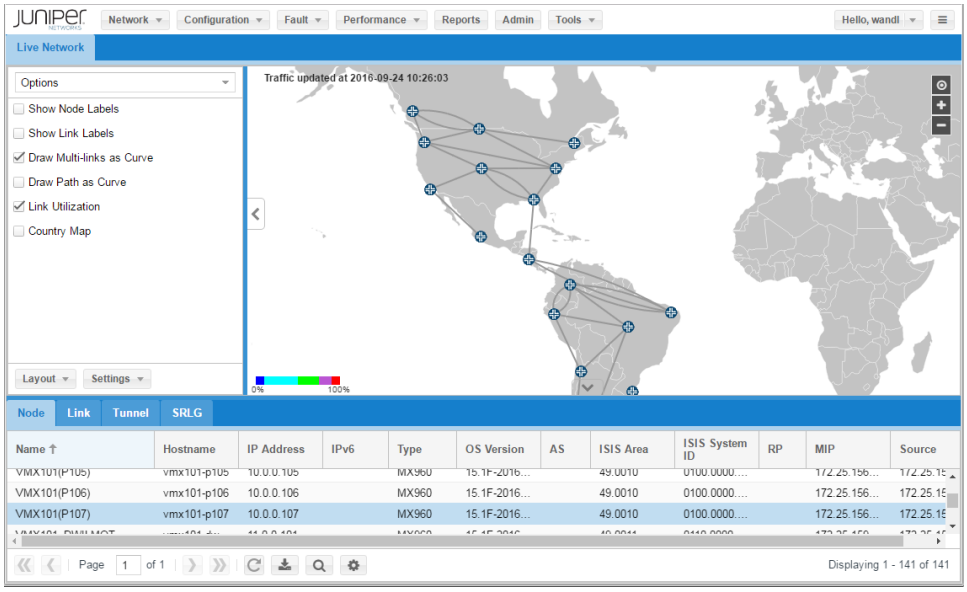


The default language is English (United States). To change the language the first time you log in, select **Choose Language > Chinese (Simplified)** or **Choose Language > Russian**. Select **Do not load topology** to not load the topology map. Select **Remember Settings** to save the selection.

Enter your login credentials and click **Submit** to display the main window of the IP/MPLSView Web interface. For information about the **Run IP/MPLSView** option, see the *IP/MPLSView Java-based Graphical User Interface Reference*.

Figure 3 on page 24 shows the main window of the IP/MPLSView Web interface.

Figure 3: Main Window



Related Documentation

- IP/MPLSView Main Window Overview on page 25

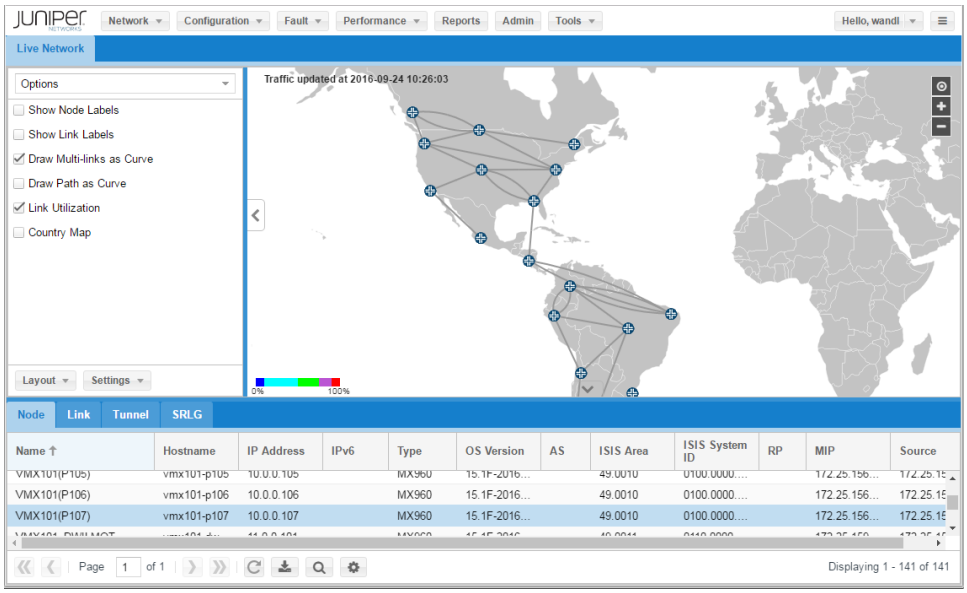
Copyright © 2018, Juniper Networks, Inc.

IP/MPLSView Main Window Overview

This topic describes the main window of the IP/MPLSView Web interface, the workspace from which all IP/MPLSView windows are launched or opened.

Figure 4 on page 25 shows the main window of the IP/MPLSView Web interface.

Figure 4: Main Window



The main window consists of the following elements: menus, topology map panes, and network information tables. Note that many functions and features do not become available until a network is loaded. Menu options may also vary depending on your license, user permissions, or modules.

Table 3 on page 25 describes each element in the main window.

Table 3: Main Window Drop-down Menus

Element Name	Description	Link to More Information
Topology Map	The topology map is a graphical representation of the baseline network. IP/MPLSView can display the topology in several views, depending on the network.	*Topology Map Window Overview* *Topology Map Right Pane*
Topology Map Left Pane	The left pane of the topology map contains expandable menus for filtering what is and is not displayed in the map. Menu selections include: Options, Types, Groups, Protocols, Events, AS, ISIS Areas, OSPF Areas, Links status, and Device/Network Performance.	*Topology Map Left Pane*
Network Menu	The Network menu provides comprehensive details on network elements, such as nodes, links, interfaces, and tunnels. Detailed information is available on services, protocols, and paths.	*Main Window Network Menu*

Copyright © 2018, Juniper Networks, Inc.

Table 3: Main Window Drop-down Menus (continued)

Element Name	Description	Link to More Information
Configuration Menu	The Configuration menu provides access to configuration files, network data, network reports, integrity check reports, and hardware inventory reports.	*Main Window Configuration Menu*
Fault Menu	The Fault menu provides access to the Event Browser, event summary reports, event charts, and event options.	*Main Window Fault Menu*
Performance Menu	The Performance menu provides access to traffic-related features such as live traffic, aggregated traffic, live VPN traffic, real-time status, real-time usage, the Traffic Collection Manager, device performance, network performance, diagnostics and reports.	*Main Window Performance Menu*
Reports Button	The Report menu is used to access the Report Manager which contains detailed network, tunnel, simulation, configuration, and user-customized reports.	*Main Window Reports Window*
Admin Button	The Admin button displays the Administration pane. From which you can access log files, login statistics, a system monitor, and release information. These functions are normally used by IP/MPLSView administrators.	*Main Window Admin Button*
Tools Menu	The Tools menu provides access to the Task Manager, MIB Browser, device profiles display, the User Administration functions and a file browser.	*Main Window Tools Menu*
Help-About Menu	Displays the About window. Displays the IP/MPLSView documentation Web page. Launches the IP/MPLSView client using Java WebStart technology.	*Main Window Hello Menu and Help-About Menu*
Network Node Table	Displays a list of the nodes in your network. Clicking on a node highlights it on the map.	*Main Window Node Table*
Network Link Table	Displays a list of links for the selected subview. Clicking on a link highlights it on the map.	*Main Window Link Table*
Network Tunnel Table	Displays the node name, IPv4 address, and IPv6 address for the node A and node Z endpoints of a tunnel.	*Main Window Tunnel Table*
Hello Menu Help-About Menu	Hello menu is used to logout. Help About menu is used to displays the software revision, license limits, license expiration date, and the licenses enabled. The Help About menus is used to launch the Java-based user interface.	*Main Window Hello Menu and Help-About Menu*

Related Documentation

- IP/MPLSView Initial Landing Page Overview on page 23

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 2

Network Topology Window

- IP/MPLSView Web Interface: Live Network Overview on page 28
- Network Topology Window Overview on page 29
- IP/MPLSView Main Window Tables on page 30
- Viewing Information About Devices and Links in the Network Topology on page 40
- Displaying Protocol Status on page 44
- Displaying Historical Device Performance on page 46
- Displaying Historical Network Performance on page 48
- Displaying Link Latency on page 54

Copyright © 2018, Juniper Networks, Inc.

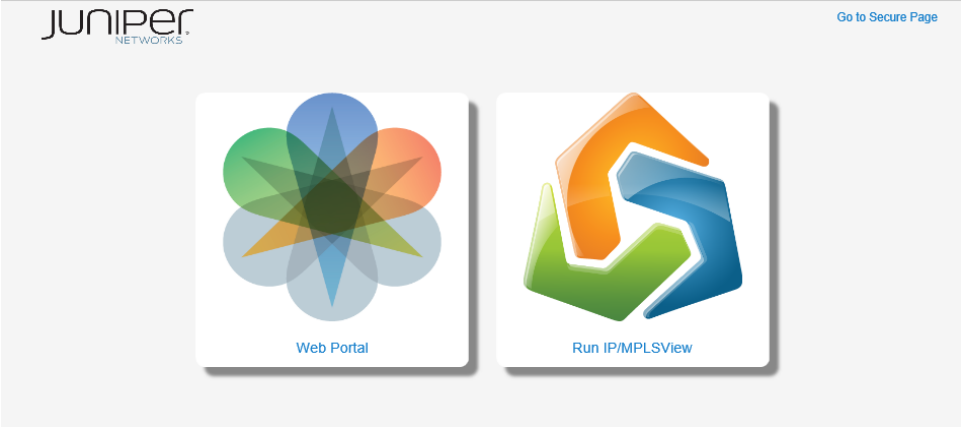
IP/MPLSView Web Interface: Live Network Overview

This chapter describes the functionality, reports, and information pertaining to the Live network that are viewable from the IP/MPLSView Web interface. In addition to Live network data, you can also view historical data from the IP/MPLSView Web.

To help you quickly find the information you need, this chapter contains sections on how to prepare the data, where applicable, describing the steps needed to make the network information available on the IP/MPLSView Web. If you only view data but are not responsible for generating the data, you can skip over these sections.

To access the Web interface, open your Web browser and navigate to http://<Your Server IP address>:8091, or https://<Your Server IP address>:8443 for secure login. You can use the IP/MPLSView client to launch the Java interface (see Figure 5 on page 28).

Figure 5: IP/MPLSView Initial Landing Page



Prior to beginning this task, you must have set up a profile for the network routers, scheduled live network collection, and scheduled traffic collection, as described in the *IP/MPLSView Java-Based Management and Monitoring Guide*.

Related Documentation

- Device Profiles on page 218
- Task Manager on page 199

Copyright © 2018, Juniper Networks, Inc.

Network Topology Window Overview

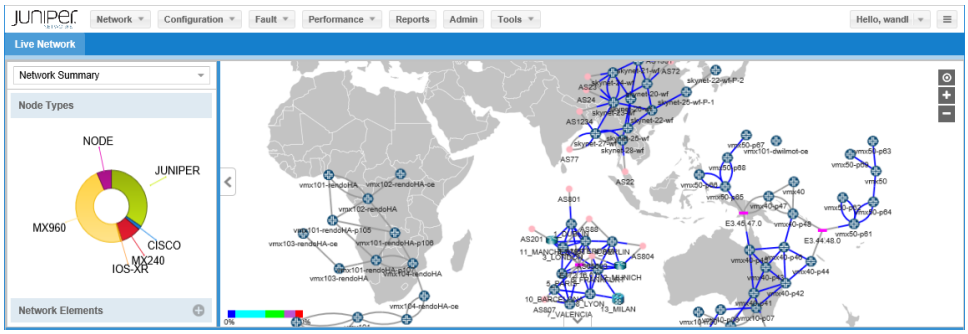
The topology in the main window provides various options for managing layout and settings. For example, you can group, ungroup, circle, and distribute selected nodes, or you can position the coordinates of the selected nodes by latitude and longitude. You can configure settings to display node and link labels by name, hostname, or IP address. You can also filter the network elements displayed in the topology by device vendors (types), groups, protocols, autonomous systems (ASs), IS-IS areas, OSPF areas, and link status.

You can conveniently launch various actions by right-clicking a device or link in the topology. For example, from a device, you can run CLI commands, view real-time CPU usage, perform a traceroute operation, or display real-time interface and tunnel traffic. From a link, you can poll real-time link traffic, display a link traffic chart, or display link status.

The network topology is the primary work area in IP/MPLSView and displays important link and node properties. The main window is divided into three panes: the left pane changes the settings of the topology, the right pane displays the network topology, and the bottom pane displays the tables for nodes (devices), links, tunnels, and interfaces.

Figure 6 on page 29 shows the topology.

Figure 6: Main Window



Selecting a network element (device or link) in the topology displays a description of the element in a pop-up window in the map pane. Right-clicking a device or link on the map opens a pop-up menu for more functions.

Links are color-coded according to a specified link property such as media type, trunk type, or vendor. By default, the links are displayed by link utilization. Alternatively, you can view links by other properties such as media, trunk type, vendor, or domain/area. Nodes are displayed as icons color-coded by vendor.

The network topology accessible from the IP/MPLSView Web interface supports the following features:

Detailed element information drill-down —Network menu

Customizable topology views for the live network—Topology

Heat map display—Topology

Time series correlation—Performance menu

Additional node information from collected data—Fault menu, Tools menu

Device performance data—Performance menu, Tools menu

Traffic information for a link—Fault menu, Performance menu

Link latency—Right-click link in Topology

Sub-views for protocols and tunnels—Network menu, right-click device or link in Topology

Retrieved protocol status—Network menu, right-click device in Topology

Retrieved historical network and device performance—Right-click device in Topology

CLI commands launched from the topology window show the device configuration—Right-click device in Topology, Performance menu

Ping diagnostics—Performance menu

Path highlighting—Select from node, link, tunnel or SRLG tables in main window

The tables for nodes (devices), links, tunnels, and interfaces interact with the network topology and respond to your actions. For example, when you right-click a device on the topology and select **Interfaces at Node** from the pop-up menu, the interfaces table displays the interfaces that originate at the selected device.

Related Documentation

- Viewing Information About Devices and Links in the Network Topology on page 40
- IP/MPLSView Main Window Tables on page 30

IP/MPLSView Main Window Tables

- Main Window Tables on page 31
- Main Window Node Table on page 31
- Main Window Link Table on page 33
- Main Window Tunnel Table on page 36
- Main Window SRLG Table on page 38

Copyright © 2018, Juniper Networks, Inc.

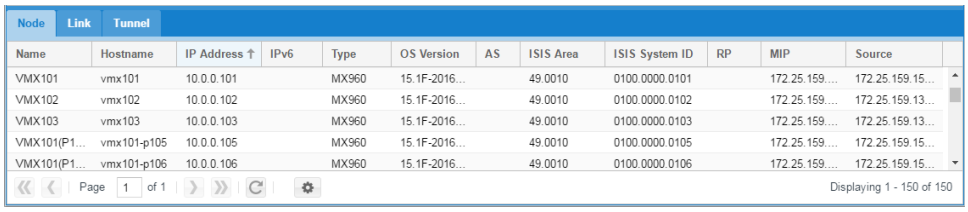
Main Window Tables

The IP/MPLSView main window has network information tables that contain detailed information about nodes, links, tunnels, and shared risk link groups (SRLGs).

Main Window Node Table

Figure 7 on page 31 shows the main window node table.

Figure 7: Main Window Node Table



Each column head has a menu. From the menu within each column, the element information can be sorted in ascending or descending order. You can select which columns are displayed or hidden. Columns can also be resized and the order can be rearranged.

Table 4 on page 31 describes the node table columns.

Table 4: Main Window Node Table Columns

Column Name	Description
Name	Displays the name of the node. If the node is a logical system configured on a physical device, the logical system name is displayed in parenthesis.
Hostname	Displays the name of the node. If the node is a logical system configured on a physical device, the logical system name is hyphenated.
IP Address	Displays the IPv4 address of the node.
IPv6	Displays the IPv6 address of the node, if configured.
Type	Displays the name of the node vendor.
OS Version	Displays the release number of the node operating system.
AS	Displays the BGP autonomous system number of the node, if configured.
ISIS Area	Displays the IS-IS area number of the node, if configured.
ISIS System ID	Displays the IS-IS system identifier number of the node, if configured.
RP	Displays the IPv4 address of the multicast rendezvous point (RP).
MIP	Displays the management IP (MIP) address, if configured. This is the IP address that was used from the router profile to collect information for this router.

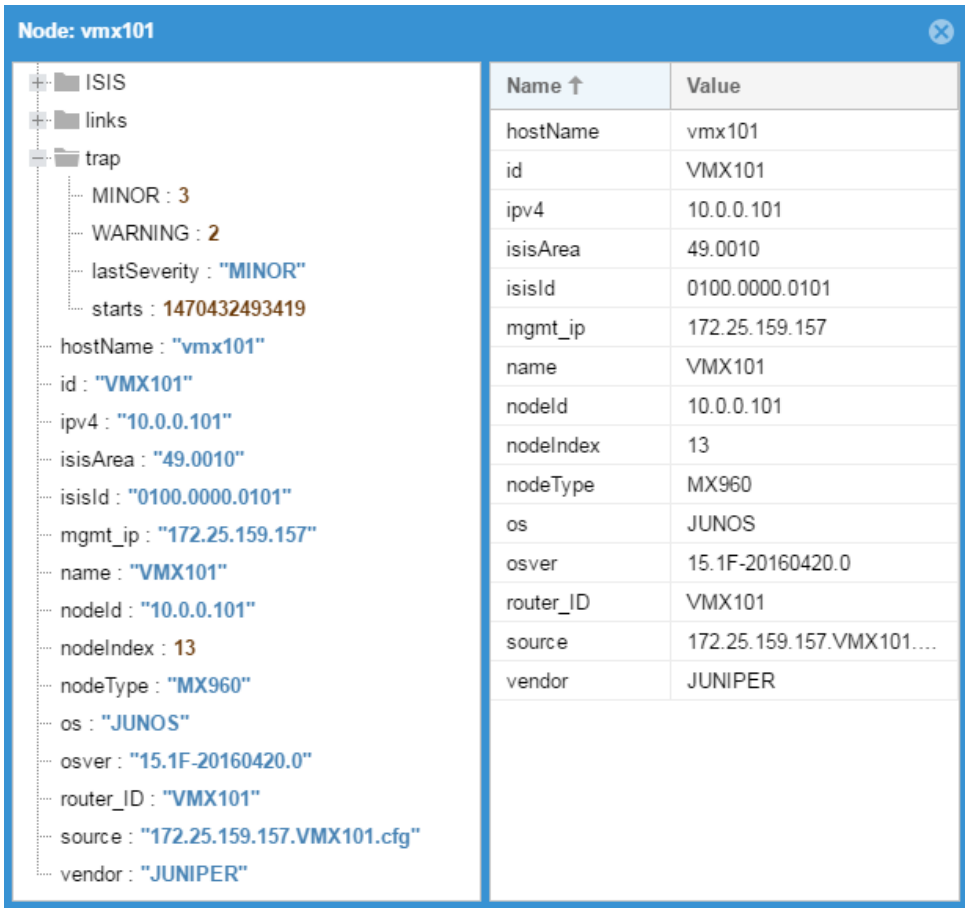
Copyright © 2018, Juniper Networks, Inc.

Table 4: Main Window Node Table Columns (continued)

Column Name	Description
Source	Displays the source of the information displayed in the table. This might be the filename of the node configuration file (172.25.159.157.VMX101.cfg) or the SNMP host discovery file (172.25.159.157.snmp).

Double-click a node in the table to display the node details window. Figure 8 on page 32 shows the node details window.

Figure 8: Node Details Window

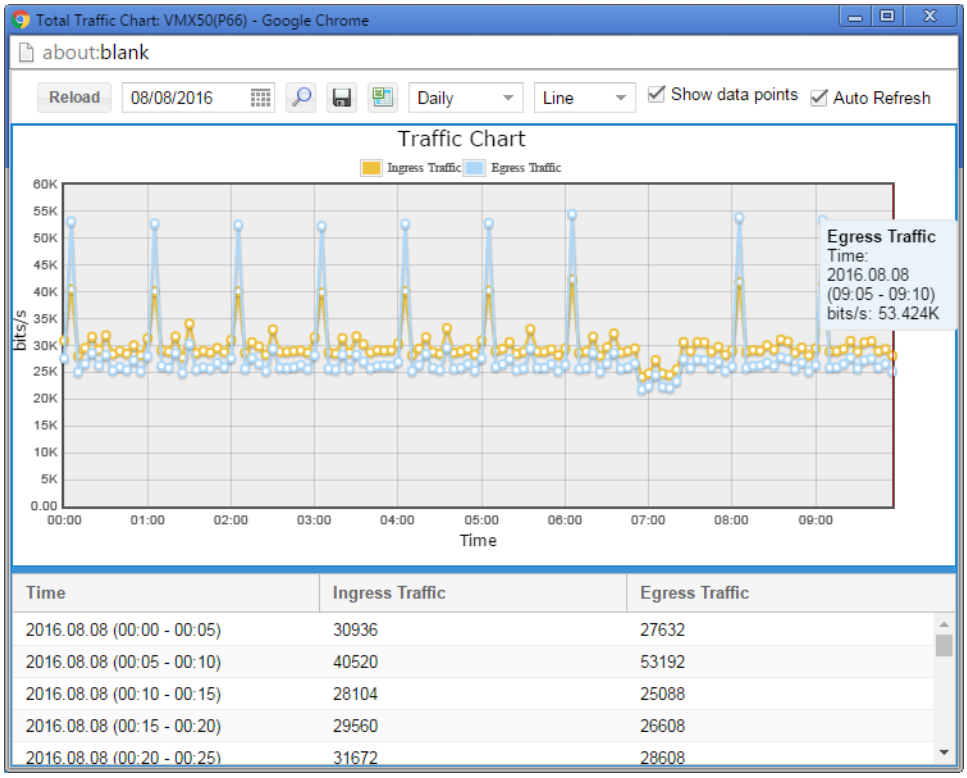


Expand the lists in the left pane to display additional information about the protocols, links, and trap events configured on or associated with this node. Select the information in the left pane to display that same information in the right pane. This is useful when there are multiple elements, such as protocols, displayed in the left pane.

Select a node in the table, right-click, and select **Display Total Traffic Chart** to display the total node traffic chart. Figure 9 on page 33 shows the total node traffic chart for both ingress traffic and egress traffic.

Copyright © 2018, Juniper Networks, Inc.

Figure 9: Total Node Traffic Chart



In the chart window, you can use the controls at the top of the window to reload the chart, select the date, reset the zoom, save the chart as an image, export to Excel, select the chart time period, select the chart style, show or hide the data points, and enable automatic refresh. Hold your mouse pointer over a data point to display a pop-up pane that shows the time and traffic value. Drag your mouse over a section of the chart to zoom in.

The table in the lower pane displays the time the traffic sample was taken and the bits per second reported for the sample.

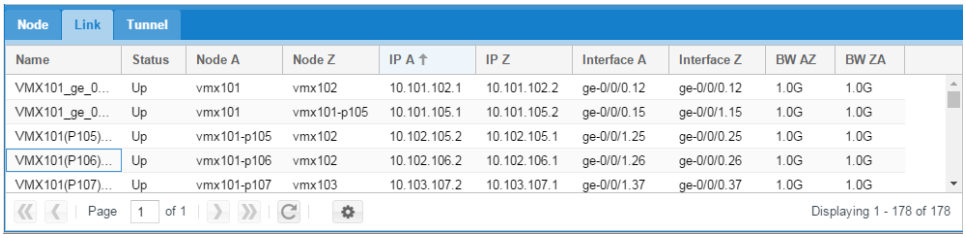
See Also

- *Topology Map Window Overview*

Main Window Link Table

Figure 10 on page 34 shows the main window link table.

Figure 10: Main Window Link Table



Each column head has a menu. From the menu within each column, the element information can be sorted in ascending or descending order. You can select which columns are displayed or hidden. Columns can also be resized and the order can be rearranged.

Table 5 on page 34 describes the link table columns.

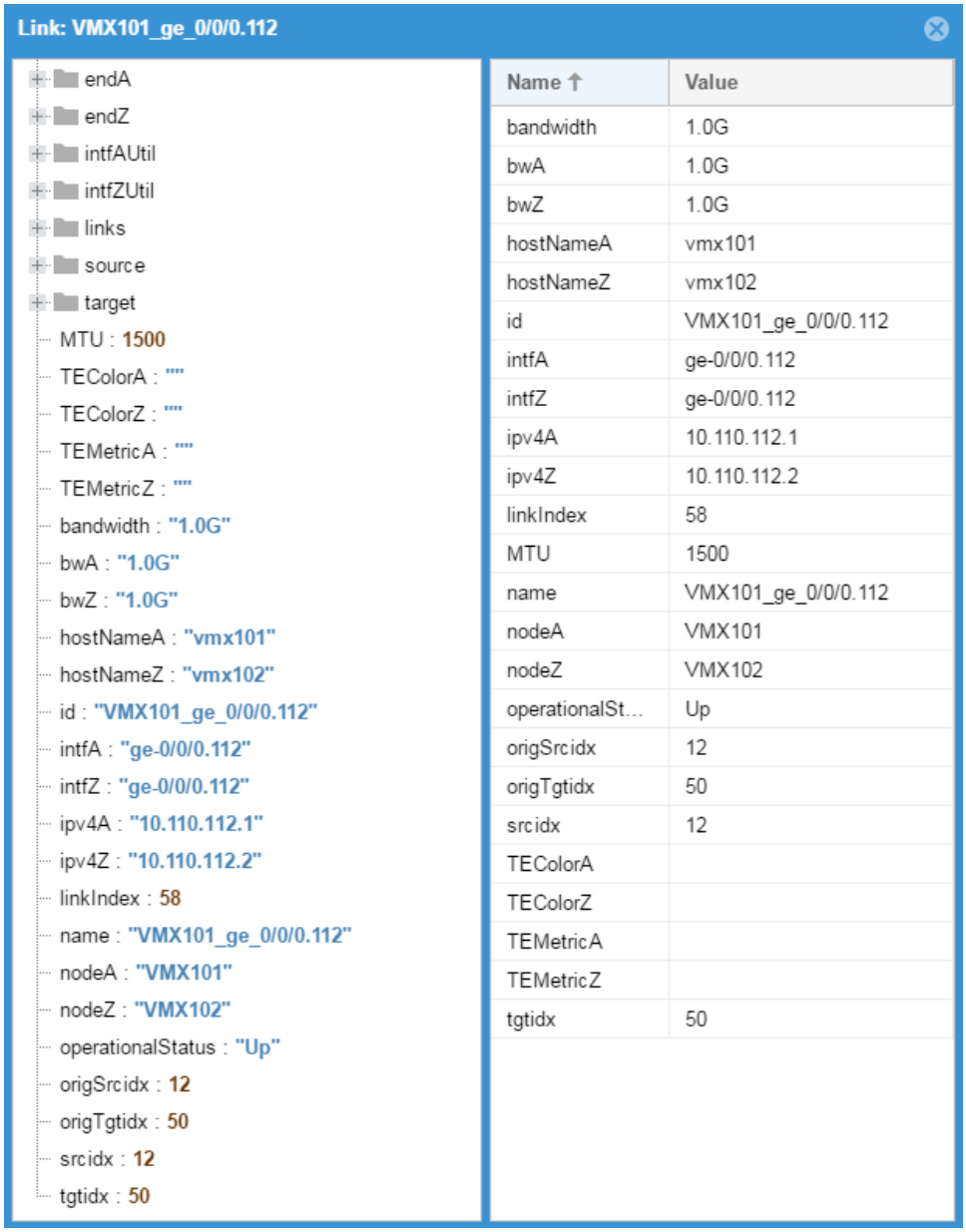
Table 5: Main Window Link Table Columns

Column Name	Description
Name	Name of the link.
Status	Status of the link.
Node A	Name of node A at one end of the link.
Node Z	Name of node Z at one end of the link.
IP A	IP address of node A at one end of the link.
IP Z	IP address of node Z at one end of the link.
Interface A	Physical and logical interface on node A at one end of the link.
Interface Z	Physical and logical interface on node Z at one end of the link.
BW AZ	Allocated bandwidth from node A to node Z.
BW ZA	Allocated bandwidth from node Z to node A.
MTU	Maximum transmission unit. Size in bytes of the largest protocol data unit that can be passed on in a link. The standard MTU for an Ethernet link is 1500.
Util AZ	Utilization from node A to node Z.
Util ZA	Utilization from node Z to node A.

Double-click a link in the table to display the link details window. Figure 11 on page 35 shows the link details window.

Copyright © 2018, Juniper Networks, Inc.

Figure 11: Link Details Window



Expand the lists in the left pane to display additional information about the interface the link is coming from (endA), the interface the link is going to (endZ), the interface utilization at each end of the link, the node the link is coming from, and the node the link is going to. Select the information in the left pane to display that same information in the right pane. This is useful when there are multiple elements, such as links, displayed in the left pane.

See Also

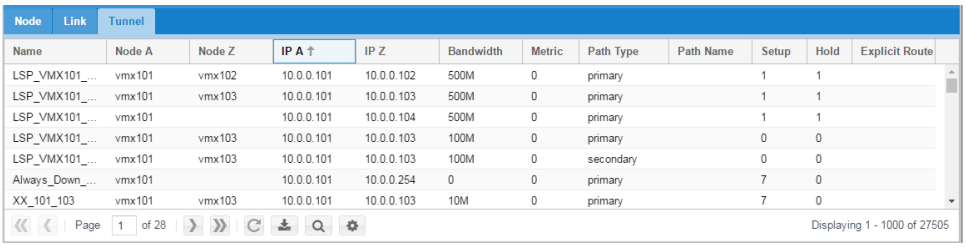
- *Topology Map Window Overview*
- *Main Window Node Table*

- *Main Window Tunnel Table*

Main Window Tunnel Table

Figure 12 on page 36 shows the main window tunnel table.

Figure 12: Main Window Tunnel Table



Node | Link | Tunnel

Name	Node A	Node Z	IP A	IP Z	Bandwidth	Metric	Path Type	Path Name	Setup	Hold	Explicit Route
LSP_VMX101_...	vmx101	vmx102	10.0.0.101	10.0.0.102	500M	0	primary		1	1	
LSP_VMX101_...	vmx101	vmx103	10.0.0.101	10.0.0.103	500M	0	primary		1	1	
LSP_VMX101_...	vmx101		10.0.0.101	10.0.0.104	500M	0	primary		1	1	
LSP_VMX101_...	vmx101	vmx103	10.0.0.101	10.0.0.103	100M	0	primary		0	0	
LSP_VMX101_...	vmx101	vmx103	10.0.0.101	10.0.0.103	100M	0	secondary		0	0	
Always_Down_...	vmx101		10.0.0.101	10.0.0.254	0	0	primary		7	0	
XX_101_103	vmx101	vmx103	10.0.0.101	10.0.0.103	10M	0	primary		7	0	

Page 1 of 28 Displaying 1 - 1000 of 27505

Each column head has a menu. From the menu within each column, the element information can be sorted in ascending or descending order. You can select which columns are displayed or hidden. Columns can also be resized and the order can be rearranged.

Table 6 on page 36 describes the tunnel table columns.

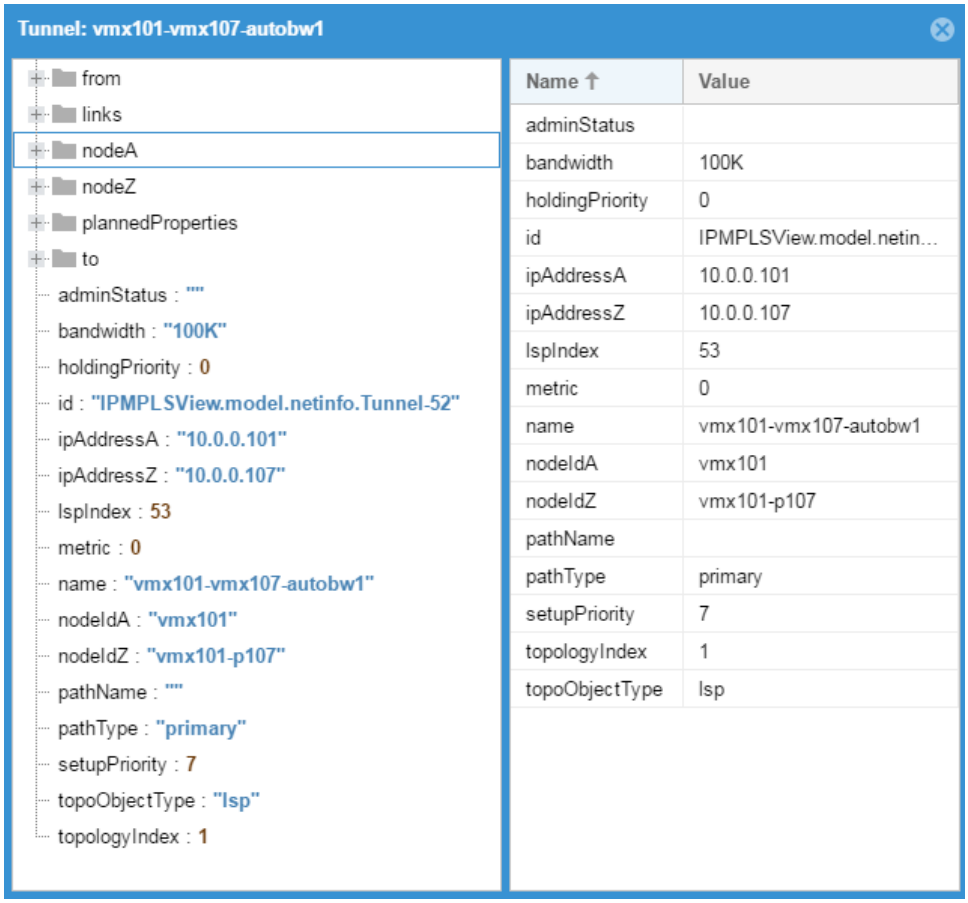
Table 6: Main Window Tunnel Table Columns

Column Name	Description
Name	Name of the tunnel.
Node A	Name of node A at one end of the tunnel.
Node Z	Name of node Z at one end of the tunnel.
IP A	IP address of node A at one end of the tunnel.
IP Z	IP address of node Z at one end of the tunnel.
Bandwidth	Bandwidth required by the tunnel.
Metric	The routing tunnel metric.
Path Type	Type of path: Primary, Secondary, or Standby.
Path Name	Path name, if configured.
Setup	RSVP setup priority for the tunnel traffic.
Hold	RSVP hold priority for the tunnel traffic.
Explicit Route	RSVP explicit route object for the tunnel, if configured.

 Copyright © 2018, Juniper Networks, Inc.

Double-click a tunnel in the table to display the tunnel details window. Figure 13 on page 37 shows the tunnel details window.

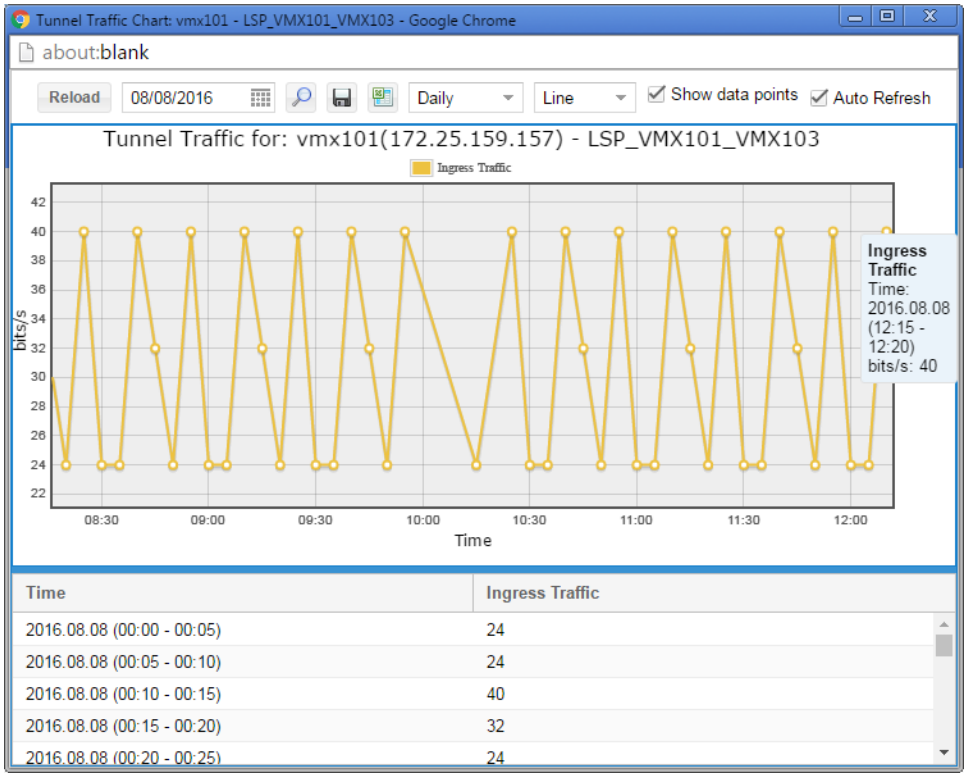
Figure 13: Tunnel Details Window



Expand the lists in the left pane to display additional information about the node the link is coming from, node the link is going to, IPv4 address, nodeA and nodeZ at each end of the tunnel, and the planned tunnel properties. Select the information in the left pane to display that same information in the right pane. This is useful when there are multiple elements, such as links, displayed in the left pane.

Select a tunnel in the table, right-click and select **Display Tunnel Traffic Chart** to display the tunnel traffic chart. Figure 14 on page 38 shows the tunnel traffic chart for ingress traffic.

Figure 14: Tunnel Traffic Chart



In the chart window, you can use the controls at the top of the window to reload the chart, select the date, reset the zoom, save the chart as an image, export to Excel, select the chart time period, select the chart style, show or hide the data points, show bandwidth (if configured), and enable automatic refresh. Hold your mouse pointer over a data point to display a pop-up pane that shows the time and traffic value. Drag your mouse over a section of the chart to zoom in.

See Also

- *Node Menu*
- *Node Menu Tunnels at Node*
- *Node Menu Interfaces at Node*

Main Window SRLG Table

Identifying SRLGs is important when planning MPLS label-switched path (LSP) diversity.

Figure 15 on page 39 shows the main window SRLG table, the SRLG details window, and the SRLG links highlighted in the topology map.

Copyright © 2018, Juniper Networks, Inc.

Figure 15: Main Window SRLG Table

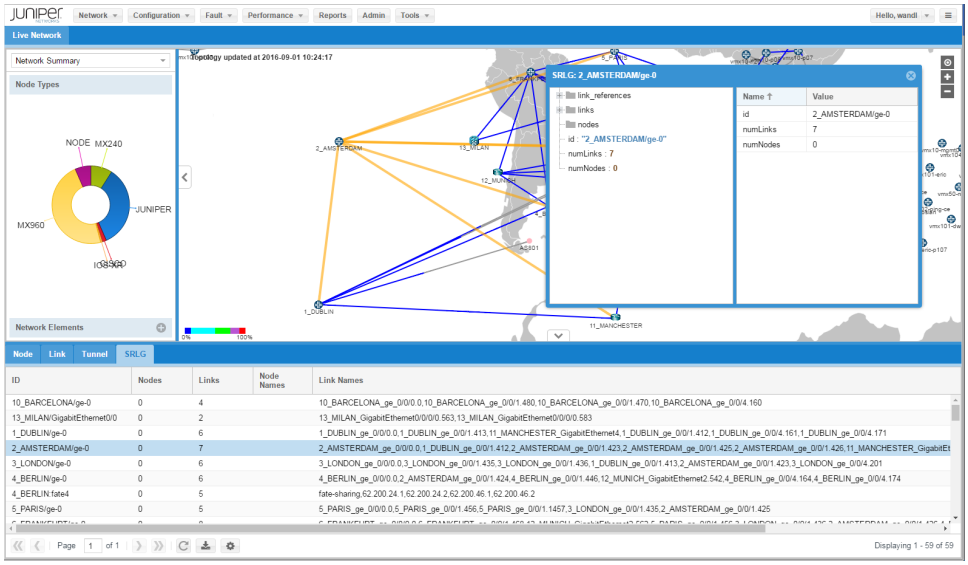


Table 7 on page 39 describes the SRLG table columns.

Table 7: Main Window SRLG Table Columns

Column Name	Description
ID	Identifier of the SRLG. For SRLGs created automatically, the name is derived from the node name and common part of the interface names. If you create the SRLGs, you configure the name.
Nodes	Number of nodes. SRLGs created automatically do not include the nod and the display is 0. SRLGs created manually might include nodes and links.
Links	Number of links that are in the shared risk group.
Node Names	The name of the node in manually created SRLGs.
Link Names	Name of the links that are in the shared risk group.

Double-click the SRLG identifier. An SRLG detail window is displayed, and the SRLG links are highlighted in the topology map.

In the SRLG details window, expand the lists to display information such as the name of the links, the protocols configured on the links, and the RSVP bandwidth on the source node and the target (destination) nodes at each end of the links.

See Also

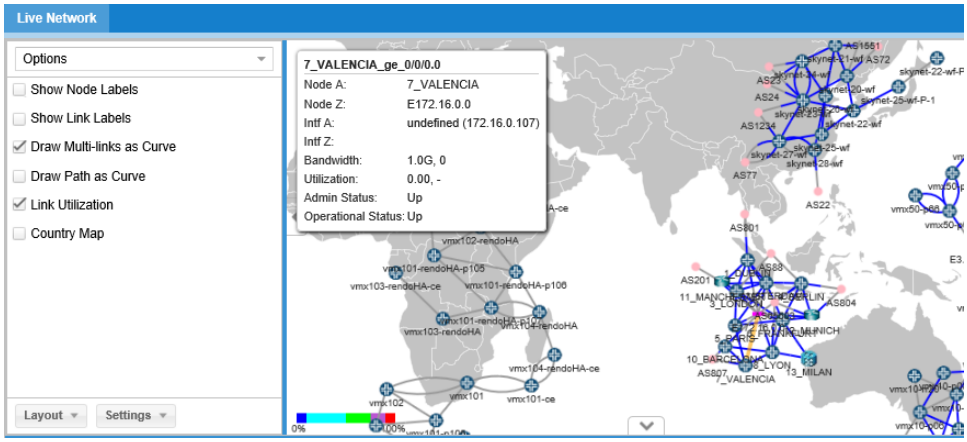
- *Topology Map Window Overview*
- *Main Window Tunnel Table*

Viewing Information About Devices and Links in the Network Topology

When you select (click) or right-click a network element on the network topology in the IP/MPLSView Web interface, you can launch a variety of associated actions to monitor these network elements.

When you select a network element (device or link) in the topology, a window is displayed with a description of the element. For example, Figure 16 on page 40 shows the topology with a window that displays the key properties of the Gigabit Ethernet link between devices 8_LYON and 10_BARCELONA.

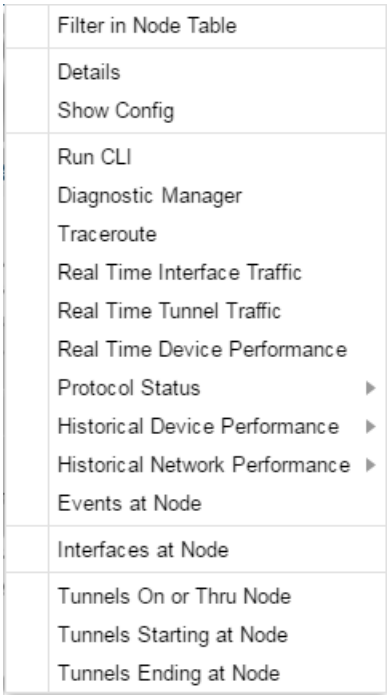
Figure 16: Descriptive Pop-Up Window for Selected Link



When you right-click a device (sometimes referred to as a node) in the topology, you can select any of the actions shown in the Node menu inFigure 17 on page 41.

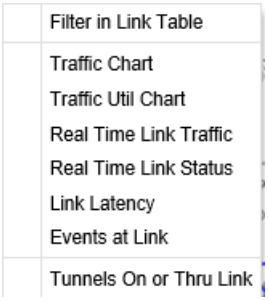
Copyright © 2018, Juniper Networks, Inc.

Figure 17: Main Window Node Menu



When you right-click a link in the topology, you can select any of the following actions from the Link menu shown in Figure 18 on page 41.

Figure 18: Main Window Link Menu



The following procedures show how to launch a few of the associated actions from the network topology by right-clicking a device or link.

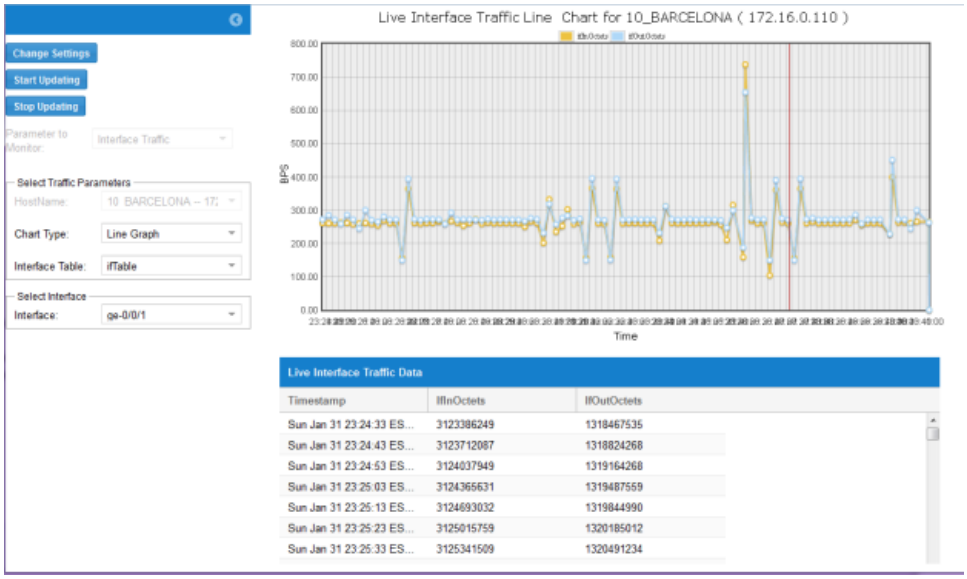
To view real-time interface traffic for a device:

1. Right-click the device on the network map.

2. Select **Real Time Interface Traffic** from the menu.

   The Live Interface Traffic Chart for the selected device is displayed.

Figure 19: Live Interface Traffic Chart



The upper pane shows the ingress and egress traffic charts. The bottom pane lists the traffic values for each data point time. Hold your mouse pointer over a data point to display a pane that shows the time and traffic value.

To run CLI statements for a device:

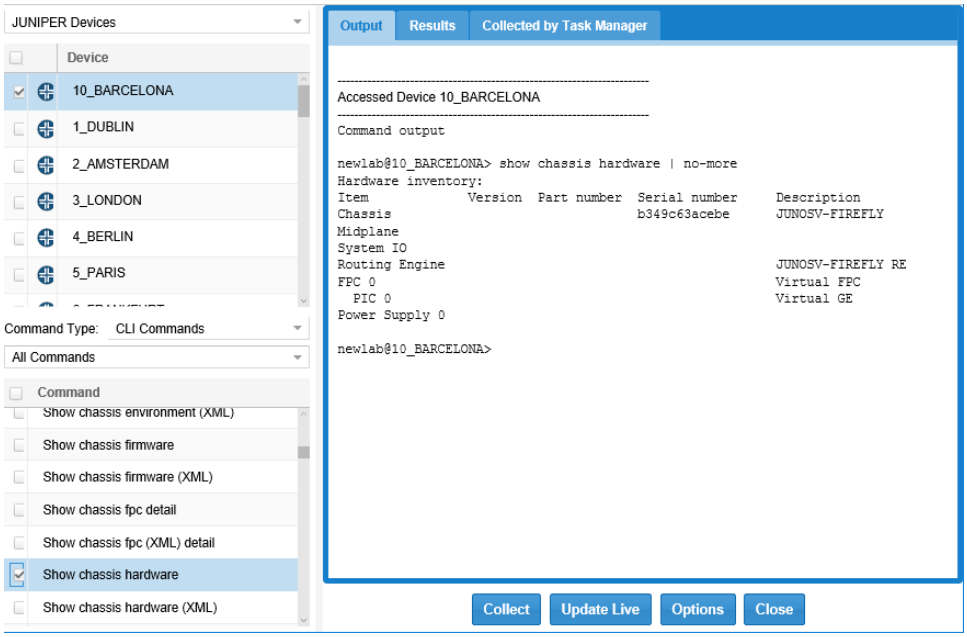
1. Right-click the device on the network map.

2. Select **Run CLI** from the menu.

   The Run CLI window is displayed for the selected device.

Copyright © 2018, Juniper Networks, Inc.

Figure 20: Run CLI Window for Selected Device



3. In the CLI Commands pane, navigate to and select the CLI command you want to run.

4. Click **Collect**, and then click **Run CLI**.

   The output of the command you selected appears in the Output pane.

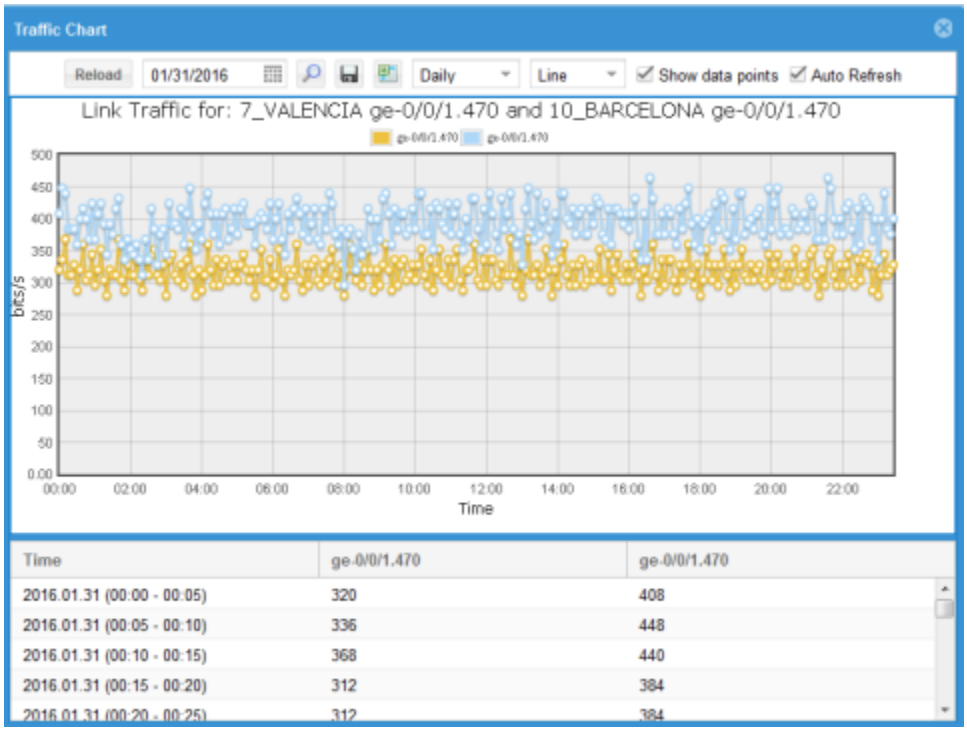
To display a traffic chart for a link:

1. Right-click the link for which you want to display the traffic chart.

2. Select **Traffic Chart** from the pop-up menu.

   The Link Traffic Chart for the selected link is displayed.

Figure 21: Traffic Chart for Selected Link



The upper pane shows the ingress and egress traffic charts. The bottom pane lists the traffic values for each data point time. You can use the controls at the top of the window to reload the chart, select the day, week, month, or year, reset the zoom, save the chart as an image, export to Excel, select the time period, select the chart style, show or hide the data points, and enable auto refresh. Hold your mouse pointer over a data point to display a pane that shows the time and traffic value.

Related Documentation

- Network Topology Window Overview on page 29

Displaying Protocol Status

- Protocol Status on page 44
- Displaying Protocol Status for BGP Neighbors at Node on page 45
- Displaying Protocol Status for Tunnels at Node on page 46

Protocol Status

The Protocol Status menu retrieves protocol status for the selected node and displays information by using the available network routing protocols.

To prepare the protocol status data, select **Tools > Task Manager > Scheduling Live Network Collection**. Schedule and run this task to collect the network topology data, including nodes, links, tunnels, and configured paths.

Copyright © 2018, Juniper Networks, Inc.

Table 8 on page 45 lists and describes the menu options.

Table 8: Protocol Status Options

Menu Item	Description
BGP Neighbors at Node	Polls the BGP MIB for the selected node, and reports status data in a table. For example, data includes the name of the node that is the BGP speaker, the interface used to establish the neighbor peer session, the IP address of the node that is the BGP neighbor node, the autonomous system numbers of nodes, and the status of the peer relationship.
Tunnels at Node	All tunnels from the node are displayed, along with the tunnel information. For example, data includes the name of the tunnel, the names and IP addresses of nodes at each end of the tunnel, the tunnel role, the operational status, and the tunnel up time.
OSPF Neighbors at Node	Displays the OSPF neighbors at the selected node and polls the OSPF MIB. For example, data includes the OSPF router ID of the node, the interface used to establish the OSPF neighbor adjacency, the name of the node that is the OSPF neighbor, the OSPF priority used, and the state of OSPF neighbor adjacency.
ISIS Adjacencies at Node	Displays the IS-IS adjacencies for the selected node. For example, data includes the IS-IS system ID of the node, the interface used to establish the IS-IS neighbor adjacency, the name of the node that is the IS-IS neighbor, the interface on the neighbor node used to establish the IS-IS neighbor adjacency, the state of the IS-IS neighbor adjacency, and the adjacency type.

See Also

- *Scheduling Live Network Collection*

Displaying Protocol Status for BGP Neighbors at Node

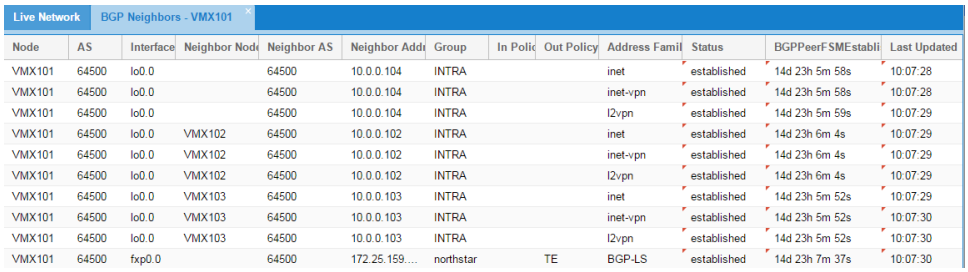
To display the protocol status for BGP neighbors at node:

1. Right-click the device on the network map.

2. Select **Protocol Status > BGP Neighbors at Node**.

   The BGP neighbors status for the selected node is displayed.

Figure 22: BGP Neighbors at Node



Live Network | BGP Neighbors - VMX101

Node	AS	Interface	Neighbor Node	Neighbor AS	Neighbor Addr	Group	In Polic	Out Policy	Address Famil	Status	BGPPeerFSMEstabli	Last Updated
VMX101	64500	lo0.0		64500	10.0.0.104	INTRA			inet	established	14d 23h 5m 58s	10:07:28
VMX101	64500	lo0.0		64500	10.0.0.104	INTRA			inet-vpn	established	14d 23h 5m 58s	10:07:28
VMX101	64500	lo0.0		64500	10.0.0.104	INTRA			l2vpn	established	14d 23h 5m 59s	10:07:29
VMX101	64500	lo0.0	VMX102	64500	10.0.0.102	INTRA			inet	established	14d 23h 6m 4s	10:07:29
VMX101	64500	lo0.0	VMX102	64500	10.0.0.102	INTRA			inet-vpn	established	14d 23h 6m 4s	10:07:29
VMX101	64500	lo0.0	VMX102	64500	10.0.0.102	INTRA			l2vpn	established	14d 23h 6m 4s	10:07:29
VMX101	64500	lo0.0	VMX103	64500	10.0.0.103	INTRA			inet	established	14d 23h 5m 52s	10:07:29
VMX101	64500	lo0.0	VMX103	64500	10.0.0.103	INTRA			inet-vpn	established	14d 23h 5m 52s	10:07:30
VMX101	64500	lo0.0	VMX103	64500	10.0.0.103	INTRA			l2vpn	established	14d 23h 5m 52s	10:07:30
VMX101	64500	fxp0.0		64500	172.25.159....	northstar		TE	BGP-LS	established	14d 23h 7m 37s	10:07:30

See Also

- Displaying Historical Device Performance on page 46
- Displaying Historical Network Performance on page 48
- Displaying Link Latency on page 54

Displaying Protocol Status for Tunnels at Node

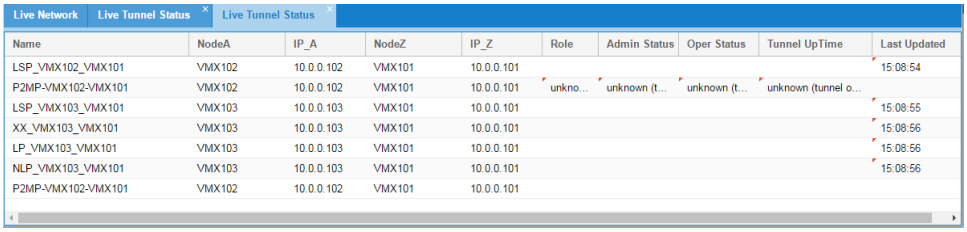
To display the protocol status for tunnels at node:

1. Right-click the device on the network map.

2. Select **Protocol Status > Tunnels at Node**.

   The tunnel status for the selected node is displayed.

Figure 23: Tunnels at Node



Live Network | Live Tunnel Status | Live Tunnel Status

Name	NodeA	IP_A	NodeZ	IP_Z	Role	Admin Status	Oper Status	Tunnel UpTime	Last Updated
LSP_VMX102_VMX101	VMX102	10.0.0.102	VMX101	10.0.0.101					15:08:54
P2MP-VMX102-VMX101	VMX102	10.0.0.102	VMX101	10.0.0.101	unkno...	unknown (t...	unknown (t...	unknown (tunnel o...	
LSP_VMX103_VMX101	VMX103	10.0.0.103	VMX101	10.0.0.101					15:08:55
XX_VMX103_VMX101	VMX103	10.0.0.103	VMX101	10.0.0.101					15:08:56
LP_VMX103_VMX101	VMX103	10.0.0.103	VMX101	10.0.0.101					15:08:56
NLP_VMX103_VMX101	VMX103	10.0.0.103	VMX101	10.0.0.101					15:08:56
P2MP-VMX102-VMX101	VMX102	10.0.0.102	VMX101	10.0.0.101					

See Also

- Displaying Historical Device Performance on page 46
- Displaying Historical Network Performance on page 48
- Displaying Link Latency on page 54

Displaying Historical Device Performance

- Historical Device Performance on page 46
- Displaying System Uptime for a Device on page 47
- Displaying Memory Usage for a Device on page 47

Historical Device Performance

Historical device performance can monitor options from the selected node.

Table 9 on page 46 lists and describes the menu options.

Table 9: Historical Device Performance Options

Menu Item	Description
System Uptime	Displays the system uptime availability.
CPU Usage	Displays CPU utilization.
CPU Temperature	Displays the operating CPU temperature.
Memory Usage	Shows memory used, total memory, and memory utilization.

Copyright © 2018, Juniper Networks, Inc.

To prepare the historical device performance data, select **Tools > Task Manager > Device SNMP Collection**. Schedule and run the task periodically for the device profile containing the devices for which device performance data needs to be collected. The Device SNMP Collection task should be set up to collect CPU usage, CPU temperature, memory usage, and system uptime.

See Also

- *Device SNMP Collection*
- Monitoring Real-Time Traffic and Device Performance on page 152

Displaying System Uptime for a Device

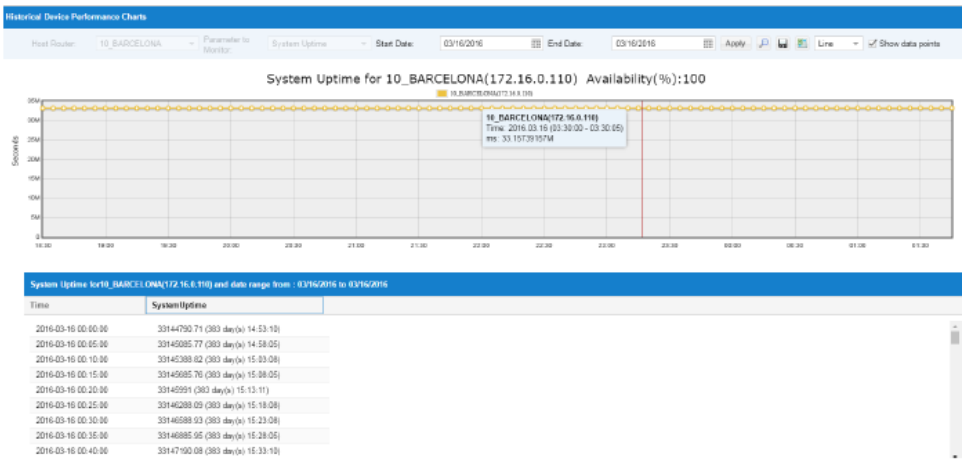
To display system uptime for a device:

1. Right-click the device on the network map.

2. Select **Historical Device Performance > System Uptime**.

   The Historical Device Performance Charts window is displayed.

Figure 24: Historical Device Performance Charts for System Uptime



The system uptime data for the selected device displays in a chart and table. By default, the data is retrieved for the current day. You can change the start and end dates in the Historical Device Charts window. You can change from a line chart to a bar chart, save the chart data as an image file, or export the table data as a .csv file.

See Also

- Displaying Historical Network Performance on page 48
- Monitoring Real-Time Traffic and Device Performance on page 152

Displaying Memory Usage for a Device

To display memory usage for a device:

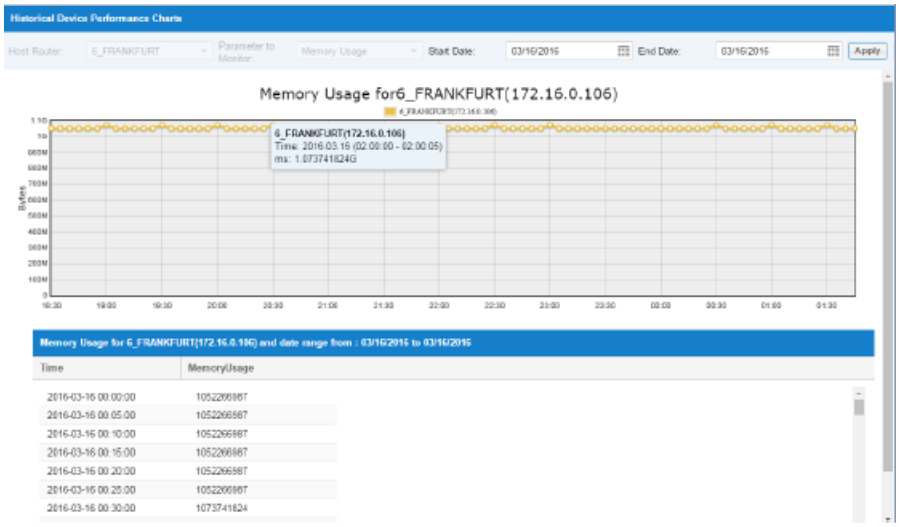
1. Right-click the device on the network map.

2. Select **Historical Device Performance > Memory Usage**.

   The Historical Device Performance Charts window is displayed.

   Figure 25 on page 48 shows the Historical Device Performance Charts window.

Figure 25: Historical Device Performance Charts for Memory Usage



The upper pane shows the memory usage data for the selected device in a chart. The bottom pane lists the memory usage values for each point in time. By default, the data is retrieved for the current day. You can change the start and end dates in the Historical Device Charts window.

See Also

- Displaying Historical Network Performance on page 48
- Monitoring Real-Time Traffic and Device Performance on page 152

Displaying Historical Network Performance

- Historical Network Performance on page 48
- Displaying Historical Network Performance for Ping on page 49
- Displaying Historical Network Performance for Advanced Ping on page 51
- Displaying Historical Network Performance for LSP Ping on page 52
- Displaying Historical Network Performance for SLAs on page 53

Historical Network Performance

Historical network performance includes ping, advanced ping, LSP ping, and SLA function invoked from the topology link.

To prepare the historical network performance, use Task Manager to set up and run the tasks listed in Table 10 on page 49.

Copyright © 2018, Juniper Networks, Inc.

Table 10: Task Manager Tasks for Historical Network Performance

Task	Description	Link to More Information
Ping	Use this task to schedule ping tests between two sets of routers or devices.	*Device Ping Collection*
Advanced ping	Schedule this task to run advanced ping statistics that include minimum, maximum, average, and standard deviation data.	*Advanced Ping Collection*
LSP ping	Use this task to run MPLS ping commands on label-switching routers. MPLS ping can be used to detect broken LSPs which normal ICMP ping cannot.	*LSP Ping Collection*
SLA	Schedule this task to run periodically and store SLA-related information.	*Device SLA Collection*

See Also

- *Task Manager*
- Monitoring the Status of Your Network on page 149

Displaying Historical Network Performance for Ping

To display the historical network performance for ping:

1. Right-click the device on the network map.

2. Select **Historical Network Performance > Ping**.

   The Enter Start and End Date window is displayed for the selected device.

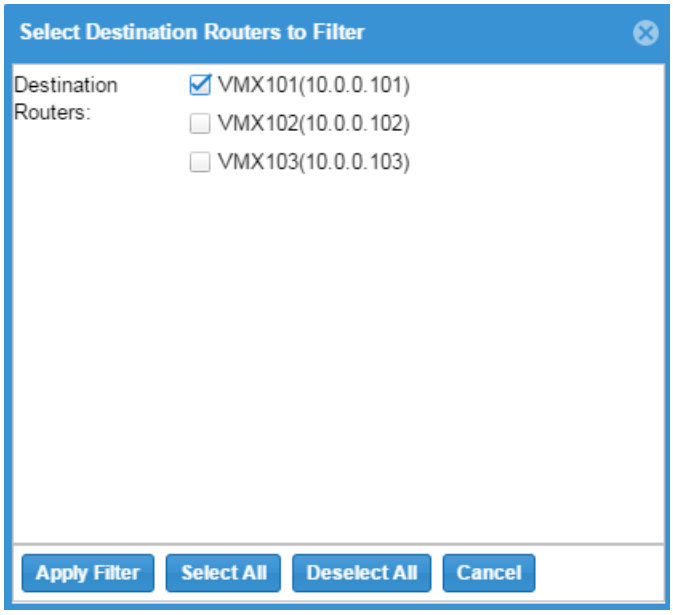
3. Select a start date and end date to collect the ping data, then click **OK**.

   By default, the data is retrieved for the current day. You can change the start and end date in the panel window where there is an input to change the date and retrieve data for a different date.

   The Select Destination Routers to Filter window is displayed in the Output pane.

   Figure 26 on page 50 shows the Select Destination Routers to Filter window.

Figure 26: Select Destination Routers to Filter

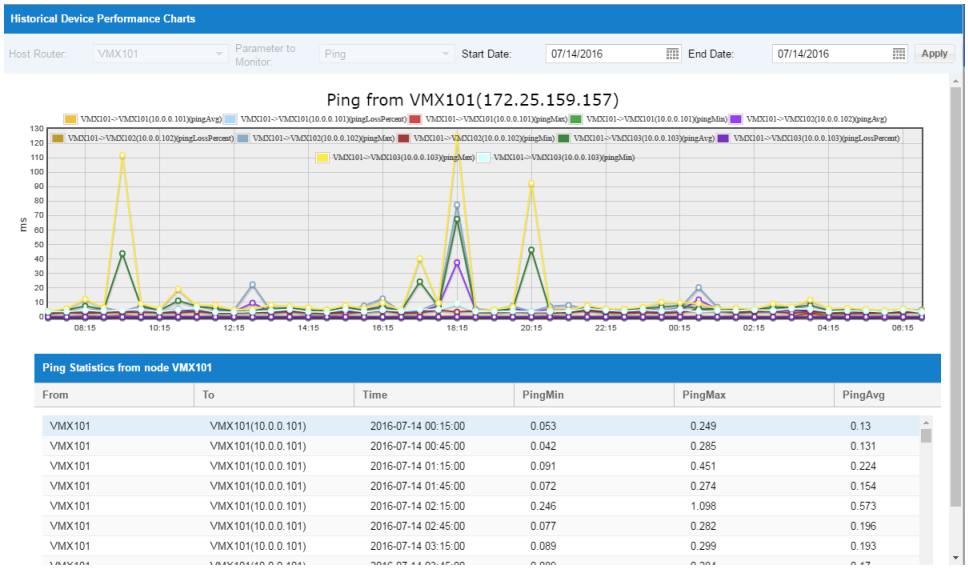


4. Select one or more destination routers to generate ping data, then click **Apply Filter**.

   The Historical Device Performance Charts window is displayed.

   Figure 27 on page 50 shows the Historical Device Performance Charts window.

Figure 27: Historical Device Performance Charts for Ping



The upper pane shows the ping data for the selected node and destination routers in a chart. The bottom pane lists ping values for each point in time.

See Also

- Diagnostic Manager on page 166

Copyright © 2018, Juniper Networks, Inc.

- Monitoring Real-Time Traffic and Device Performance on page 152

Displaying Historical Network Performance for Advanced Ping

To display the historical network performance for advanced ping:

1. Right-click the device on the network map.

2. Select **Historical Network Performance > Advanced Ping**.

   The Enter Start and End Date window is displayed for the selected device.

3. Select a start date and end date to collect the advanced ping data, then click **OK**.

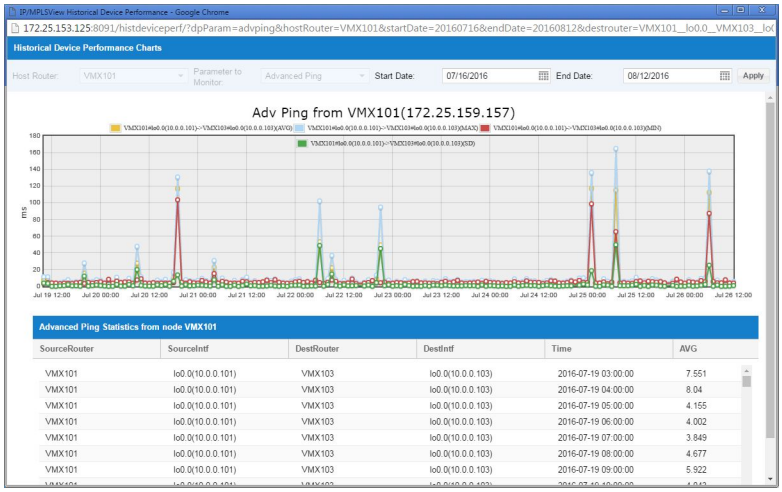
   By default, the data is retrieved for the current day. You can change the start and end date in the panel window where there is an input to change the date and retrieve data for a different date. The Select Source Destination Pairs to Filter window is displayed in the Output pane.

4. Select the check box for the source destination pairs for which you want to generate the advanced ping, then click **Apply Filter**.

   The Historical Device Performance Charts window is displayed.

   Figure 28 on page 51 shows the Historical Device Performance Charts window.

Figure 28: Historical Device Performance Charts for Advanced Ping



The upper pane shows the advanced ping data for the selected source destination pairs in a chart. The bottom pane lists the advanced ping values for each point in time.

See Also

- Diagnostic Manager on page 166
- Monitoring Real-Time Traffic and Device Performance on page 152

Displaying Historical Network Performance for LSP Ping

To display the historical network performance for LSP ping:

1. Right-click the device on the network map.

2. Select **Historical Network Performance > LSP Ping**.

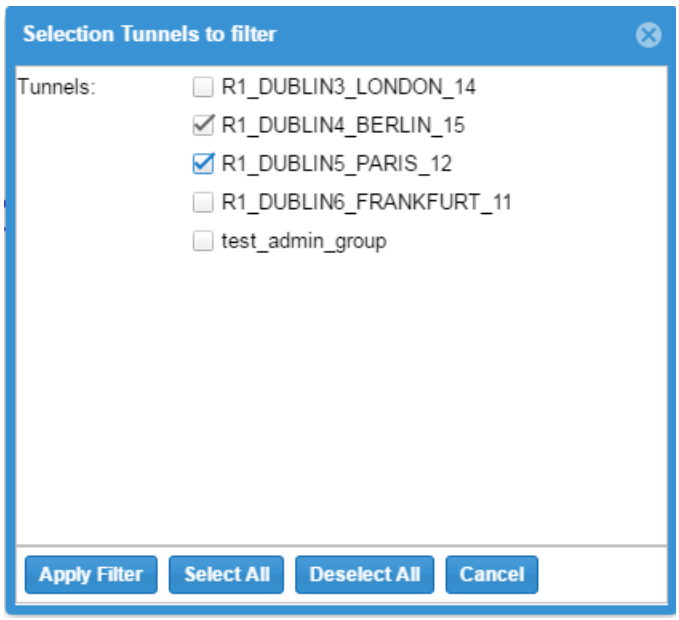
   The Enter Start and End Date window is displayed for the selected device.

3. Select a start date and end date to collect the LSP ping data, then click **OK**.

   By default, the data is retrieved for the current day. You can change the start and end date in the panel window where there is an input to change the date and retrieve data for a different date. The Select Tunnels to Filter window is displayed in the Output pane.

   Figure 29 on page 52 shows the Select Tunnels to Filter window.

Figure 29: Select Tunnels to Filter



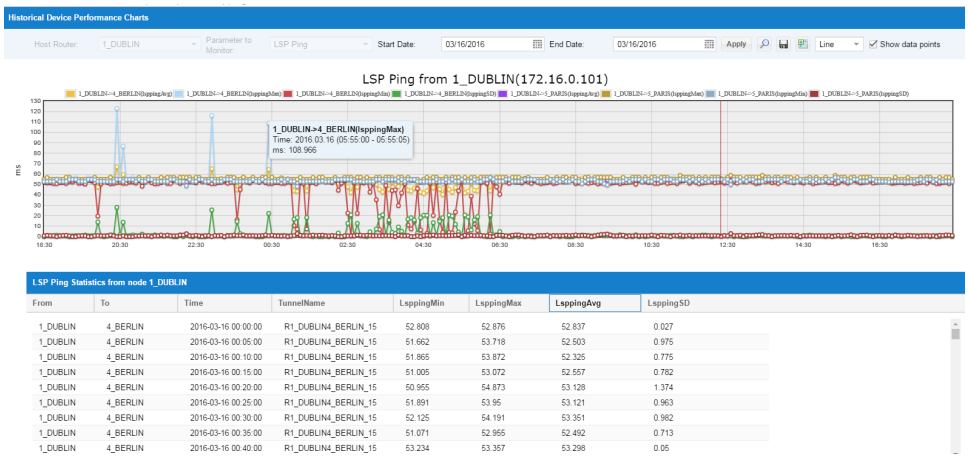
4. Select the check box for the tunnels for which you want to generate the ping, then click **Apply Filter**.

   The Historical Device Performance Charts window is displayed. The upper pane shows the LSP ping data for the selected source destination pairs in a chart. The bottom pane lists the LSP ping values for each point in time.

   Figure 30 on page 53 shows the Historical Device Performance Charts window.

Copyright © 2018, Juniper Networks, Inc.

Figure 30: Historical Device Performance Charts for LSP Ping



From	To	Time	TunnelName	LsppingMin	LsppingMax	LsppingAvg	LsppingSD
1_DUBLIN	4_BERLIN	2016-03-16 00:00:00	R1_DUBLIN4_BERLIN_15	52.808	52.876	52.837	0.027
1_DUBLIN	4_BERLIN	2016-03-16 00:05:00	R1_DUBLIN4_BERLIN_15	51.662	53.718	52.503	0.975
1_DUBLIN	4_BERLIN	2016-03-16 00:10:00	R1_DUBLIN4_BERLIN_15	51.865	53.872	52.325	0.775
1_DUBLIN	4_BERLIN	2016-03-16 00:15:00	R1_DUBLIN4_BERLIN_15	51.005	53.072	52.557	0.782
1_DUBLIN	4_BERLIN	2016-03-16 00:20:00	R1_DUBLIN4_BERLIN_15	50.955	54.873	53.128	1.374
1_DUBLIN	4_BERLIN	2016-03-16 00:25:00	R1_DUBLIN4_BERLIN_15	51.891	53.95	53.121	0.963
1_DUBLIN	4_BERLIN	2016-03-16 00:30:00	R1_DUBLIN4_BERLIN_15	52.125	54.191	53.351	0.982
1_DUBLIN	4_BERLIN	2016-03-16 00:35:00	R1_DUBLIN4_BERLIN_15	51.071	52.955	52.492	0.713
1_DUBLIN	4_BERLIN	2016-03-16 00:40:00	R1_DUBLIN4_BERLIN_15	53.234	53.357	53.298	0.05

See Also

- Diagnostic Manager on page 166
- Monitoring Real-Time Traffic and Device Performance on page 152

Displaying Historical Network Performance for SLAs

To display the historical network performance for SLAs:

1. Right-click the device on the network map.

2. Select **Historical Network Performance > SLA**.

   The Enter Start and End Date window is displayed for the selected device.

3. Select a start date and end date to collect the SLA data, then click **OK**.

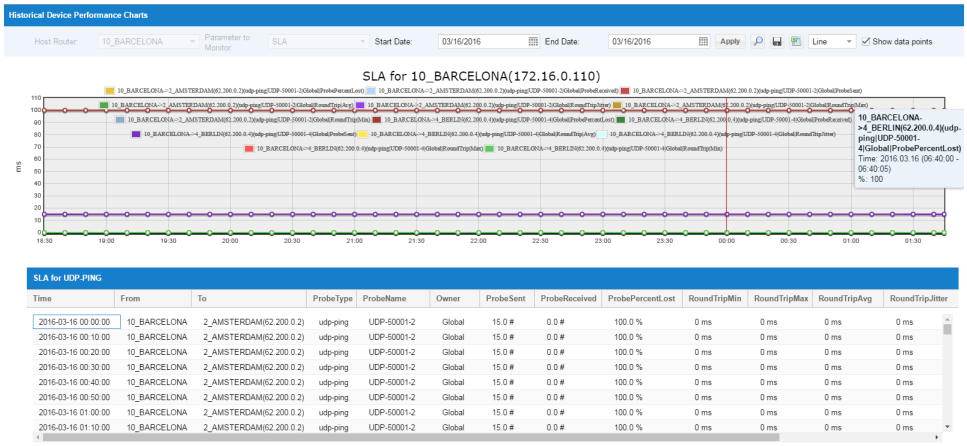
   By default, the data is retrieved for the current day. You can change the start and end date in the panel window where there is an input to change the date and retrieve data for a different date. The Select Destination Router and Probe Name to Filter window is displayed in the Output pane.

4. Select the check box for the destination routers and probe names for which you want to generate SLA data, then click **Apply Filter**.

   The Historical Device Performance Charts window is displayed. The upper pane shows the SLA data for the selected source destination pairs in a chart. The bottom pane lists the SLA values for each point in time.

   Figure 31 on page 54 shows the Historical Device Performance Charts window.

Figure 31: Historical Device Performance Charts for SLA



See Also

- Diagnostic Manager on page 166
- Monitoring Real-Time Traffic and Device Performance on page 152

Displaying Link Latency

To display the link latency:

1. Right-click the link on the network map for which you want to display the link latency.

2. Select **Link Latency**.

   The Enter Start and End Date window is displayed for the selected device.

3. Select a start date and end date to collect the link latency data, then click **OK**.

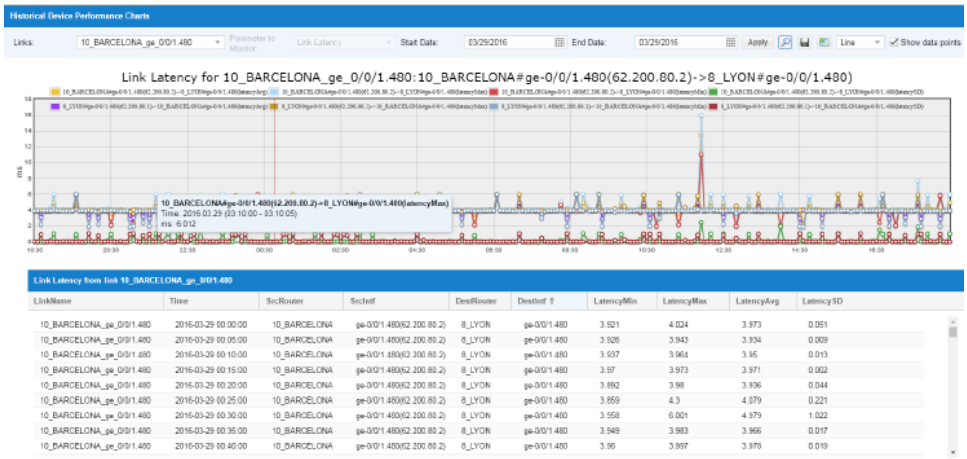
   By default, the data will be retrieved for the current day. You can change the start and end date in the panel window where there is an input to change the date and retrieve data for a different date.

   The Historical Device Performance Charts window is displayed. The upper pane shows the minimum, maximum, average, and standard deviation for the link data for the selected source destination pairs in a chart. The bottom pane lists the link latency values for each point in time.

   Figure 32 on page 55 shows the Historical Device Performance Charts window.

Copyright © 2018, Juniper Networks, Inc.

Figure 32: Historical Device Performance Charts for Link Latency



Related Documentation

- Displaying Historical Network Performance on page 48
- Monitoring Real-Time Traffic and Device Performance on page 152

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 3

Network Monitoring

- Nodes on page 57
- VPNs by VPN Types Using the Network Tab on page 68
- Network Dashboard on page 73
- Network Summary on page 74

Nodes

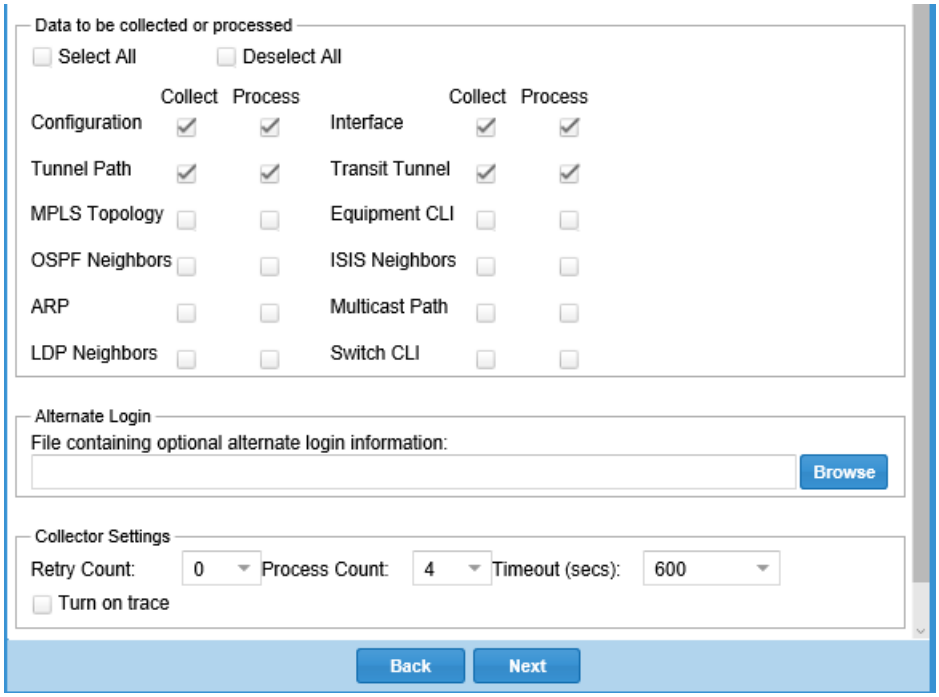
The Network > Nodes view lists all the routers in the network, organized by the groups set in the Map View. Each node has the following tabs in the right panel:

- Details
- Interfaces
- Tunnels
- Performance
- Actions

To prepare network data, select the **Tools > Task Manager > New Task > Scheduling Live Network Collection** task, selecting configuration, interface, tunnel path, and transit tunnel options. Figure 33 on page 58 shows the Scheduling Live Network Collection Task Options.

Copyright © 2018, Juniper Networks, Inc.

Figure 33: Scheduling Live Network Collection Task Options



To prepare traffic collection, select **Performance > Traffic Collection Manager > Choose Collection Tables**, using the IF, IFX, COS, and MCAST options. See Figure 34 on page 59.

Copyright © 2018, Juniper Networks, Inc.

Figure 34: Traffic Collection Manager

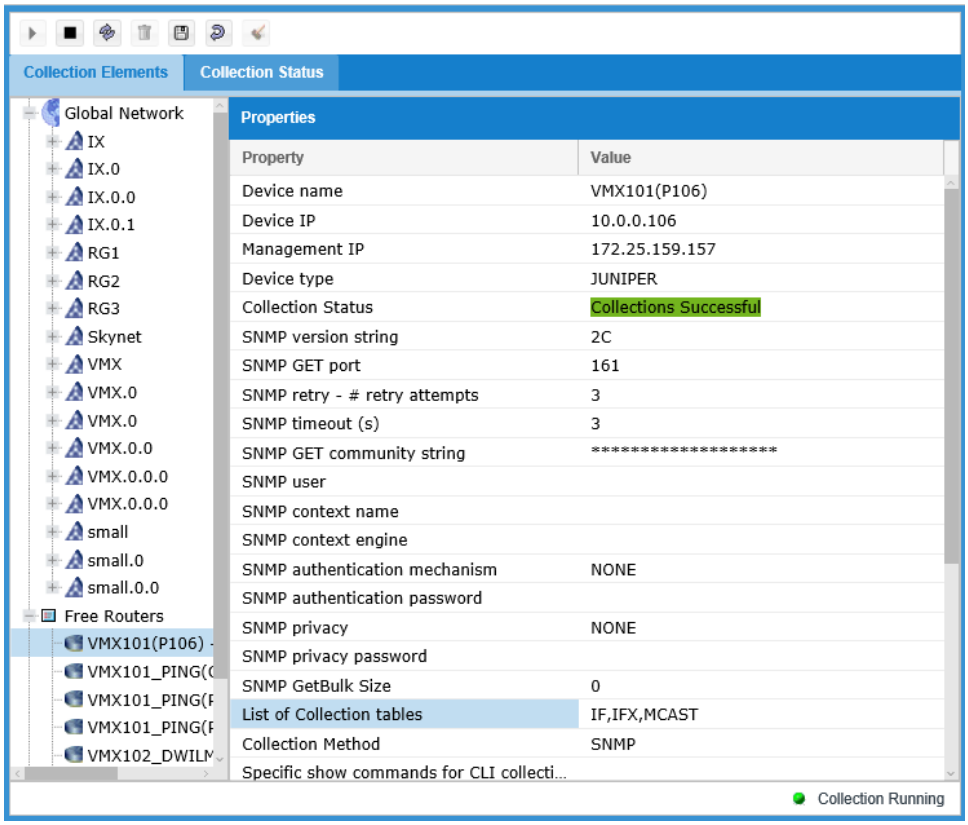
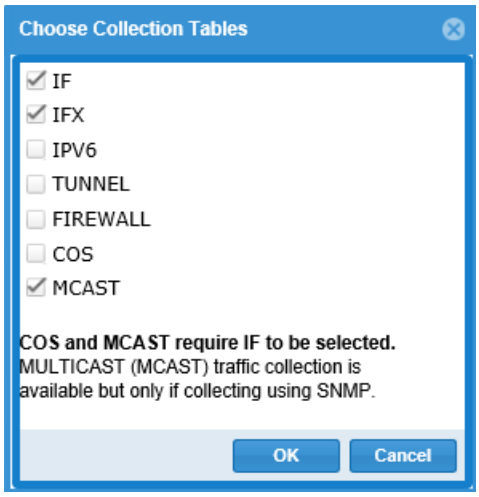


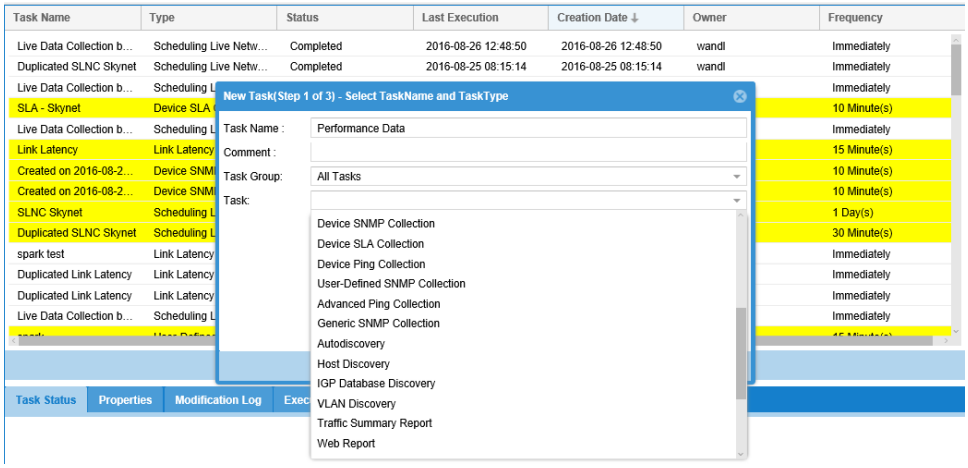
Figure 35 on page 59 shows the Choose Collection Tables window.

Figure 35: Choose Collection Tables



To prepare performance data, select **Tools > Task Manager > New Task**, then select the Device Ping, Device SLA, and Device SNMP Collection tasks. See Figure 36 on page 60.

Figure 36: Prepare Performance Data



To display node details, select **Network > Nodes**. The Details tab displays the router name, router type, IP address, management IP address, and group. Figure 37 on page 60 shows the node details.

Figure 37: Node Details

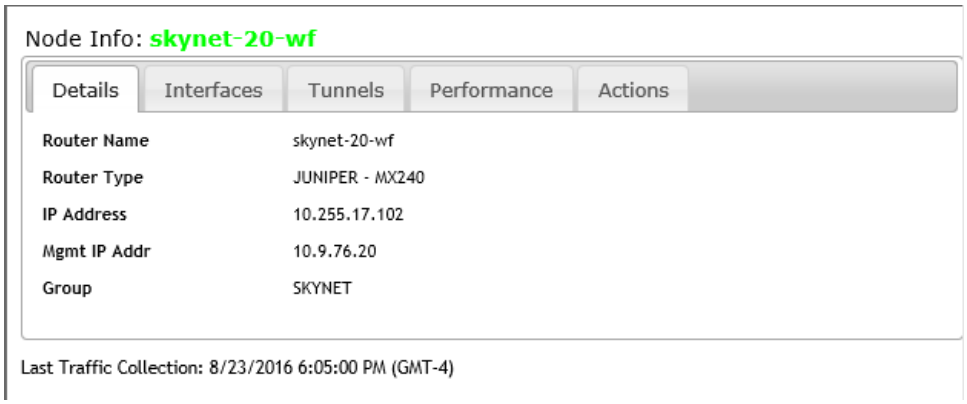


Table 11 on page 60 describes the items in the Details tab.

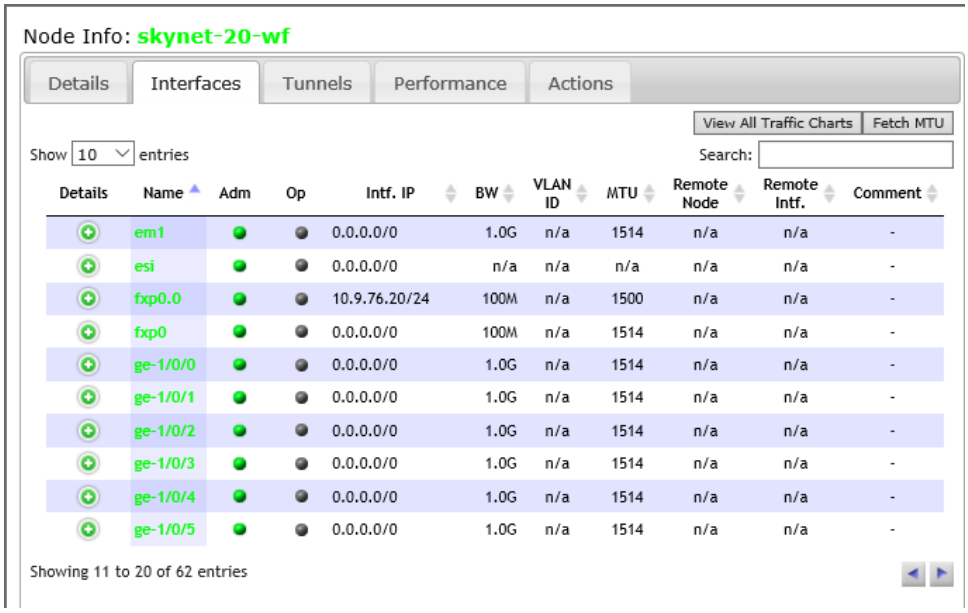
Table 11: Node Details Tab Descriptions

Field	Description
Router Name	Device hostname.
Router Type	Hardware vendor.
IP Address	IP address of device.
Management IP Address	IP address in the device profile used for collection.
Group	The topology group for that device. Groups are defined in the IP/MPLSView client.

Copyright © 2018, Juniper Networks, Inc.

The Interfaces tab displays the interface information. Figure 38 on page 61 shows the interface information.

Figure 38: Node Interfaces



Details	Name	Adm	Op	Intf. IP	BW	VLAN ID	MTU	Remote Node	Remote Intf.	Comment
	em1			0.0.0.0/0	1.0G	n/a	1514	n/a	n/a	-
	esi			0.0.0.0/0	n/a	n/a	n/a	n/a	n/a	-
	fxp0.0			10.9.76.20/24	100M	n/a	1500	n/a	n/a	-
	fxp0			0.0.0.0/0	100M	n/a	1514	n/a	n/a	-
	ge-1/0/0			0.0.0.0/0	1.0G	n/a	1514	n/a	n/a	-
	ge-1/0/1			0.0.0.0/0	1.0G	n/a	1514	n/a	n/a	-
	ge-1/0/2			0.0.0.0/0	1.0G	n/a	1514	n/a	n/a	-
	ge-1/0/3			0.0.0.0/0	1.0G	n/a	1514	n/a	n/a	-
	ge-1/0/4			0.0.0.0/0	1.0G	n/a	1514	n/a	n/a	-
	ge-1/0/5			0.0.0.0/0	1.0G	n/a	1514	n/a	n/a	-

Table 12 on page 61 describes the items in the Interfaces tab.

Table 12: Node Interfaces Tab Descriptions

Field	Description
Details	Click the Details icon to display detailed information and traffic charts for each interface.
Name	Interface name.
Adm	Administrative status.
Op	Operational status (green for up and red for down).
Interface IP	IP address of the interface.
BW	Bandwidth of this interface.
VLAN ID	Virtual LAN identifier (if applicable).
MTU (Maximum Transmission Unit)	The smallest MTU of any of the hops on the path between the source and destination. Click **Fetch MTU** to populate this data.
Remote Node	Hostname of the remote end node.
Remote Intf	Interface name of the remote end node.

Copyright © 2018, Juniper Networks, Inc.

Table 12: Node Interfaces Tab Descriptions (continued)

Field	Description
Comment	Interface description.

Click the **Details** icon or **View All Traffic Charts** button to display detailed information and charts on each interface. See Figure 39 on page 62.

Figure 39: Interfaces Traffic Chart

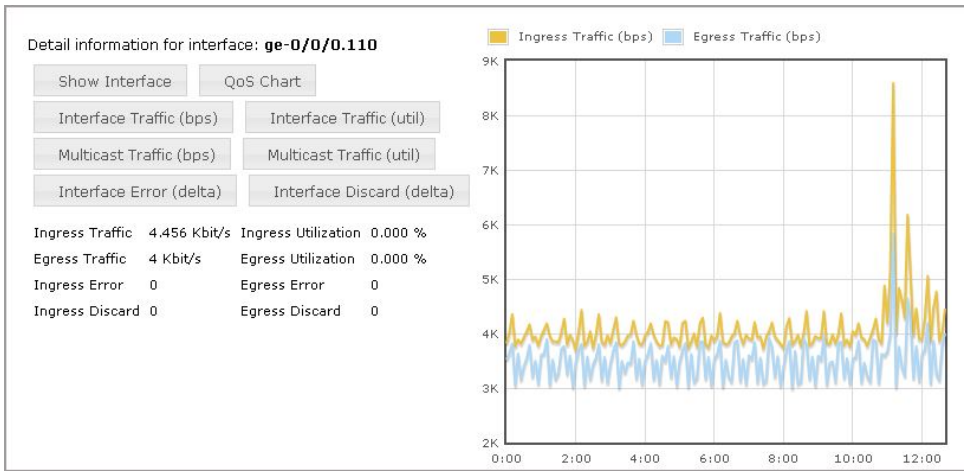


Table 13 on page 62 describes the items in the detail information for the interface.

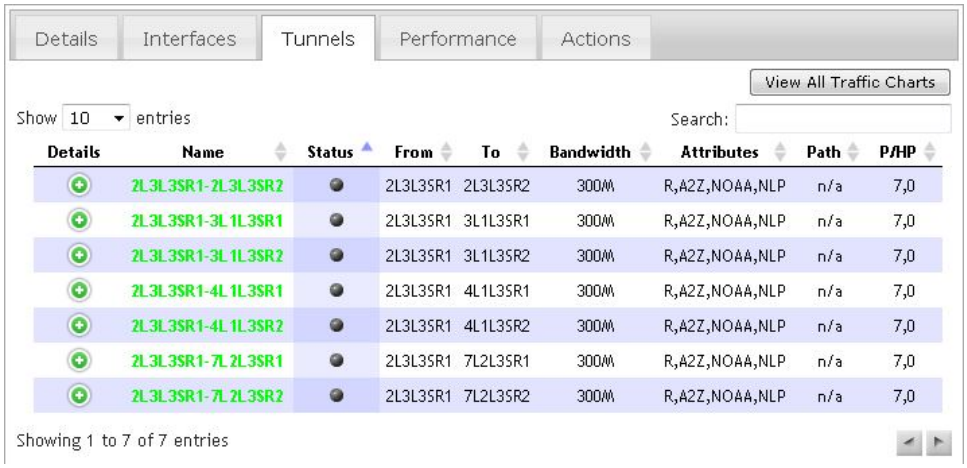
Table 13: Detailed Interface Information Descriptions

Field	Description
Show Interface	Issues a **show interface** command and displays the results in a pop-up window.
Show QoS	Displays the CoS traffic chart.
Interface Traffic (bps)	Displays the ingress and egress traffic chart.
Interface Traffic (bps)	Displays the ingress and egress utilization chart.
Multicast Traffic (bps)	Displays the multicast traffic chart.
Multicast Traffic (bps)	Displays the multicast utilization chart.
Interface Error (delta)	Displays the interface error charts.
Interface Discard (delta)	Displays the interface discard charts.

The Tunnels tab displays the tunnel information. See Figure 40 on page 63.

Copyright © 2018, Juniper Networks, Inc.

Figure 40: Node Tunnels



Details	Name	Status	From	To	Bandwidth	Attributes	Path	P/HP
	2L3L3SR1-2L3L3SR2		2L3L3SR1	2L3L3SR2	300M	R,A2Z,NOAA,NLP	n/a	7,0
	2L3L3SR1-3L1L3SR1		2L3L3SR1	3L1L3SR1	300M	R,A2Z,NOAA,NLP	n/a	7,0
	2L3L3SR1-3L1L3SR2		2L3L3SR1	3L1L3SR2	300M	R,A2Z,NOAA,NLP	n/a	7,0
	2L3L3SR1-4L1L3SR1		2L3L3SR1	4L1L3SR1	300M	R,A2Z,NOAA,NLP	n/a	7,0
	2L3L3SR1-4L1L3SR2		2L3L3SR1	4L1L3SR2	300M	R,A2Z,NOAA,NLP	n/a	7,0
	2L3L3SR1-7L2L3SR1		2L3L3SR1	7L2L3SR1	300M	R,A2Z,NOAA,NLP	n/a	7,0
	2L3L3SR1-7L2L3SR2		2L3L3SR1	7L2L3SR2	300M	R,A2Z,NOAA,NLP	n/a	7,0

Table 14 on page 63 describes the items in the Tunnels tab.

Table 14: Tunnels Information Descriptions

Field	Description
Details	Click the Details icon to display detailed information and traffic charts for each tunnel.
Name	Tunnel name.
Status	Tunnel status (green means up and red means down).
From	Name of the source node.
To	Name of the source node.
Bandwidth	Bandwidth of this tunnel.
Attributes	Displays any tunnel type parameters.
Path	Pathname for this tunnel.
P/HP	Setup priority/holding priority.

Click the **Details** icon or **View All Traffic Charts** button to toggle the right panel to display detailed information and charts for each tunnel. See Figure 41 on page 64.

Figure 41: Tunnels Traffic Chart

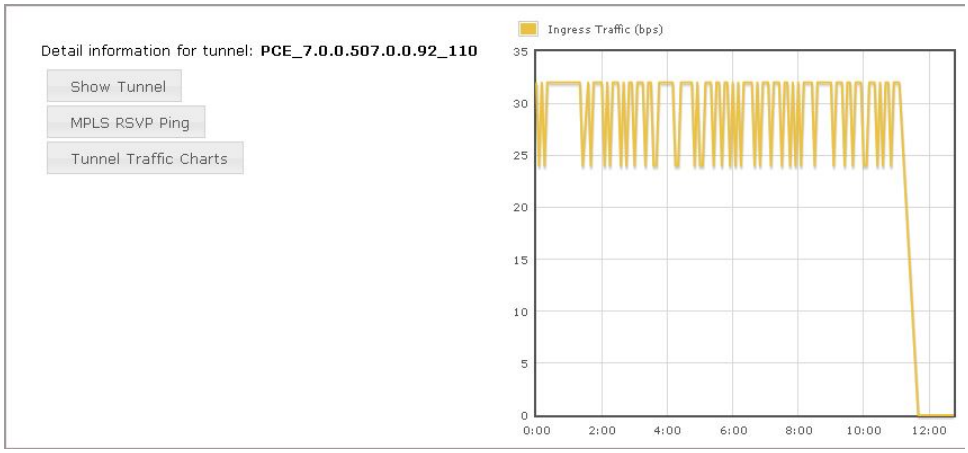


Table 15 on page 64 describes the items in the detail information for the tunnels.

Table 15: Detailed Tunnel Information Descriptions

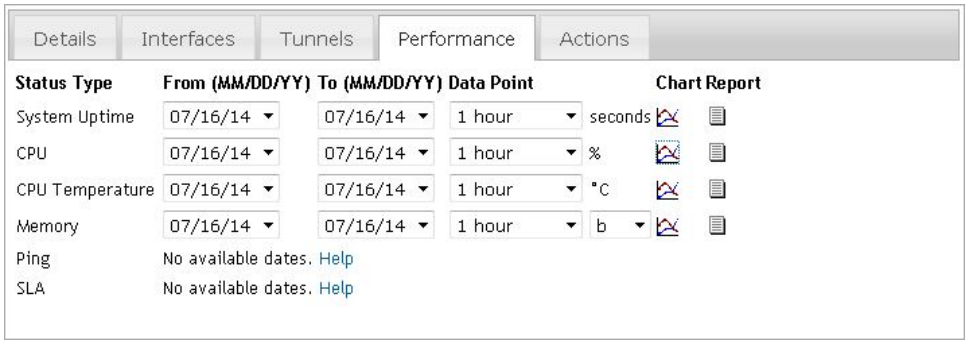
Field	Description
Show Tunnel	Issues a **show mpls traffic eng tunnels** (Cisco) or **show mpls lsp name** (Juniper) command, or the equivalent command for other hardware types in a new window.
MPLS RVSP Ping	Performs an MPLS ping.
Tunnel Traffic Charts	Displays the tunnel traffic on this interface in a traffic chart over the last 24 hours, beginning at midnight.

The Performance tab displays charts for the system uptime, CPU, CPU temperature, memory, ping, and SLA. See Figure 42 on page 64.

This data is derived from scheduling the relevant tasks in the Task Manager: Device SNMP Collection, Device Ping Collection, and Device SLA Collection.

To display a chart, choose select the date range, data point, units, and then click the **Chart** icon. The chart opens in a new pop-up window.

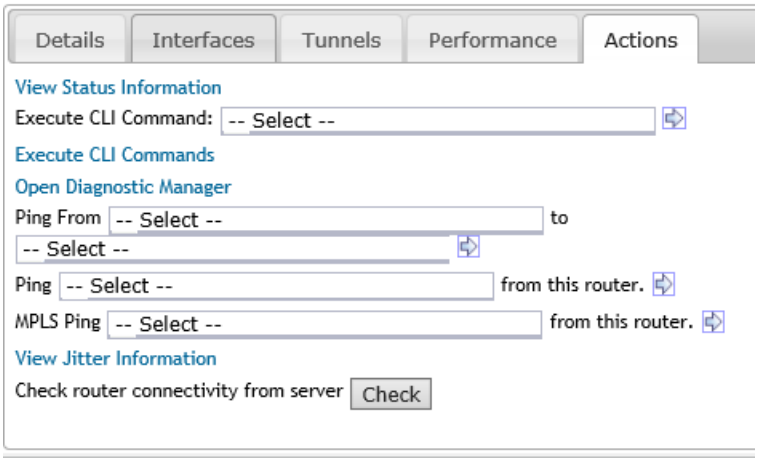
Figure 42: Node Performance



Copyright © 2018, Juniper Networks, Inc.

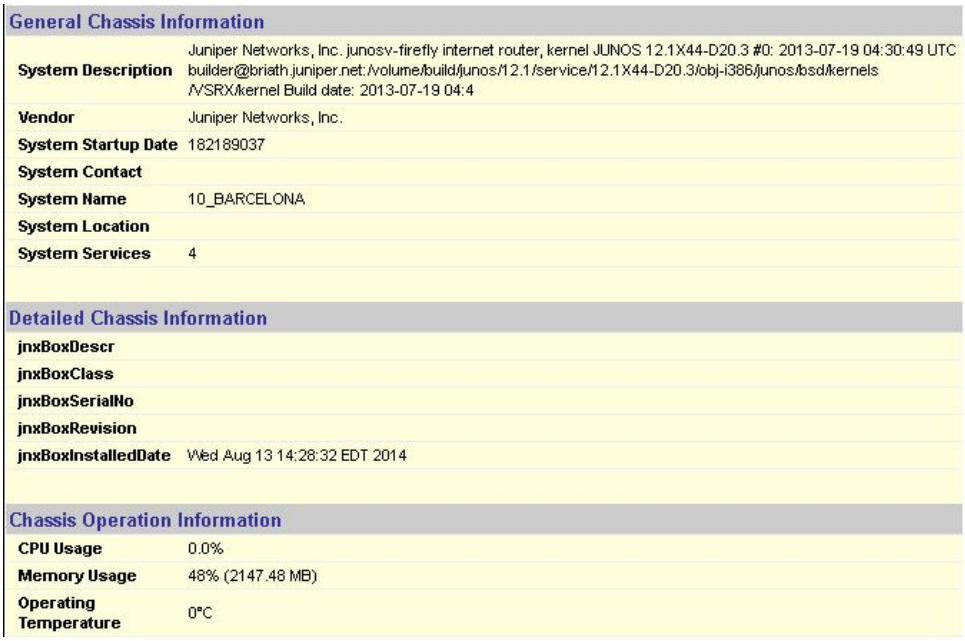
The Actions tab displays information about the node status, SNMP, and jitter; execute CLI commands, open diagnostic manager, ping routers, and check router connectivity. See Figure 43 on page 65.

Figure 43: Node Actions



- View Status Information: Displays general chassis information for the device. Depending on the hardware device type, you may also see sections on the page regarding detailed chassis information and chassis operation information. See Figure 44 on page 65.

Figure 44: Sample Status Information



General Chassis Information

System Description	Juniper Networks, Inc. junosv-firefly internet router, kernel JUNOS 12.1X44-D20.3 #0: 2013-07-19 04:30:49 UTC builder@briath.juniper.net:/volume/build/junos/12.1/service/12.1X44-D20.3/obj-i386/junos/bsd/kernels /VSRX/kernel Build date: 2013-07-19 04:4
Vendor	Juniper Networks, Inc.
System Startup Date	182189037
System Contact	
System Name	10_BARCELONA
System Location	
System Services	4

Detailed Chassis Information

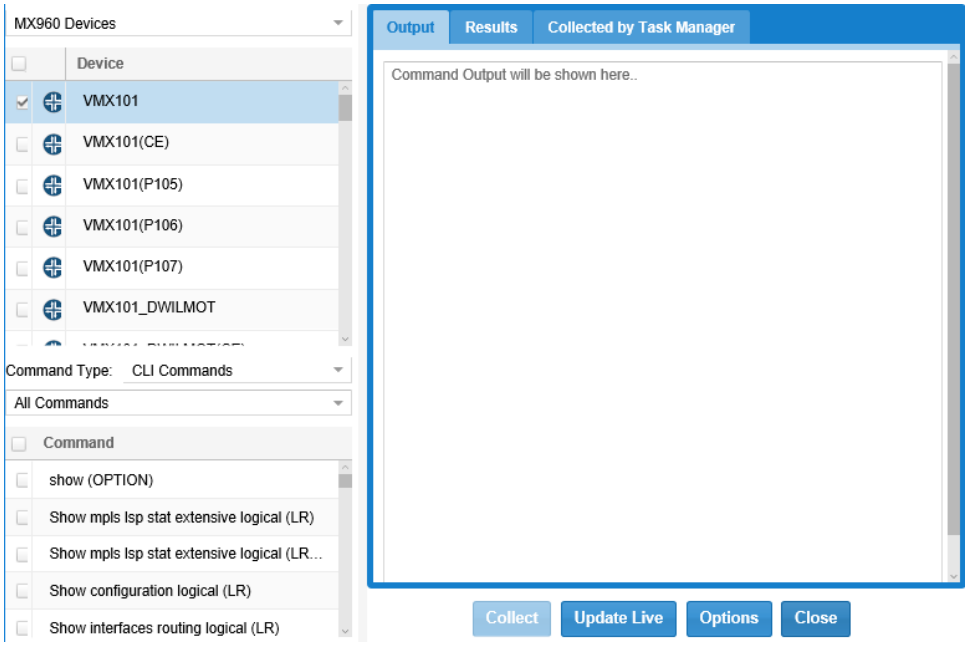
jnxBoxDescr	
jnxBoxClass	
jnxBoxSerialNo	
jnxBoxRevision	
jnxBoxInstalledDate	Wed Aug 13 14:28:32 EDT 2014

Chassis Operation Information

CPU Usage	0.0%
Memory Usage	48% (2147.48 MB)
Operating Temperature	0°C

- **Execute CLI Command:** This feature allows you to issue **show** commands to the device and is intended to serve as a shortcut for your most frequently used **show** commands. Select the command from the drop-down box. This will display a pop-up window with the command output. Some commands are parameterized, meaning that you need to input additional variables to run the commands. See Figure 45 on page 66.

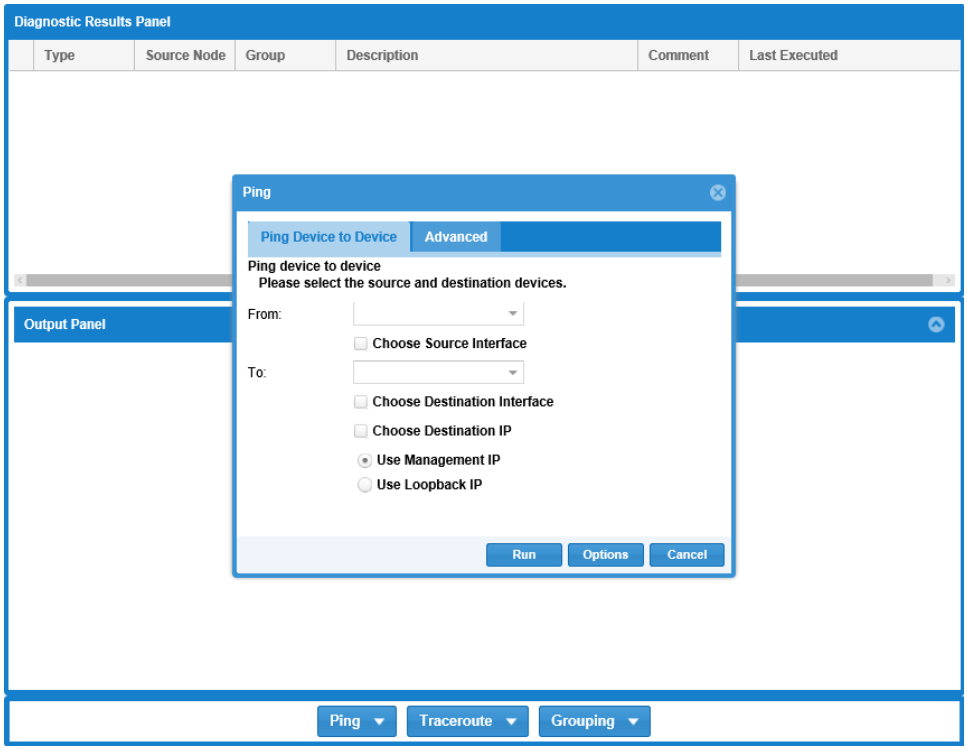
Figure 45: Execute CLI Command



- **Open Diagnostics Manager:** Opens the Diagnostics Manager window. See Figure 46 on page 67.
  - To run ping, click **Ping**, select from the menu items, input your selections, and click **Run**.
  - To run traceroute, click **Traceroute**, select from the menu items, input your selections, and click **Run**.

Copyright © 2018, Juniper Networks, Inc.

Figure 46: Diagnostic Manager



- **Ping**: These ping operations check router connectivity by pinging between devices, pinging from this router to another selected device, or performing a MPLS ping. Choose the devices from the drop-down boxes and click **Run** to execute.
- **View Jitter Information:** This displays jitter information collected from the router, including total round-trip delay, egress/ingress round-trip delay, and recent probe results. Not all routers are able to display jitter information. See Figure 47 on page 68.

Figure 47: Sample Jitter Information

Entry #: 400			
Round Trip Time Information:			
# RTT's successfully measured	199		
Sum of RTT's successfully measured	386	Sum of squares of RTT's successfully measured	766
Minimum of RTT's that were successfully measured	1	Maximum of RTT's that were successfully measured	3
Positive (Source to Destination) Jitter Values:			
Sum of number of all positive jitter values from packets	3		
Minimum of all positive jitter values from packets sent	1	Maximum of all positive jitter values from packets sent	1
Sum of RTT's of all positive jitter values from packets	3	Sum of square of RTT's of all positive jitter values	3
Negative (Source to Destination) Jitter Values:			
Sum of number of all negative jitter values from packets	3		
Minimum of all negative jitter values from packets sent	1	Maximum of all negative jitter values from packets sent	1
Sum of RTT's of all negative jitter values from packets	3	Sum of square of RTT's of all negative jitter values	3
Positive (Destination to Source) Jitter Values:			
Sum of number of all positive jitter values from packets	14		
Minimum of all positive jitter values from packets sent	1	Maximum of all positive jitter values from packets sent	1
Sum of RTT's of all positive jitter values from packets	14	Sum of square of RTT's of all positive jitter values	14
Negative (Source to Destination) Jitter Values:			
Sum of number of all negative jitter values from packets	14		
Minimum of all negative jitter values from packets sent	1	Maximum of all negative jitter values from packets sent	1
Sum of RTT's of all negative jitter values from packets	14	Sum of square of RTT's of all negative jitter values	14
Packet Information:			
# of packets arrived out of sequence	0		
# of packets lost when sent from source to destination	1	# of packets lost when sent from destination to source.	0
# of packets that are lost for which we cannot determine the direction	0	# of packets that arrived after the timeout	0
Latency (Source to Destination):			
Sum of one way latency	0	Sum of squares of one way latency	0
Minimum of all one way latency	0	Maximum of all one way latency	0
Latency (Destination to Source):			
Sum of one way latency	0	Sum of squares of one way latency	0
Minimum of all one way latency	0	Maximum of all one way latency	0
# of successful one way latency measurements:		0	
MOS value for the latest jitter operation in hundreds:		*n/a*	
An application specific sense code for the completion status:		*n/a*	
A sense description for the completion status:			

Related Documentation

- Network Topology Window Overview on page 29
- Running the CLI on page 162
- Diagnostic Manager on page 166

VPNs by VPN Types Using the Network Tab

The VPNs by VPN Types feature allows you to examine the VPN information (if any) at a particular node. Select **Network > VPNs by VPN Types** to display the VPN information. For each VPN, click the arrow to expand the VPN to show the provider edges (PEs) belonging to that VPN.

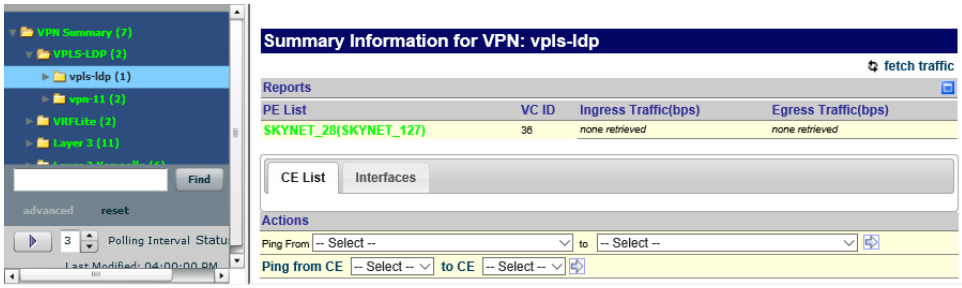
Click on a VPN in the left tree to view the details for that VPN in the right panel. In the right panel, click **fetch traffic** to populate the ingress and egress traffic information.

Click on a PE or customer edge (CE) device name from the Summary Information for VPN window to bring up the Node Information window for that node. Figure 48 on page 69

 Copyright © 2018, Juniper Networks, Inc.

shows the Summary Information for VPN window. The Node Information window is divided into tabs for Details, Interfaces, Tunnels, Performance, and Actions.

Figure 48: VPNs by VPN Type



Item	Description
PE List	List of provider edges in the selected VPN.
VPN/VRF	VPN name or virtual routing and forwarding instance.
Ingress/Egress Traffic	Summary view of ingress and egress traffic.
CE List	List of customer edges in the selected VPN.
Interfaces	List of interfaces in the selected VPN.
Ping from PE to PE/CE	Select a PE from the first drop-down box and a PE or CE from the second drop-down box. Click the arrow to view connectivity information.
Ping from CE to CE	Select a CE from the first drop-down box and a CE from the second drop-down box. Click the arrow to view connectivity information.

The Detailed Node Information that is displayed varies depending upon the VPN type. For a general understanding of the VPN types supported by IP/MPLSView and the various VPN properties, see the *Router Feature Guide for IP/MPLSView*. The fields in the Detailed PE Information section should be self-explanatory. Table 16 on page 69 lists the fields available for different VPN types. You can access the VPN types from Network > VPNs by VPN Type, then select VPN type from the VPN Summary list.

Figure 49 on page 70 describes the items in the Details tab information for the node VPN.

Table 16: Detailed Node VPN Types

VPN Type	Fields
Layer 3	Router name, VRF name, Layer, Route Distinguisher, Route Target Export/Import, Protocol
Layer 2-Martini	Router name, Layer, VC ID, Node A/Z, Circuit A/Z, Encapsulation, Bandwidth
Layer 2-Kompella	Router name, Layer, Node A/Z, Interface A/Z, Site A/Z, Site ID A/Z, Transmit/Receive LSP, Encapsulation A/Z, VRF A/Z, Route Distinguisher, Route Target Export/Import

Copyright © 2018, Juniper Networks, Inc.

Table 16: Detailed Node VPN Types (continued)

VPN Type	Fields
VPLS-BGP	Router name, VRF name, Layer, Route Distinguisher, Route Target Export/Import, Protocol, Site Name, Site ID
VPLS-LDP	Router name, VPN name, VC ID, Encapsulation

Table 17: Detailed PE Node Information

Detailed PE Information Field	Description
Protocol	The protocol whose routes were redistributed into IBGP for distribution among the PEs in the MPLS backbone (for example, BGP, OSPF, RIP, static). • NOTE: "Static" refers to static routes. "Connected" indicates all local subnets that are directly connected to the PE.

Figure 49: Detailed VPN Info

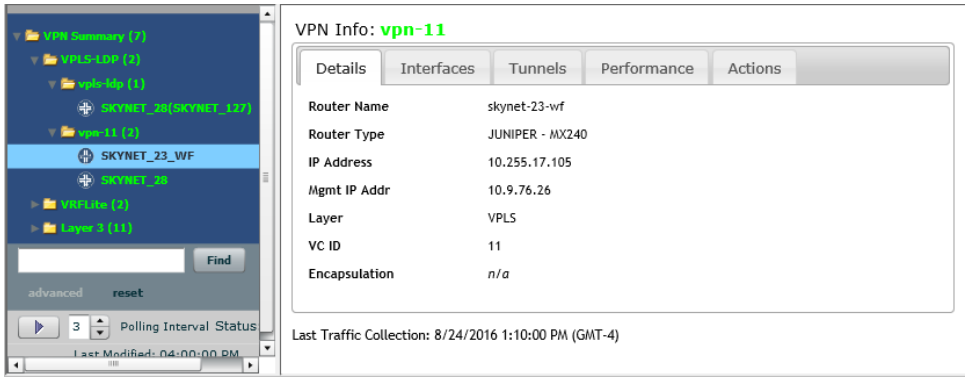


Table 18: Interfaces

PE Interfaces Column	Description
PE Name/IP Addr	Hostname and IP address of the provider edge router.
CE Name/IP Addr	Hostname and IP address of the customer edge router.
Bandwidth	Bandwidth of the interface.
VLAN ID	Virtual LAN identifier (if applicable).
MTU	The smallest MTU of any of the hops on the path between the source and destination. Click **Fetch MTU** to populate this data.
Remote Node Name	Name of the node to which this interface is connected.
Remote Intf Name	Name of the interface to which this interface is connected.

Copyright © 2018, Juniper Networks, Inc.

Table 18: Interfaces (continued)

PE Interfaces Column	Description
View CLI Interface Details (icon)	Issues a **show interface** command and displays the results in a pop-up window.
View Chart (icon)	Displays the ingress and egress traffic on this interface in a traffic chart over the last 24 hours, beginning at midnight.

Figure 50: VPN Interface Traffic Chart

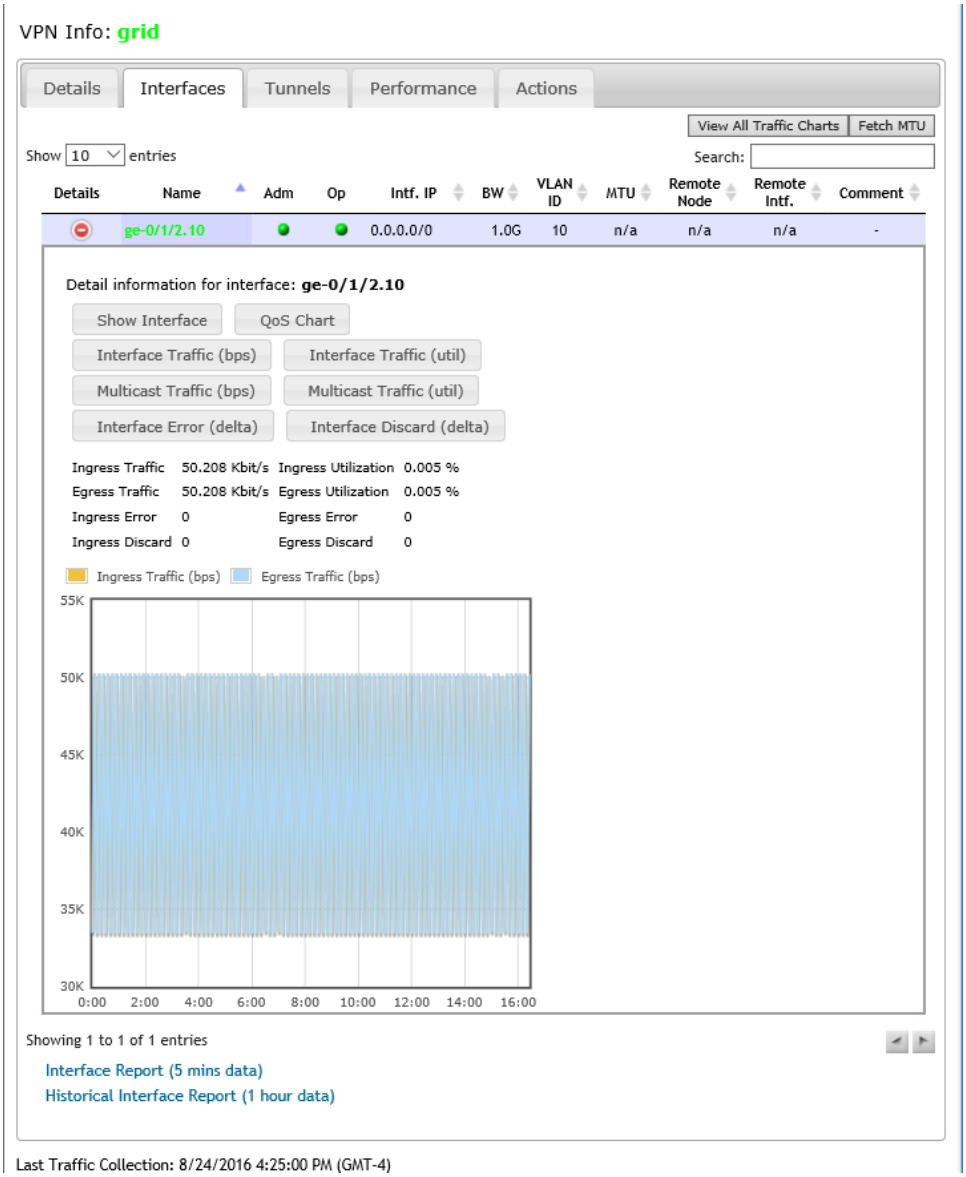


Table 19: Tunnels

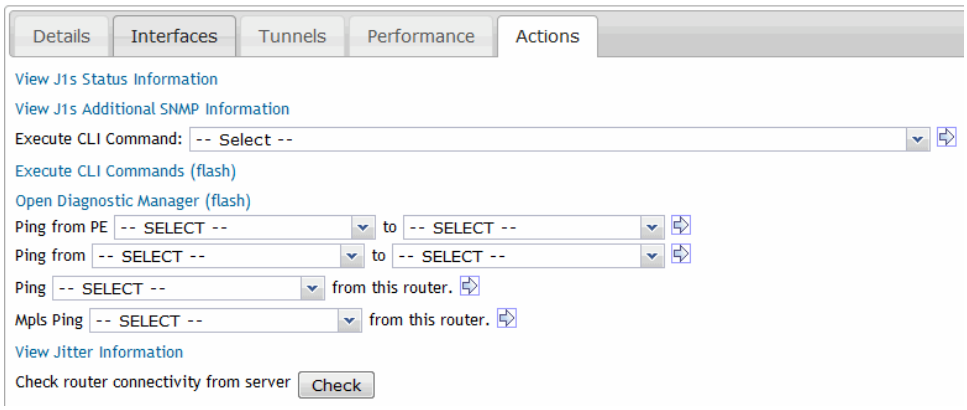
Field	Description
Tunnel Name	Tunnel name.
From Name	Name of the source node.
To IP	IP address of the destination node.
Bandwidth	Bandwidth of this tunnel.
Attributes	Displays any tunnel type parameters. For detailed information on the various tunnel type parameters, see the Modeling Tunnels chapter of the *Router Feature Guide for IP/MPLSView*.
Path	Pathname for this tunnel.
P/HP	Setup priority/holding priority.
View CLI Tunnel Details (icon)	Issues a **show mpls traffic eng tunnels** (Cisco) or **show mpls lsp name** (Juniper) command, or the equivalent command for other hardware types in a new window.
View Chart (icon)	Displays the tunnel traffic on this interface in a traffic chart over the last 24 hours, beginning at midnight.

Table 20: Actions

Item	Description
Select command to view	Select a **show** command from the drop-down menu and click the arrow icon to the right to view the results for this device. Note that because there are numerous **show** commands, but only a few that each user cares about, **show** commands need to be configured first. Contact your administrator for assistance. For instructions on how to configure additional VPN show commands, see *Configuring the Show Commands* in the *IP/MPLSView Java-Based Management and Monitoring Guide*.
Ping from PE to PE/CE	Issue a ping from a selected PE to a selected PE or CE from the drop-down list. For information on interpreting ping results, see *Ping Device From Device* in the *IP/MPLSView Java-Based Management and Monitoring Guide*.
Ping	Issue a ping from this router to another router in the network. For information on interpreting ping results, see *Ping Device From Device* in the *IP/MPLSView Java-Based Management and Monitoring Guide*.
MPLS Ping	This pings the LSP between the current router and the selected router.
View Jitter Information	Displays a report of jitter information, including total round-trip delay, egress/ingress round-trip delay, and recent probe results.

Copyright © 2018, Juniper Networks, Inc.

Figure 51: VPN Actions

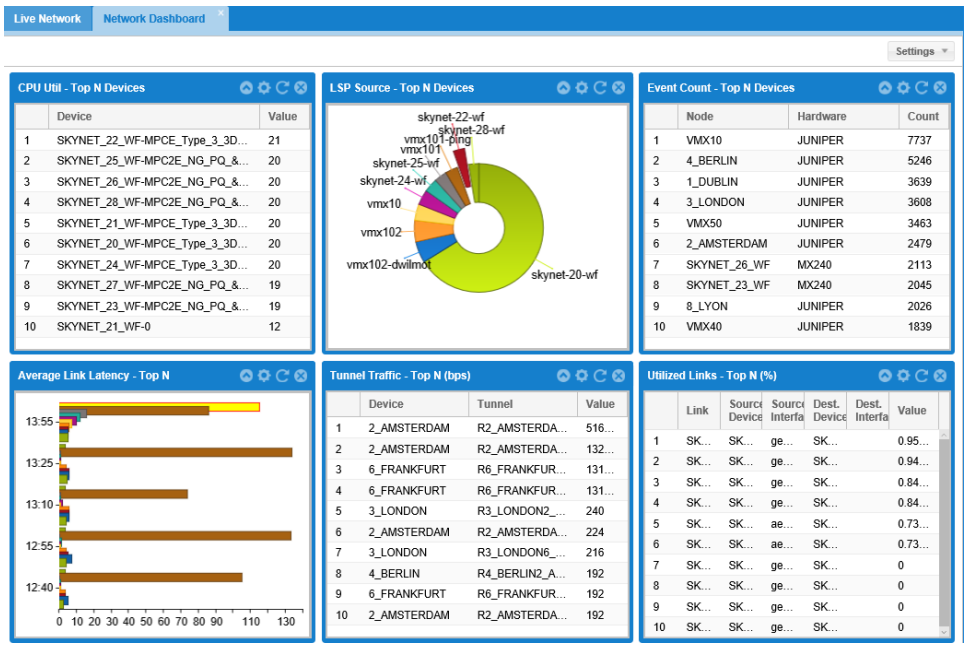


For more information about VLANs, see the *Router Feature Guide for IP/MPLSView*.

Network Dashboard

The Network Dashboard feature allows you to see a variety of details from across IP/MPLSView, such as snapshots of the charts, top 10 events, and common issues in the integrity check. Figure 52 on page 73 shows the Network Dashboard window.

Figure 52: Network Dashboard



To create the charts, select the appropriate Content Category. Then select the check boxes of the charts that you would like to generate. Select to either display a table (Tabular view) or a chart (line, bar, and in some cases pie chart), and the number of data points to include.

The following appropriate prerequisite steps need to be run in order for these charts to be displayed:

- The Device SNMP Collection task should be set up for CPU/memory data.
- The event server and SNMP trap server should be started and the router should be set up to forward traps to the IP/MPLSView server for event data.
- The Link Latency Collection task should be set up for link latency data,
- The Device Ping Collection task should be set up for ping content.
- The Traffic Collection Manager should be set up for traffic information.

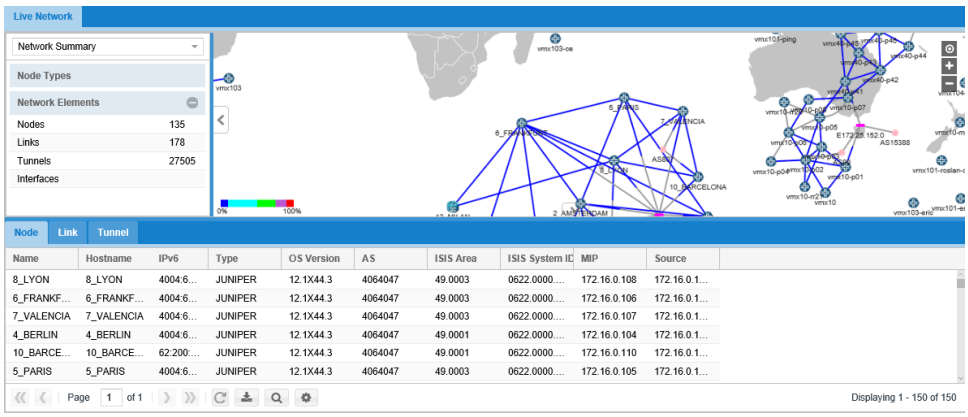
Network Summary

The Network Summary displays the total number of nodes, groups, tunnels, links, VPNs, and interfaces in the network.

To access the Network Summary:

1. From the Live Network tab and in the left pane, select **Network Summary** from the list.

Figure 53: Summary of Network Elements



2. Select **Network Elements**.

   The left pane expands and the number of network elements is displayed. The above window shows an example of the network elements.

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 4

Configuration Management

- Network Data on page 75
- Network Reports on page 76
- Integrity Check Reports on page 78
- Hardware Inventory Reports on page 78
- Equipment View on page 82
- Configuration Revision Manager on page 84
- Device Library on page 86
- Miscellaneous Reports on page 90

Network Data

To access the Network Data features, select **Configuration > Network Data** from the IP/MPLSView main window.

The Network Model Data feature enables you to browse the latest network model data derived from the Scheduling Live Network Collection task in the **/u/wandl/data/.network** directory. See Figure 54 on page 75.

Figure 54: Network Model Data

Network Model Data

Name		Size	Date
aclist.x	*Excel* | *Text*	5677 bytes	Apr 16, 2014 4:37:29 PM
atconfig.x	*Excel* | *Text*	2504 bytes	Apr 16, 2014 4:37:29 PM
attunnel.x	*Excel* | *Text*	177 bytes	Apr 10, 2014 10:45:33 AM

The Network Config Data feature enables you to browse the latest configuration data from the Scheduling Live Network Collection task in the **/u/wandl/data/collection/.LiveNetwork/** directory. The “config” option must be selected from the task. See Figure 55 on page 76.

Copyright © 2018, Juniper Networks, Inc.

Figure 55: Network Config Data

Network Config Data

Name	Size	Date
[config]	2048 bytes	Apr 16, 2014 4:37:19 PM
[equipment_cli]	1536 bytes	Apr 16, 2014 4:37:26 PM
[interface]	1536 bytes	Apr 16, 2014 4:37:15 PM
[log]	512 bytes	Apr 16, 2014 4:33:22 PM
[switch_cli]	1536 bytes	Apr 10, 2014 10:45:25 AM
[topo]	1024 bytes	Apr 10, 2014 10:45:14 AM
[transit_tunnel]	1536 bytes	Apr 10, 2014 10:45:13 AM
[tunnel_path]	1024 bytes	Apr 10, 2014 10:45:08 AM

The User Collected CLI Data feature enables you to browse the data collected from the User CLI task in the **/u/wandl/data/UserCLI** directory. If you log in as the admin user, you can browse for the User CLI directory. See Figure 56 on page 76.

Figure 56: User Collected Data

User Collected Data

Excel1: open in Excel with space and tab delimiter
Excel2: open in Excel with comma (,) delimiter

	Name	Size	Date
☐	[201407021213]	4096 bytes	Aug 2, 2014 12:18:00 PM
☐	[201407021248]	4096 bytes	Aug 2, 2014 12:53:00 PM
☐	[201407021308]	4096 bytes	Aug 2, 2014 1:13:00 PM
☐	[201407030613]	4096 bytes	Aug 3, 2014 6:18:00 AM

To generate the collection files, open Task Manager and run the User CLI Collection task. If the task is scheduled with a non-default collection directory, then on the Web, log in as admin to change the default collection directory path before viewing the collected files. For more information about the User CLI task, see User CLI Collection Task in the *IP/MPLSView Java-Based Management and Monitoring Guide*.

Related Documentation

- Network Reports on page 76
- Configuration Revision Manager on page 84

Network Reports

- Understanding Network Reports on page 76
- Displaying Network Reports on page 77

Understanding Network Reports

The Network Reports feature enables you to display Web reports associated with the Live Network.

How to Prepare the Data

There are two ways to make this report available:

Copyright © 2018, Juniper Networks, Inc.

- Run the Scheduling Live Network Collection task with the **Configuration** option selected in the Collection Options window. Then save the network reports in IP/MPLSView by selecting **File > Export to Web** while in the Live Network.
- Run the Web Report task periodically with the **Use Live Network** and **General Reports** options selected in the New Task (Step 2 of 3) - Web Report window.

See Also

- Integrity Check Reports on page 78
- Hardware Inventory Reports on page 78

Displaying Network Reports

To display network reports:

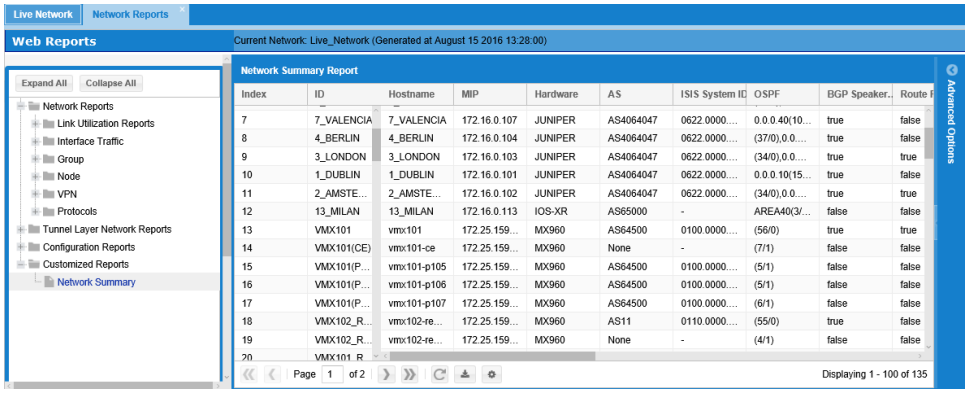
1. Select **Configuration > Network Reports**.

2. Expand the menu items in the Web Reports pane to list the individual reports. Click the report name to display the report.

   For example, in the Web Reports pane, expand Customized Reports and select **Network Summary**.

   The Network Summary Report window is displayed. Figure 57 on page 77 shows the Network Summary Report window.

Figure 57: Network Summary Report



3. The following options are available:

   - Select the **Download** icon to export the report as a CSV or text file.
   - Select the **Settings** icon to control the number of items displayed per page.
   - Expand **Advanced Options** to perform a more specific search. For example, search by hostname or IP address.

Related Documentation

- Integrity Check Reports on page 78

- Hardware Inventory Reports on page 78

Integrity Check Reports

The Integrity Check Reports feature enables you to view the available integrity checks and config reports associated with the live network. See Figure 58 on page 78.

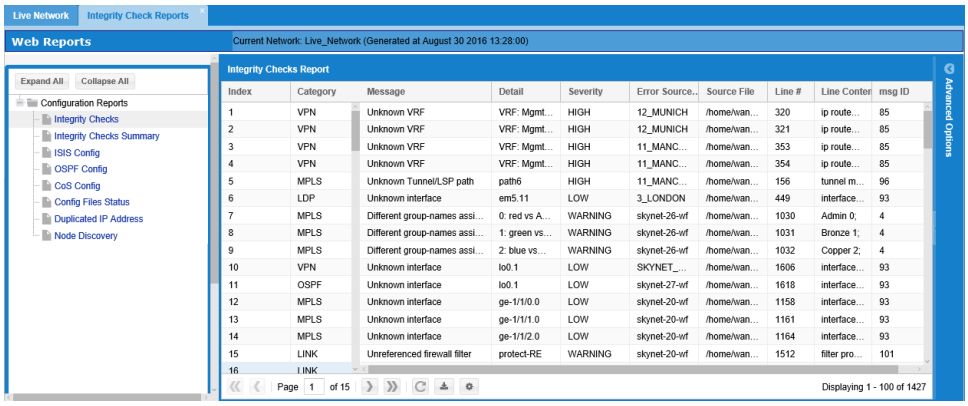
How to Prepare the Data

There are three ways to make this report visible:

- Run the Scheduling Live Network Collection task with at least the config option. Then save the network reports in the IP/MPLSView client program by selecting **File > Export to Web**.
- Schedule the Config Comparison, Conformance, and IC Report task to run periodically from the Integrity Check Report tab. Select **Use Live Network** and **Save the report to make it available on the web** options.
- Schedule the Web Report task with the **Use Live Network** and **General Reports** options checked.

NOTE: **In order for these Web reports to be visible, the Integrity Check task option "Save the report to make it available on the web" must be selected.**

Figure 58: Integrity Check Reports



Related Documentation

- Network Reports on page 76
- Hardware Inventory Reports on page 78

Hardware Inventory Reports

- Understanding Hardware Inventory Reports on page 79
- Displaying Hardware Inventory for Routers on page 80

Copyright © 2018, Juniper Networks, Inc.

- Displaying Hardware Inventory for Line Cards on page 80
- Displaying Hardware Inventory for Transceivers on page 81
- Displaying Hardware Inventory for Extensive Parts List on page 81

Understanding Hardware Inventory Reports

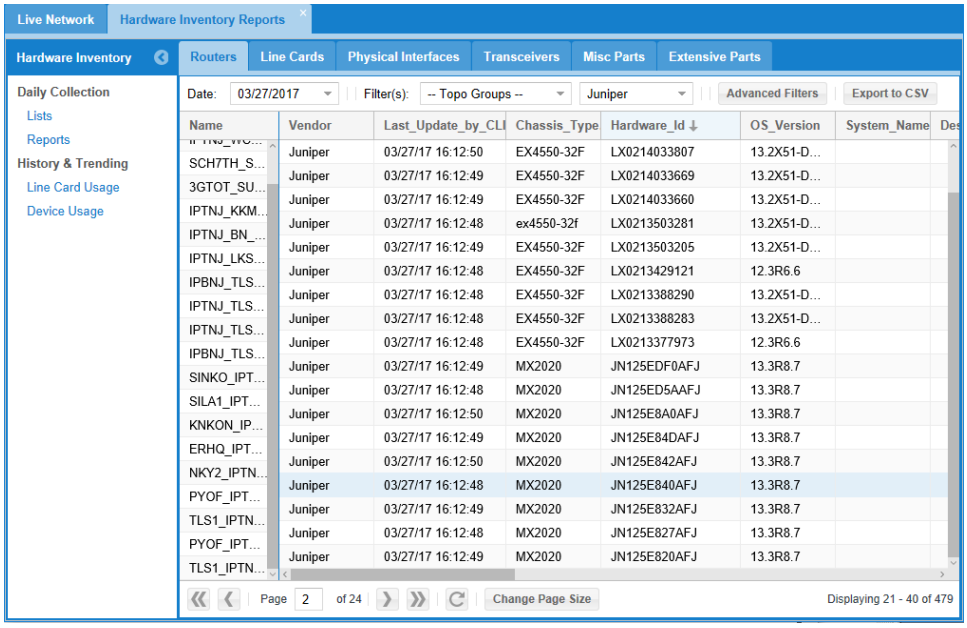
The Hardware Inventory Reports feature enables you to display the available hardware associated with the Live Network.

There are two ways to make the hardware inventory report available:

- Run the Scheduling Live Network Collection task with the **Configuration** and **Equipment CLI** options selected in the Collection Options window. Then save the network reports in IP/MPLSView by selecting **File > Export to Web** while in the Live Network.
- Run the Hardware Inventory Report task periodically with the **Live Network** and **Save Reports on the web** options selected in the New Task (Step 2 of 3) - Hardware Inventory Report window.

From the Routers tab, you can add columns that display the IPv6 addresses, autonomous system (AS) numbers, and hardware id. Figure 59 on page 79 shows a router inventory report with some of these columns hidden.

Figure 59: Hardware Inventory Reports for Devices



In the left navigation pane, select **Reports** to display device-specific reports. Select the **Hardware Inventory, Device Usage, Line Card Usage, CapEx**, or **CapEx by Parts** tab to display daily usage and estimated cost reports.

In the left navigation pane, select **Line Card Usage** or **Device Usage** to display usage reports for a specified time period.

See Also

- Equipment View on page 82

Displaying Hardware Inventory for Routers

To display a hardware inventory for routers:

1. Select **Configuration > Hardware Inventory Reports**.

   The Router tab is selected by default and the Hardware Inventory Reports window is displayed, as shown in Figure 59 on page 79.

2. (Optional) From the header menus, select a date, a topology group, or a vendor to filter the report.

See Also

- Equipment View on page 82

Displaying Hardware Inventory for Line Cards

To display a hardware inventory for line cards:

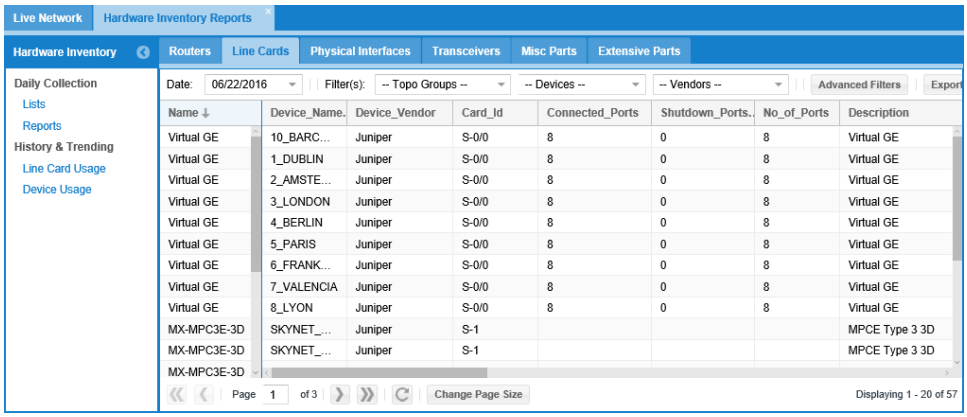
1. Select **Configuration > Hardware Inventory Reports**.

   The Hardware Inventory Reports window is displayed, as shown in Figure 59 on page 79.

2. Select the **Line Cards** tab.

   The Hardware Inventory Reports for Line Cards is displayed, as shown in Figure 60 on page 80.

Figure 60: Hardware Inventory Report Window for Line Cards



3. (Optional) From the header menus, select a date, a topology group, or a vendor to filter the report.

See Also

- Equipment View on page 82

Copyright © 2018, Juniper Networks, Inc.

Displaying Hardware Inventory for Transceivers

When a small form-factor pluggable (SFP) transceiver is connected to the port, the type of transceiver (1-Gigabit Ethernet copper, 1-Gigabit Ethernet optical, 10-Gigibit Ethernet), serial number, and other information is provided.

To display a hardware inventory for transceivers:

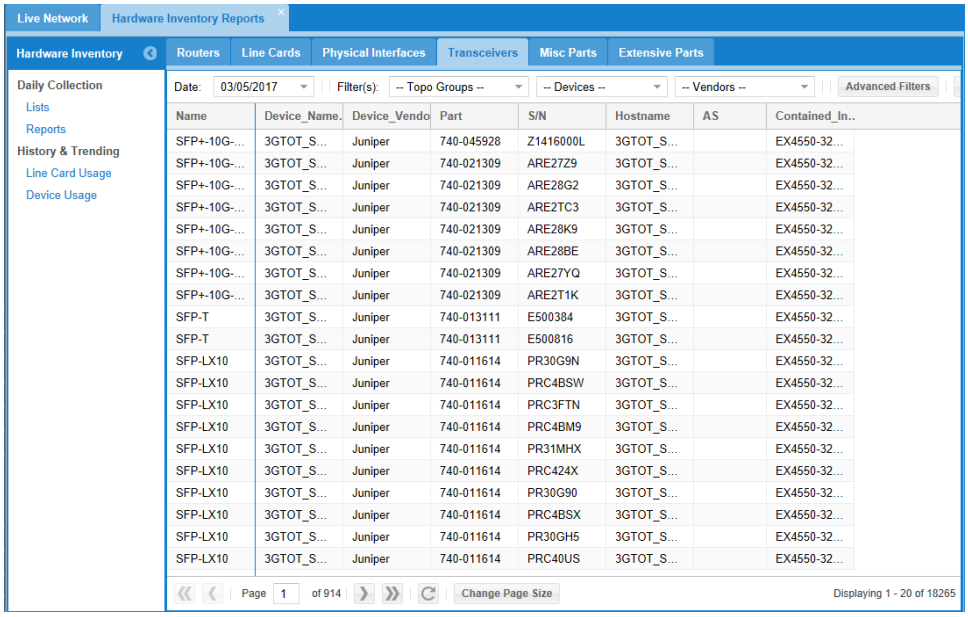
1. Select **Configuration > Hardware Inventory Reports**.

   The Hardware Inventory Reports window is displayed, as shown in Figure 59 on page 79.

2. Select the **Transceivers** tab.

   The hardware Inventory Reports for transceivers is displayed, as shown in Figure 61 on page 81.

Figure 61: Hardware Inventory Report Window for Transceivers



3. (Optional) From the header menus, select a date, a topology group, or a vendor to filter the report.

Displaying Hardware Inventory for Extensive Parts List

To display hardware inventory for extensive parts list:

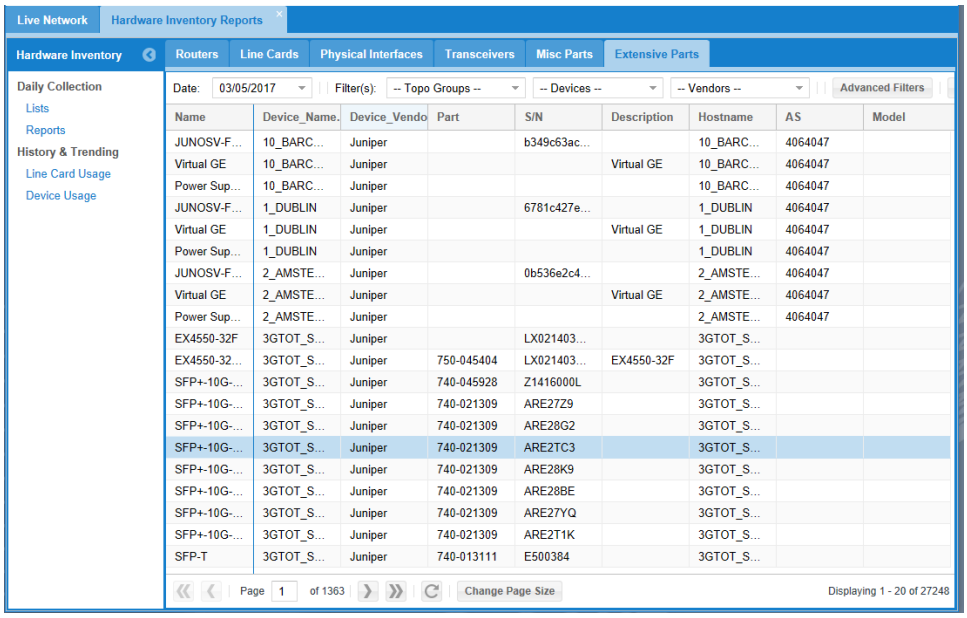
1. Select **Configuration > Hardware Inventory Reports**.

   The Hardware Inventory Reports window is displayed, as shown in Figure 59 on page 79.

2. Select the **Extensive Parts List** tab.

The Hardware Inventory Reports for Extensive Parts List is displayed, as shown in Figure 62 on page 82.

Figure 62: Hardware Inventory Report Window for Extensive Parts



3. (Optional) From the header menus, select a date, a topology group, or a vendor to filter the report.

Equipment View

- Understanding the Equipment View on page 82
- Displaying the Equipment View on page 84

Understanding the Equipment View

There are two main views in the device's Equipment View window. The Logical View depicts a graphical view of the cards and ports in the device. The Tabular View depicts in tabular format, details such as interface status and bandwidth. See Figure 63 on page 83.

Copyright © 2018, Juniper Networks, Inc.

Figure 63: Logical View

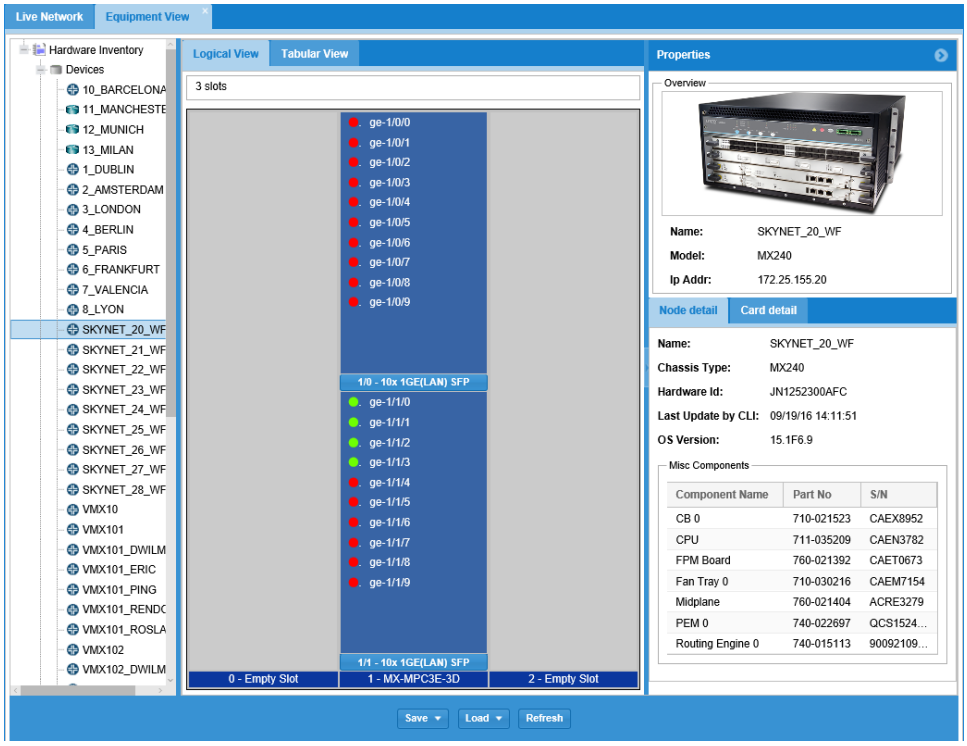


Table 21 on page 83 describes the Equipment View window.

Table 21: Equipment View Descriptions

Item	Description
Hardware Inventory pane	Select **Devices** to display a list of devices.
Logical View pane	Displays number of slots. Select an interface to display the IP address and bandwidth.
Tabular View pane	Displays the interface, admin status, operation status, IP address, and bandwidth.
Properties Overview	Provides a picture of the equipment, model, and IP address.
Node detail	Lists the device name, chassis type, hardware ID, last update by CLI, OS Version, and miscellaneous components such as board, CPU, and Routing Engine.
Card detail	Lists the slot, card ID, description, part number, serial, and ports.

See Also

- Hardware Inventory Reports on page 78

Displaying the Equipment View

To display the device equipment view:

1. Select **Configuration > Equipment View**.

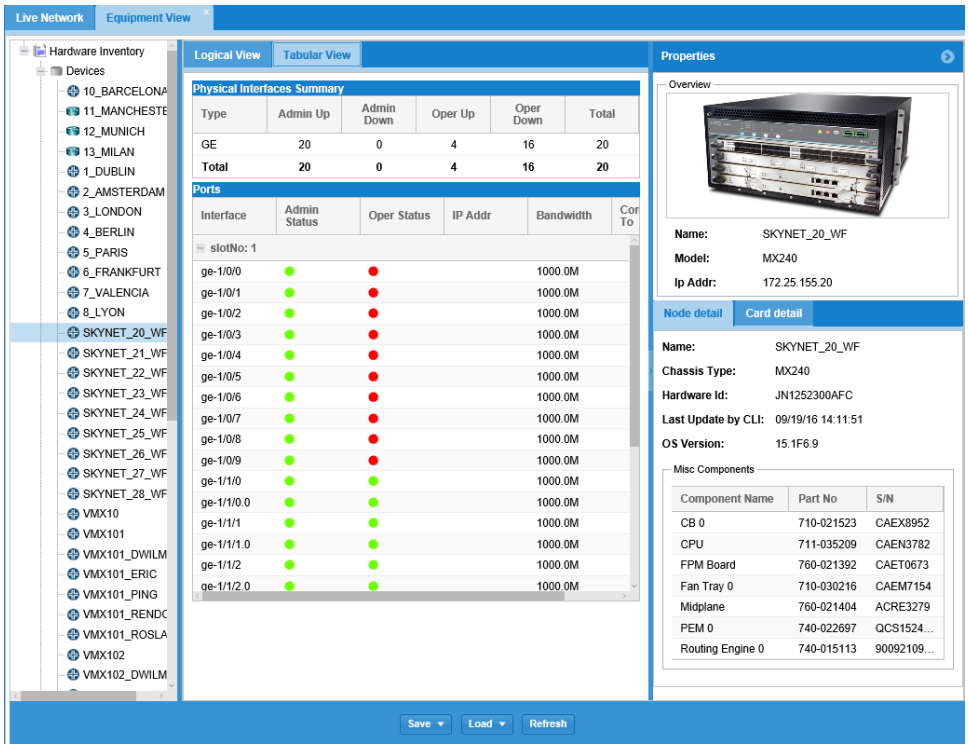
   The Hardware Inventory Summary window is displayed.

2. Expand the Devices list in the Hardware Inventory pane and select the equipment to view.

   The equipment Logical View is displayed, as shown in Figure 63 on page 83.

3. (Optional) Select the **Tabular View** tab for details such as interface status and bandwidth, as shown in Figure 64 on page 84.

Figure 64: Tabular View



See Also

- Hardware Inventory Reports on page 78

Configuration Revision Manager

- Understanding the Configuration Revision Manager on page 85
- Displaying and Comparing Configuration Revisions on page 85

Copyright © 2018, Juniper Networks, Inc.

Understanding the Configuration Revision Manager

IP/MPLSView has a revision manager that can be used to track changes to device configuration files. The Configuration Revision Manager can be used to check-in new revisions, perform comparisons, and view current or previous revision versions of a configuration file.

How to Prepare the Data

Schedule the Scheduling Live Network Collection task at a regular interval in Task Manager to perform repeated configuration file collection. This establishes a baseline of the configuration files, against which future versions of the files are compared.

See Also

- *Scheduling Live Network Collection*
- *Configuration and Tunnel Path Files*

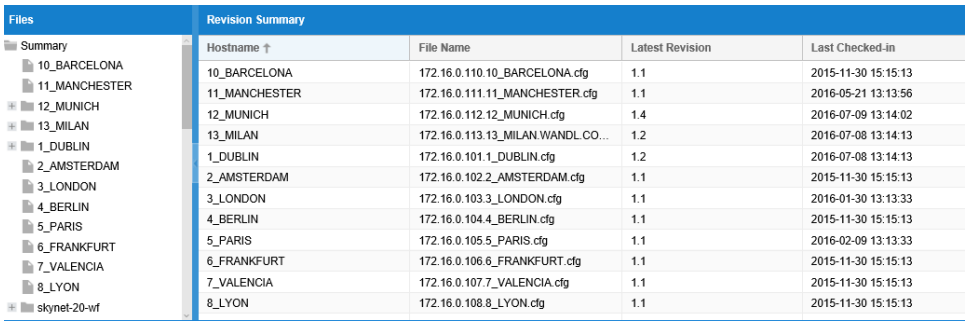
Displaying and Comparing Configuration Revisions

To display and compare configuration revisions:

1. Select **Configuration > Config Revision Manager**.

   The Revision Summary page is displayed showing the hostname, filename, latest revision, and the date that revision was checked-in. Devices are listed in the side pane. Figure 65 on page 85 shows the Revision Summary window.

Figure 65: Revision Summary



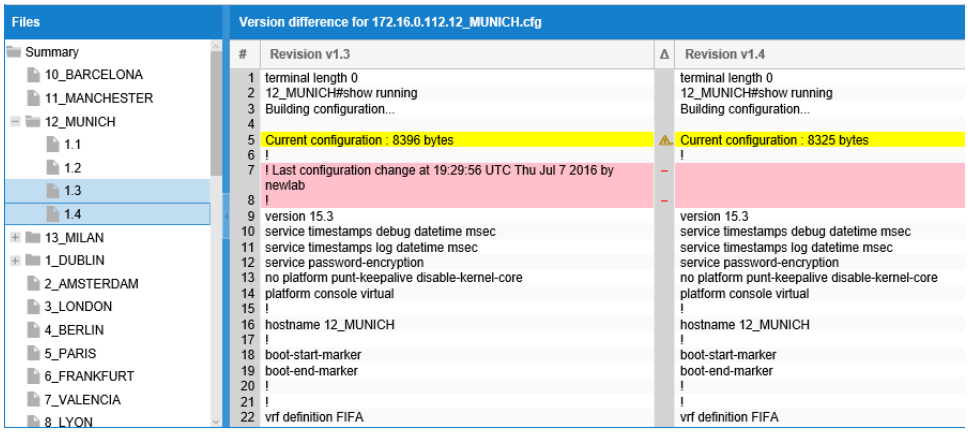
Hostname	File Name	Latest Revision	Last Checked-in
10_BARCELONA	172.16.0.110.10_BARCELONA.cfg	1.1	2015-11-30 15:15:13
11_MANCHESTER	172.16.0.111.11_MANCHESTER.cfg	1.1	2016-05-21 13:13:56
12_MUNICH	172.16.0.112.12_MUNICH.cfg	1.4	2016-07-09 13:14:02
13_MILAN	172.16.0.113.13_MILAN.WANDL.CO...	1.2	2016-07-08 13:14:13
1_DUBLIN	172.16.0.101.1_DUBLIN.cfg	1.2	2016-07-08 13:14:13
2_AMSTERDAM	172.16.0.102.2_AMSTERDAM.cfg	1.1	2015-11-30 15:15:13
3_LONDON	172.16.0.103.3_LONDON.cfg	1.1	2016-01-30 13:13:33
4_BERLIN	172.16.0.104.4_BERLIN.cfg	1.1	2015-11-30 15:15:13
5_PARIS	172.16.0.105.5_PARIS.cfg	1.1	2016-02-09 13:13:33
6_FRANKFURT	172.16.0.106.6_FRANKFURT.cfg	1.1	2015-11-30 15:15:13
7_VALENCIA	172.16.0.107.7_VALENCIA.cfg	1.1	2015-11-30 15:15:13
8_LYON	172.16.0.108.8_LYON.cfg	1.1	2015-11-30 15:15:13

2. Select a device in the side pane to display the configuration file in the main pane.

   If a device has multiple revisions, you can expand the menu item in the side pane to list the individual revisions.

3. (Optional) To compare two revisions side-by-side, select two revisions and right-click. Figure 66 on page 86 shows the Version difference window.

Figure 66: Version Difference Comparison



The configuration changes are color-coded:

- Yellow—Indicates changes in the newer version.
- Green—Indicates additions in the newer version.
- Red—Indicates changes that were deleted in the newer version.

4. (Optional) Right-click in the Revision panel and select **Print** to print the configuration that is displayed.

See Also

- *Configuration and Tunnel Path Files*

Device Library

- Understanding the Device Library on page 86
- Modifying a Web Image Icon on page 87
- Modifying the CLI Template on page 88
- Adding a New Hardware Type on page 89

Understanding the Device Library

You can manage the hardware vendor and hardware type using the Device Library. From the Device Library, you can do the following:

- Add new hardware types.
- Set images to use in the interfaces and topology map.
- Create a template of the statements to be run before executing any CLI command from the Run CLI window.

The CLI Template pane shows the file path to the template file used for CLI commands. Select **Modify** to change the CLI screen width used.

Copyright © 2018, Juniper Networks, Inc.

To add a new hardware type, select **Add**. The New Hardware Type window is displayed. Select the vendor from the Vendor Family menu, type the name of the new hardware type, and select **Save**. To delete a hardware type, select the type and select **Delete**.

The **vendortemplatefile.csv** file in the**/u/wandl/db/config/** directory contains the mapping of vendor, command template, and icon used.

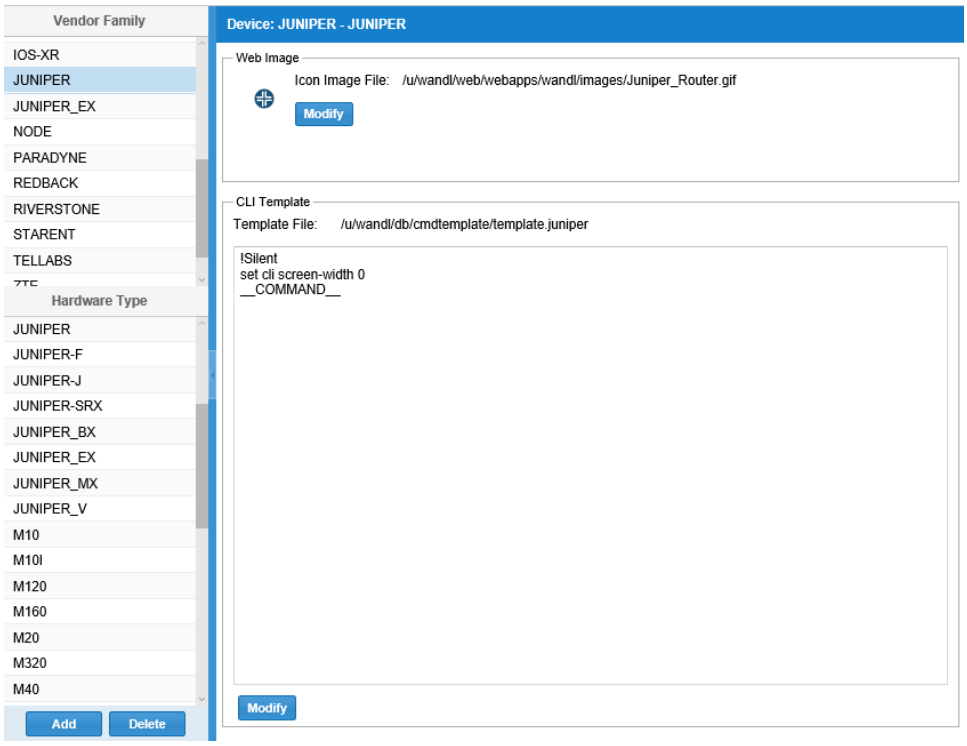
Modifying a Web Image Icon

To modify a Web image icon:

1. Select **Configuration** > **Device Library**.

   The Device Library window is displayed. The Web Image pane shows the file path to the icon file for the device selected. Figure 67 on page 87 shows the Device Library window.

Figure 67: Device Library Window



2. Select **Modify** to change the icon used for a node in IP/MPLSView.

   The Server File Browser window is displayed.

   - To display the contents of a sub-directory, double-click the directory name.
   - To return to the default directory, select the home icon.
   - To refresh the display, select the blue-circle icon.
   - To move up to the parent directory, select the up arrow icon.

3. Browse for the icon image (for example, .gif file) to display, and click **Select**.

See Also

- Hardware Inventory Reports on page 78
- Equipment View on page 82

Modifying the CLI Template

To modify the CLI template:

1. Select **Configuration > Device Library**.

   The Device Library window is displayed. The CLI Template pane shows the file path to the template file used for CLI commands. The files in this directory contain templates specifying which commands to issue immediately after logging in and before running any additional commands. Figure 67 on page 87 shows the Device Library window.

2. Select the desired Vendor Family and Hardware Type from the left pane.

3. Click **Modify** to make changes to the CLI template displayed in the lower-right pane.

   The keywords and their meanings are provided in Table 22 on page 88.

Table 22: CLI Template Keywords

Keyword	Meaning/Usage
@silent	Do not capture terminal output from now on (until an !silent is issued).
!silent	Capture terminal output from now on (until an @silent is issued).
@P	Indicates that after the subsequent command is issued, the prompt on the device will change. This is needed in order to tell the program that the subsequent command has completed.
!P	Indicates that after the subsequent command is issued, the prompt on the device will remain the same.
__COMMAND__	This will be substituted with whatever command(s) a particular run CLI command includes.

As an example, the following template says a) Do not capture the output after issuing the commands **cli set terminal rows 0** and **enable**, b) Capture the output of the CLI command, and c) Do not capture the output of the **exit** command.

```
@Silent
cli set terminal rows 0
enable
!Silent
__COMMAND__
@Silent
exit
```

Corresponding Text Files

Copyright © 2018, Juniper Networks, Inc.

Table 23 on page 89 describes the corresponding text files that are modified by the changes in the Device Library graphical interface:

Table 23: Text File Descriptions

Item	Description
vendortemplatefile.csv	(located in **/u/wandl/db/config/**) Contains a mapping of the vendor, command template, and icon used.
hardwaretypemapping.csv	(located in **/u/wandl/db/config/**) Contains a mapping of recognized device models with their vendors.
template.vendor	(located in **/u/wandl/db/cmdtemplate/,** one file per vendor; for example, template.cisco) Files specify which commands are issued on devices immediately after logging in, before any additional commands are run. A few reserved IP/MPLSView keywords are defined as described in Table 22 on page 88.

See Also

- Hardware Inventory Reports on page 78
- Equipment View on page 82

Adding a New Hardware Type

To add a new node hardware type:

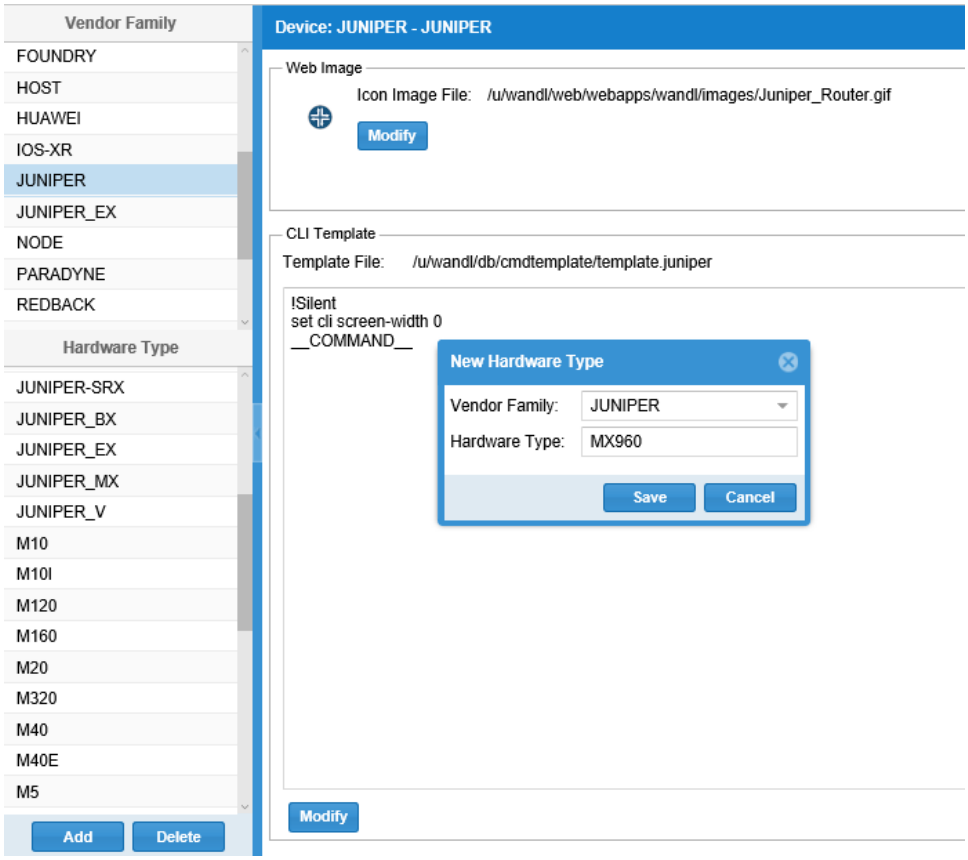
1. Select **Configuration > Device Library**.

   The Device Library window is displayed.

2. Select **Add** in the left pane.

   The New Hardware Type window is displayed. Figure 68 on page 90 shows the New Hardware Type window.

Figure 68: New Hardware Type



3. Select the vendor from the list, enter the hardware type, and click **Save**.

4. (Optional) To delete a hardware type, select the hardware type and select **Delete**.

Related Documentation

- Hardware Inventory Reports on page 78
- Equipment View on page 82

Miscellaneous Reports

To access Miscellaneous Reports, select **Configuration > Misc Reports**.

The Interface VLANs Assignment feature provides a list of the interfaces in the Live Network and the virtual LAN that each belongs to (if any).

Select **Configuration > Misc Reports > Interface VLANs Assignment**. Select the vlanid from the Select **vlanid** drop-down box, or type it directly into the text field to the right, to search for all the interfaces belonging to a particular VLAN. (See Figure 69 on page 91.) Select **None** to see all interfaces that do not have any associated vlanid. Select **All** to see all

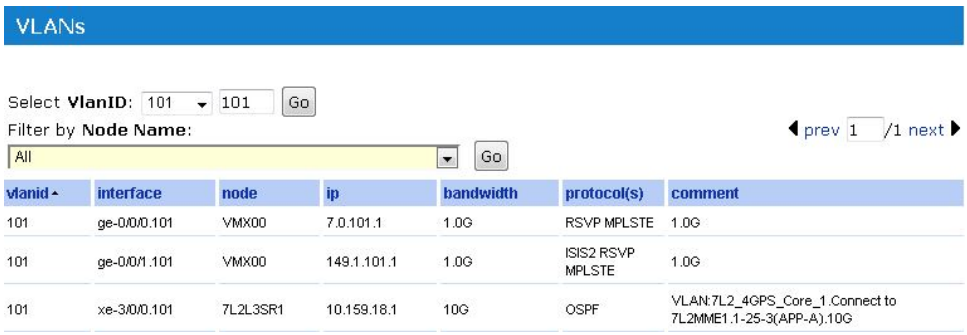
Copyright © 2018, Juniper Networks, Inc.

interfaces in the network. If the vlanid for a particular entry says n/a (data not available), then that interface does not belong to a VLAN.

You can also search for all interfaces at a particular node by using the Filter by node name text field. This filter is case-sensitive and the full node name should be entered (no regular expressions).

NOTE: Both the Select vlanid and Filter by node name options always search from within all interfaces in the network.

Figure 69: View VLANs



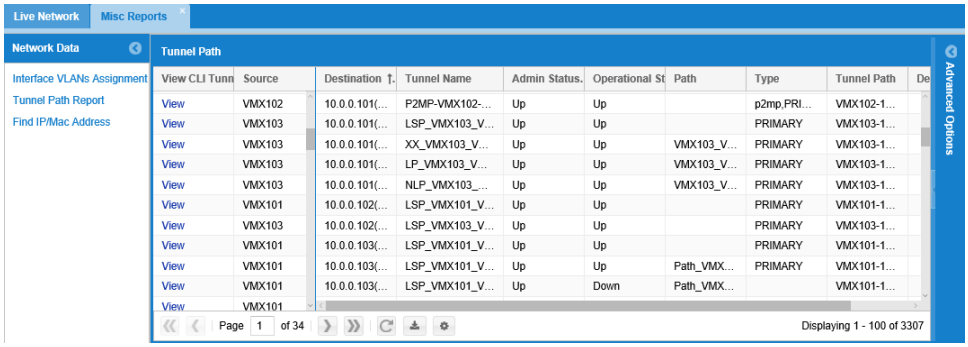
vlanid	interface	node	ip	bandwidth	protocol(s)	comment
101	ge-0/0/0.101	VMX00	7.0.101.1	1.0G	RSVP MPLSTE	1.0G
101	ge-0/0/1.101	VMX00	149.1.101.1	1.0G	ISIS2 RSVP MPLSTE	1.0G
101	xe-3/0/0.101	7L2L3SR1	10.159.18.1	10G	OSPF	VLAN:7L2_4GPS_Core_1.Connect to 7L2MME1.1-25-3(APP-A).10G

As long as a collection of “config” and “interface” have been performed from the Task Manager using either CLI Collection, Autodiscovery, or Scheduling Live Network Collection, this data will be accessible.

NOTE: The data within the View VLANs page is derived from the IP/MPLSView interface map (intfmap) file. The intfmap file is created automatically when configuration files are collected and parsed.

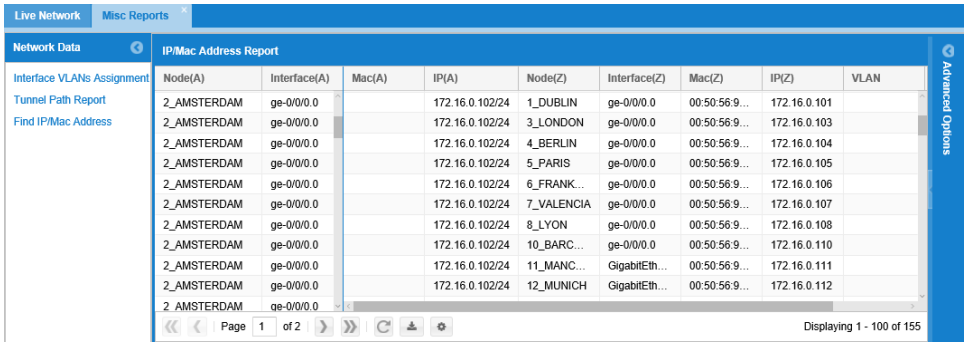
The Tunnel Path Report feature provides reports about the tunnel status and tunnel path detail (for example, the “Record Route”) based on the same command used for the “tunnel path” collection method. The IP addresses are automatically resolved to the corresponding router and interface for convenience. To view this report, run the Scheduling Live Network Collection Task with **config**, **Tunnel Path**, and **Transit Tunnel** options selected. To access the report, select **Configuration > Misc Reports > Tunnel Path Report**. Figure 70 on page 92 shows a tunnel path report.

Figure 70: Tunnel Path Report



The Find IP/Mac Address feature provides reports about IPs and MAC Addresses in the network. To view this report, run the Scheduling Live Network Collection Task with the **config** and **ARP** options selected. To access the report, select **Configuration > Misc Reports > Find IP/Mac Address**.

Figure 71: IP/Mac Address Report



Related Documentation

- Network Reports on page 235

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 5

Fault Management: Events

- Live Event Browser on page 93
- Analyzing Events on page 100
- LSP and Related Tunnel Events for LinkDown and LinkUp on page 103
- Historical Event Browser on page 107
- Error and Discard Chart for Interface Threshold Events on page 110
- Events Count Chart on page 111
- Event Summary Reports on page 114
- Event Options on page 116

Live Event Browser

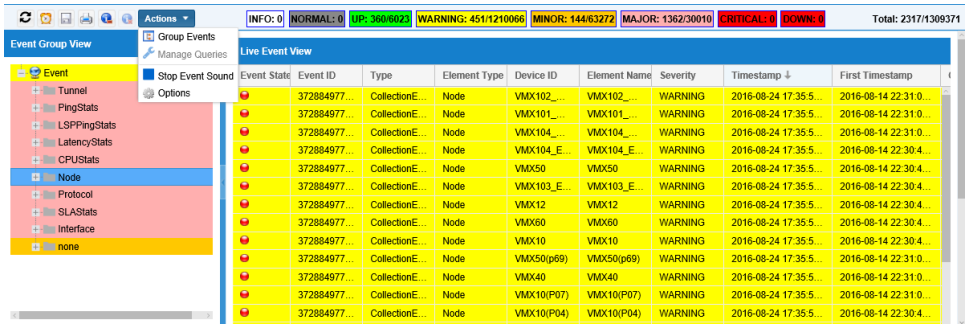
- Launching the Live Event Browser on page 93
- Acknowledging and Clearing Events on page 94
- Creating a Group Event on page 95
- Creating a New Query on page 96
- Configuring the Severity Colors on page 97
- Uploading Event Sound Clips on page 98
- Stopping Event Sounds on page 99

Launching the Live Event Browser

The Live Event Browser is used to view events and SNMP traps from devices in the Live Network and can be accessed from the Live Network by selecting **Fault > Live Event Browser**. For information about how to use the Event Browser, and the differences between the Live and Historical view, see *Fault Management: Events Overview* in the *IP/MPLSView Java-Based Management and Monitoring Guide*.

Figure 72 on page 94 shows the Live Event Browser window and Action options.

Figure 72: Live Event Browser



The Action options are accessed by selecting **Fault > Live Event Browser**.

From the Actions menu, the following options are available:

- Group Events

  You can group events by various attributes such as Device ID, Severity, or Type of event. Grouping by one property creates one level of groups below the global Events group. Grouping by a second property creates a second level of groups, and so on. These groups are displayed in a tree structure in the Event Group View in the left panel.

- Manage Queries

  You can create queries for the events collected. The Historical Event Queries window allows you to create new, edit, and delete queries.

- Stop Event Sound

  If the play event severity sound clips feature is configured, select **Stop Event Sound** to silence the sound.

- Options

  In the Event Browser Options window, you can configure the color associated with each severity level. General options for the event browser display are also available. The general options are explained in detail in *Event Browser Options* in the *IP/MPLSView Java-Based Management and Monitoring Guide*.

See Also

- Analyzing Events on page 100
- Historical Event Browser on page 107
- Event Summary Reports on page 114

Acknowledging and Clearing Events

Acknowledging and clearing events are used to track events that require attention. An event is acknowledged when you notice the event, but have not yet taken action in response to the event. Once you have rectified the event and taken any other actions required by the event, you usually clear the event.

Copyright © 2018, Juniper Networks, Inc.

Note that events of all severity types except INFO can be marked as acknowledged. To toggle the display of info events, click the **Toggle INFO Events** icon in the top toolbar. To clear all INFO events from the Live Event View, click the**Clear all INFO Events** icon in the top toolbar. Cleared events can still be queried in Historical Event Browser, explained in "Historical Event Browser" on page 107.

To acknowledge or clear an event, right-click on the event and select **Acknowledge Events** or **Clear Events**. Once an event is acknowledged, it can be unacknowledged by selecting **Unacknowledge Events**.

Multiple events can be acknowledged or cleared simultaneously by selecting the desired events and right-clicking on the selection.

Once cleared, an event is no longer visible in the Live Event View window. Cleared events can only be queried in Historical Event Browser, explained in "Historical Event Browser" on page 107.

Creating a Group Event

To create a group event:

1. Select **Fault > Live Event Browser**.

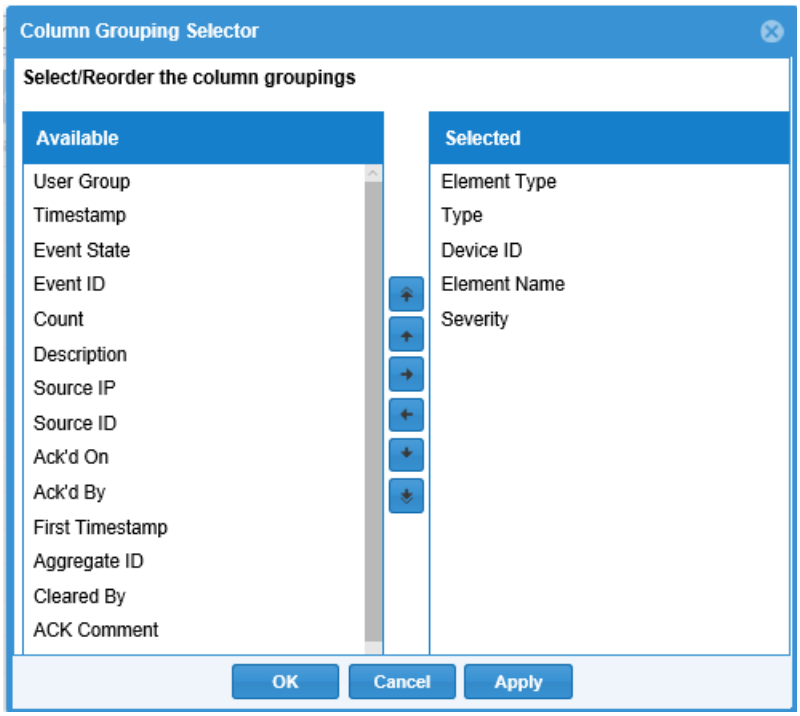
   The Live Event Browser is displayed.

2. Select **Actions > Group Events**.

   The Column Grouping Selector dialog box is displayed.

   Figure 73 on page 96 shows the Column Grouping Selector dialog box.

Figure 73: Column Grouping Selector



3. In the Column Grouping Selector dialog box, double-click the column name in the Available pane to select which columns to group by.

   When multiple columns are selected, events will be grouped hierarchically according to their order within the list, starting from the top of the list. Rearrange the grouping order by selecting a checked column and selecting **Move Up** or **Move Down**.

4. Click **Apply** for the changes to take effect, and then click **OK** to close the dialog box.

See Also

- Analyzing Events on page 100
- Historical Event Browser on page 107
- Event Summary Reports on page 114

Creating a New Query

To create a new query:

1. Select **Fault > Historical Event Browser**.

   The Historical Event View is displayed.

2. Select **Actions > Manage Queries**.

Copyright © 2018, Juniper Networks, Inc.

3. In the Historical Event Queries window, click **New**.

   The New Event Query window is displayed.

4. Select the check box for the query attribute, then select a value from the list.

5. Enter the name of the query and click **OK** to save the query entry.

   The Historical Event Queries window is displayed. Query entries are displayed in the top panel, and the query description is displayed in the bottom panel.

6. Select the query entry and click **Run Query**.

See Also

- Analyzing Events on page 100
- Historical Event Browser on page 107
- Event Summary Reports on page 114

Configuring the Severity Colors

To configure the severity colors:

1. Select **Fault > Live Event Browser**.

   The Live Event Browser is displayed.

2. Select **Actions > Options**.

   The Event Browser Options window is displayed.

Figure 74: Event Browser Options

3. Click the colored box next to the severity level that you want to configure.

4. In the color selector window, select a color or enter a hex color code, and click **OK**.

See Also

- Live Event Browser on page 93

Uploading Event Sound Clips

You can associate an event with a sound clip according to the event severity. Sound clips can be uploaded from either the application server or your local file system. The sound file format can be **.wav**, **.mps**, or **.ogg**. Also, the sound file format is dependent on whether the browser supports that format.

To upload event sound clips:

1. Select **Fault > Live Event Browser**.

   The Live Event Browser is displayed.

2. Select **Actions > Options.**

   The Event Browser Options window is displayed.

3. Select **Edit event severity sound clips**.

Copyright © 2018, Juniper Networks, Inc.

The Edit Event Sound Clips window is displayed.

4. Click the plus sign (+) in the right pane.

   A row is added for the sound clip.

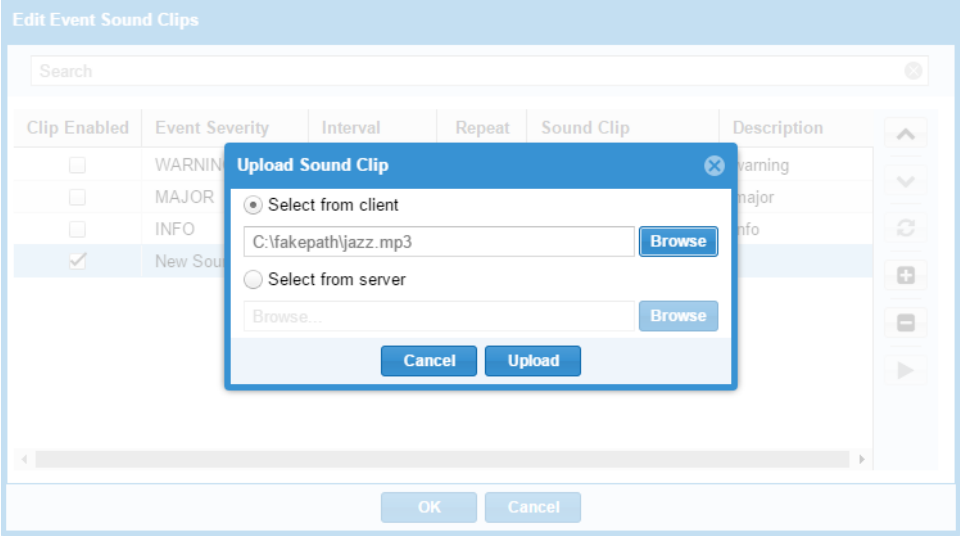
5. In the new sound clip row and in each column, select from the drop-down list:

   Event Severity—From the list, select the severity level.

   Interval—From the list, select the time interval duration, specified in seconds.

   Sound Clip—Select to display the Upload Sound Clip window. The Upload Sound Clip window is displayed in Figure 75 on page 99.

Figure 75: Upload Sound Clip



6. Select one of the following options, then select **Browse** to locate the clip:

   Select from client—Uploads a sound clip from the local file system.

   Select from server—Uploads a sound clip from the application server.

7. Select **Upload** to upload the sound clip to the server.

   The sound clip is uploaded to the **/u/wandl/app/NodeJS/client/resources/audio** directory.

Stopping Event Sounds

To stop event sounds:

1. Select **Fault > Live Event Browser**.

   The Live Event Browser is displayed.

2. Select **Actions > Stop Event Sound** to silence the alert.

See Also

- Live Event Browser on page 93

Analyzing Events

- Understanding Root Cause Analysis on page 100
- Analyzing an Event on page 102

Understanding Root Cause Analysis

Root Cause Analysis (RCA) is a fault management feature located in the Live Event Browser that allows you to diagnose trap events and recommend corrective actions. It is accessed by right-clicking an event and selecting Analyze Event from the menu. This feature references a list of rules defined for a device and event type, performs user-defined actions on the device, searches the output of those actions, and highlights if the expected results of the actions are found. The expected results can be used to diagnose the cause of the event and offer suggestions for further action.

Root Cause Analysis helps you analyze the root cause of the events based on user-defined rules in the **/u/wandl/db/config/rca-rules** file. You can define various commands such as SNMP and CLI to query event specific details or you can define rules to generate an event. After the rca-rules list is defined, these rules will appear in the Root Cause Analysis window. You can select and execute one or more commands in the RCA Rules pane. Selected commands are executed and the results and status are updated. Figure 77 on page 103 shows the Root Cause Analysis window and the RCA Rules pane.

Each rule in the **rca-rules** file should be in a single line and in the following format:

<vendor>, <type>, <action>, <expected-result>, <probable-cause>

RCA Rules Field Explanations:

vendor—Name of the device vendor. For example, **cisco, juniper, huawei**

type—Name of the SNMP trap. For example, **linkUp, linkDown, jnxVpnPwDown**

action—Command executed through the device CLI, command executed on the application server, SNMP query, or post an event. Conditional actions can be defined too.

expected-result —String that will be searched and highlighted from the output of the defined action. For example, **line protocol is down**. Supports variables such as (ElementName), simple regular expressions, and logical operators **&&** and **||**.

probable-cause—Message displayed to offer suggestions for action. For example, check cable connection.

RCA Rules Command Results:

Copyright © 2018, Juniper Networks, Inc.

<expected-result> found—Command status is updated as **Matched** and the matching text is highlighted in the command result with yellow color.

<expected-result> not found—Command status is updated as **Not Matched**.

<expected-result> is not defined for the rule—After successful completion of the command, the status is updated as **Executed**.

RCA Rules General Keywords:

ElementName—Corresponds to the Element Name variable in the Event Browser.

Device—Corresponds to the Device ID variable in the Event Browser.

#—Use to comment out a line and it will not be parsed in the file.

RCA Rules Action Commands:

@cli:<command>—Specifies the action taken is a command on the device CLI. For example, @cli:show interface.

@sh:<command>—Specifies the action taken is a command on the application server. For example, @sh:/u/wandl/bin/status_mplsview

@snmp:<OID>—Specifies the action taken is a SNMP query on the OID value. For example, @snmp:1.3.6.1.2.1.1.1.0

RCA Rules Conditional Action

Only the action command @cli: or @sh: or @snmp is required in the action field. The labelname:, @match:, and @notmatch: are optional keywords used for conditional action statements. If an action command is not specified, the root cause analysis parser will attempt to identify the type of command although it is recommended to define the action command type.

Format of conditional action field— labelname: [@cli: | @sh: | @snmp:] @match:@notmatch

<labelname:>—Tags an action with a label used for conditional actions. For example, mylabel:

@match:—<labelname:> skips to the line of the labelname if the expected-result matches.

@notmatch:—<labelname:> skips to the line of the labelname if the expected-result does not match.

exit—Ignores all the remaining rules and exits the root cause analysis.

See Also

- Live Event Browser on page 93

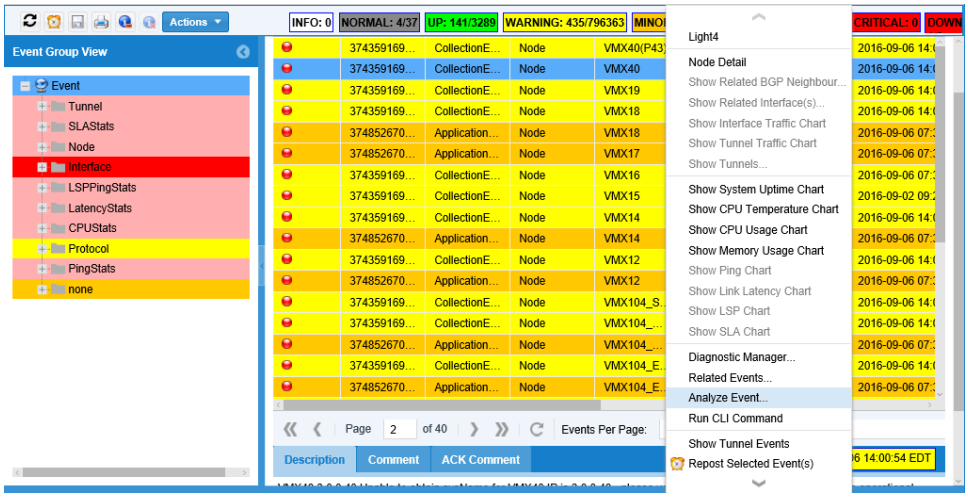
Analyzing an Event

To analyze an event:

1. Select **Fault > Live Event Browser**.

   The Live Event Browser window is displayed. The following figure shows the Live Event Browser window with Analyze Event selected.

   Figure 76: Selection for Analyze Event



2. Select the event, right-click, and select **Analyze Event**.

   The Root Cause Analysis window is displayed.

3. Select an event in the top pane.

4. In the RCA Rules pane, select the commands to use to analyze the event, and then click **Analyze**.

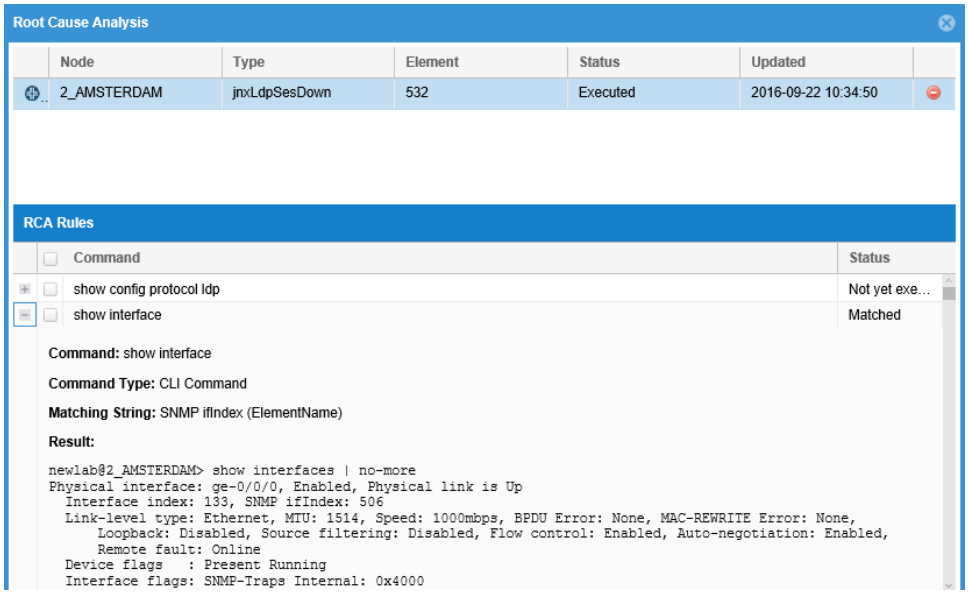
   The commands are executed on the node.

5. Expand the command in the RCA Rules pane to display the results.

   Figure 77 on page 103 shows the Root Cause Analysis window and RCA rules command results.

Copyright © 2018, Juniper Networks, Inc.

Figure 77: Root Cause Analysis Results



See Also

- Live Event Browser on page 93

LSP and Related Tunnel Events for LinkDown and LinkUp

- Correlation of Interface Index and Tunnel Index on page 103
- Mapping the Interface Index to Interface Name on page 104
- LSPs and Associated LSP Events on page 106
- Displaying LSP Events During LinkDown on page 106

Correlation of Interface Index and Tunnel Index

When there is correlation of the interface index and tunnel index, the following applies:

- Interface index and tunnel index information is collected from the network.
- Interface and tunnel details are updated in interface and tunnel events by using their index information.

Two separate tasks collect the interface index and tunnel index information by using SNMP polling. The collected information is then used to update the interface and tunnel events by correlating the index (Element Type) with the corresponding component (Element Name).

The correlation is accomplished by configuring the following two items in the SNMP Trap Editor:

- Map the interface index (Element Type) to Interface Name (Element Name).
- Map the tunnel index (Element Type) to LSP Name (Element Name).

Run the Use-Defined SNMP Collection task to collect the interface index and tunnel index information.

Mapping the Interface Index to Interface Name

Launch the SNMP Trap Editor from the Live Event Browser to configure the SNMP traps.

To map the interface index to the interface name:

1. Select **Fault > Live Event Browser**.

   The Live Event Browser is displayed.

2. In the Live Event View pane, right-click the interface that you want to configure.

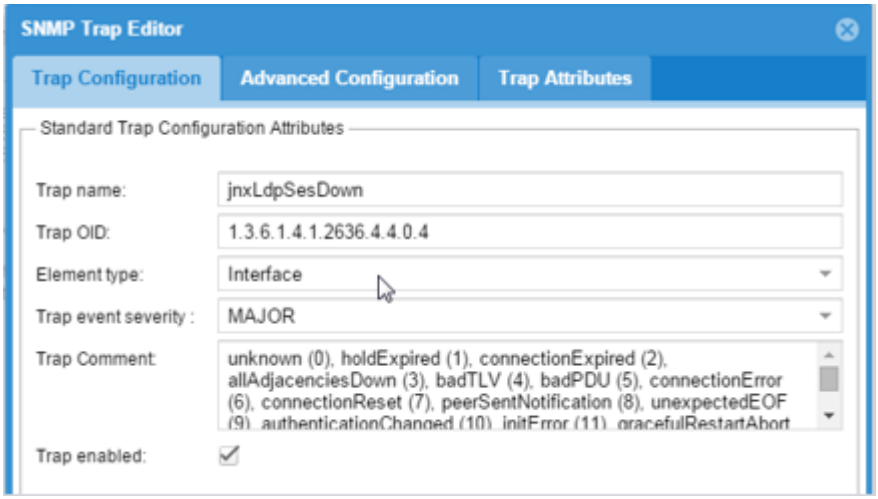
   The SNMP Trap Editor window is displayed.

3. Select the Trap Configuration tab and in Element type, select **Interface** from the drop-down list.

   You can specify the trap name, trap OID, severity, and a comment. For trap event types that used interface or tunnel indexes for correlating element names, the proper names will be updated. For example, original mplsTunnelDown event with tunnel index 12345 will be mapped to a tunnel name like Lsp12345. The jnxLdpSesDown trap with an interface index 123, will be mapped to ge-0/1/0.1.

   Select or clear the Trap enabled check box to control whether or not the SNMP trap server can process the trap. Figure 78 on page 104 displays the Trap Configuration tab.

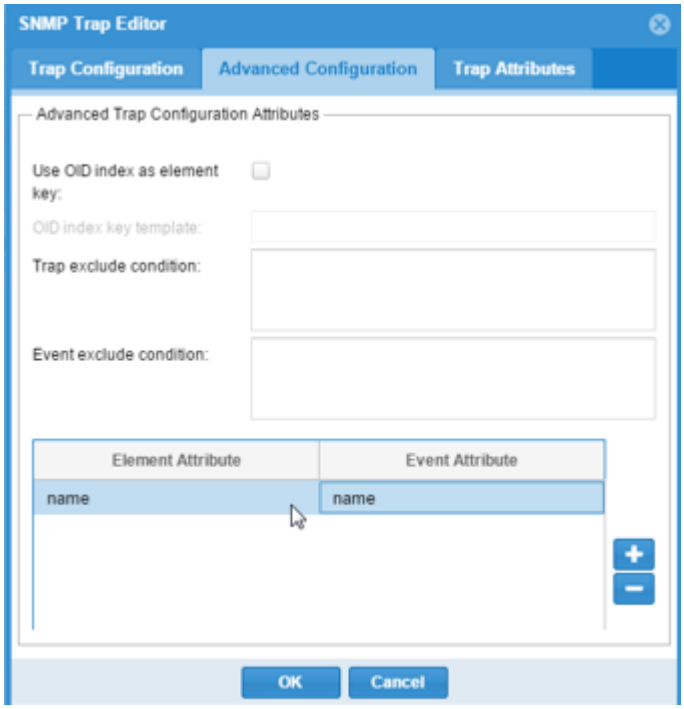
Figure 78: SNMP Trap Editor Trap Configuration Tab



4. Select the Advanced Configuration tab and in both the Element Attribute column and Event Attribute column, click the plus sign (+) and add the attribute **name**. Figure 79 on page 105 displays the Advanced Configuration tab.

Copyright © 2018, Juniper Networks, Inc.

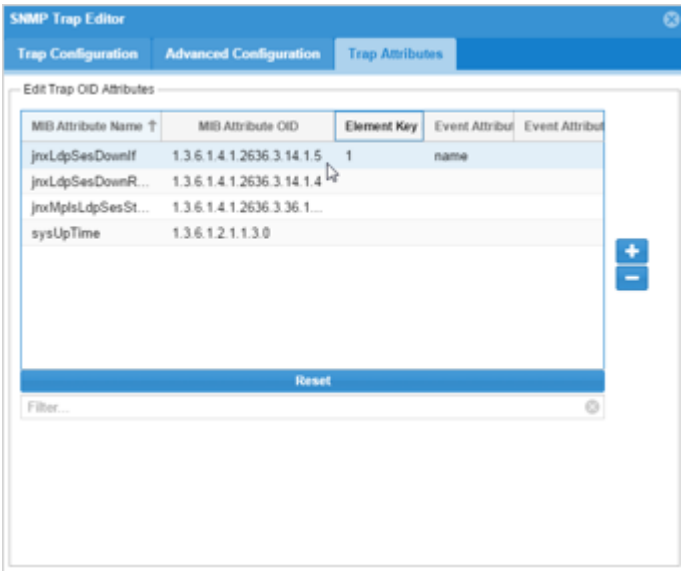
Figure 79: SNMP Trap Editor Advanced Configuration Tab



5. Select the Trap Attributes tab. The Trap Attributes tab contains a list of the various MIB Attribute OIDs associated with this trap and the corresponding MIB Attribute name. The OIDs used as the key to identify the trap with its associated network element are indicated in the Element Key Priority column with nonzero values starting with “1.”

   The Event Attribute column is used to map the value from the trap to the appropriate column of the Event Browser. In the case of the jnxLdpSesDown trap, the keyword “name” in the Event Attribute column refers to the interface name, since the element type configured on the Trap Configuration tab is the interface.

Figure 80: SNMP Trap Editor Trap Attributes Tab



6. (Optional) Click **Reset** to automatically fix incorrect OIDs entered previously.

LSPs and Associated LSP Events

LinkDown and LinkUp events include the affected interface name that is associated with a link. If an interface becomes up or down, it impacts the associated link and LSPs. Using both endpoint IP addresses of the link, impacted LSPs are identified. A panel in the Live Event Browser shows all the impacted LSPs and the associated LSP events.

Displaying LSP Events During LinkDown

To display LSP events during LinkDown:

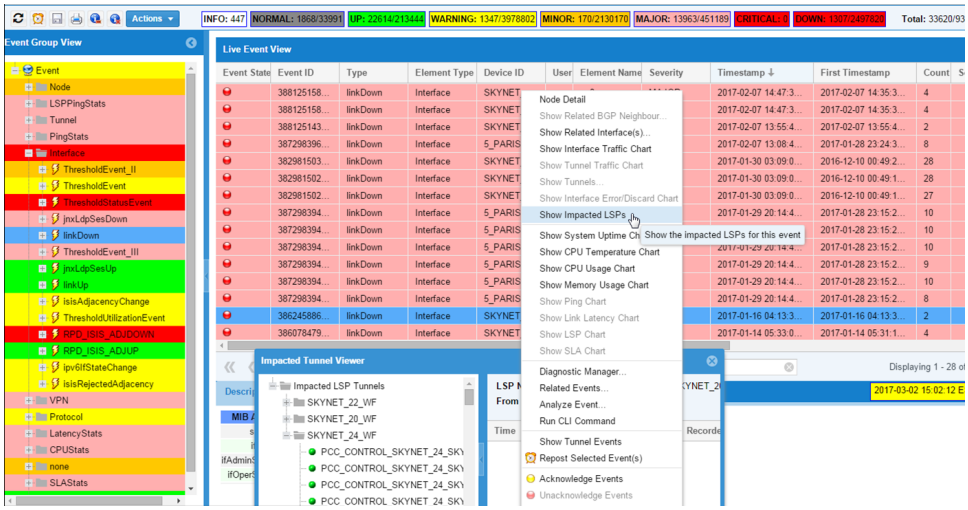
1. Select **Fault > Live Event Browser**.

   The Live Event Browser is displayed.

2. In the Live Event View pane, select the interface to check with the LinkDown type, and then right-click and select **Show Impacted LSPs**, as shown in Figure 81 on page 107.

Copyright © 2018, Juniper Networks, Inc.

Figure 81: Show Impacted LSPs



The impacted LSPs for the event are displayed in the Impacted Tunnel Viewer window. Figure 81 on page 107 displays the Impacted Tunnel Viewer.

Historical Event Browser

NOTE: **For an event to be displayed in the historical event browser, it must first be cleared in the Live Event Browser.**

To display the Historical Event Browser:

1. Select **Fault > Historical Event Browser**.

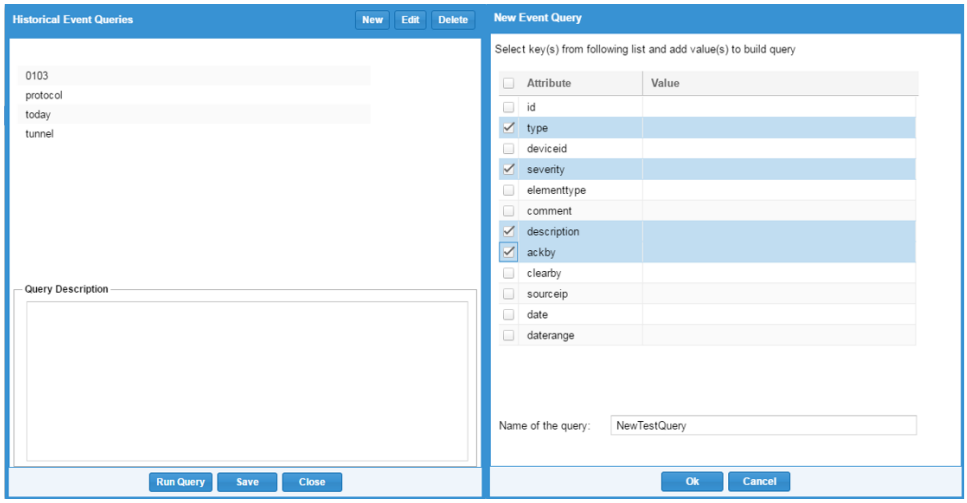
2. Select **Actions > Manage Queries** to display events in the historical event browser.

   The Historical Events Query window is displayed.

3. In the Historical Events Query window, select **New**. The New Event Query window is displayed.

4. Select the attributes you want, select a value from the menu in the field, and then click **OK**.

Figure 82: Historical Event Queries and New Event Query Window



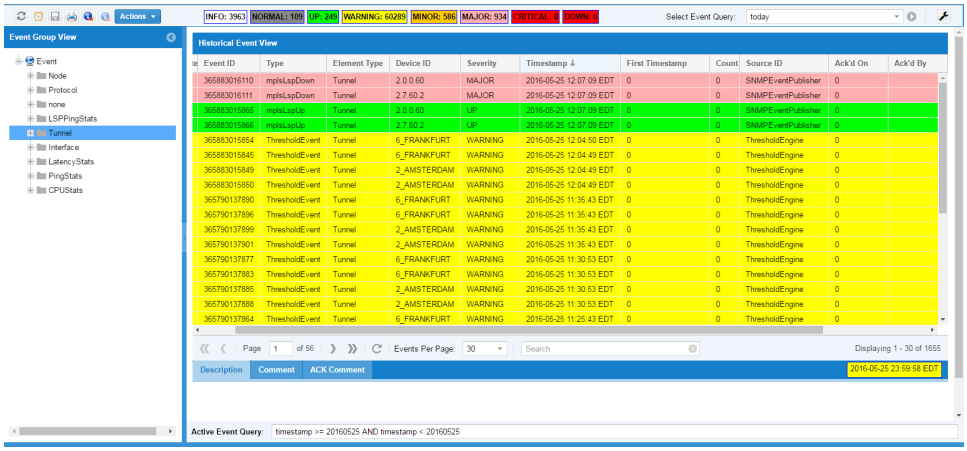
5. From the Select values window, select from the available values and click the arrow. The value is added to the New Event Query window.

6. Type a name in the **Name of the query** field and click **OK**.

7. In the Historical Event Queries window, click **Run Query**.

   The results are displayed in the Historical Event Browser window.

Figure 83: Historical Event Browser Window



Events are colored. By default, critical events are red, warnings are yellow, and major events are pink.

Icons at the top of the window are used to synchronize events with the Event Server, post network events, save events to a file, print events, toggle INFO events, and clear all INFO events.

Select an event to display event details in the lower pane of the window.

Copyright © 2018, Juniper Networks, Inc.

Table 24 on page 109 describes the Historical Event Browser table columns.

Table 24: Historical Event Browser Table Columns

Column Name	Description
Event State	The state of the event.
Event ID	The unique ID of the event. If the row corresponds to an aggregate event, this is the ID of the most recent event in the aggregated events.
Type	Supplied by the device sending the event, and is usually a terse description of the information represented by the event For example, linkUp, mplsLspDown. Event types are defined in the **/u/wandl/db/config/eventtypes.store** file.
Element Type	The element associated with the event; for example, Interface, Tunnel, VPN.
Device ID	Usually the hostname of the device. These names are derived from files created by a Scheduling Live Network Collection task in the Task Manager.
Element Name	The name of the element. For example, if the element type is Interface, the element name might be ge-0/0/3.0.
Severity	The severity of the event can be INFO, UP, WARNING, MINOR, MAJOR, CRITICAL, or DOWN. These are automatically set by default for each event, but can also be customized.
Timestamp	The time the event occurred, using the server's time zone. For aggregate events, this is the time the most recent event occurred.
First Timestamp	For aggregate events only, the timestamp of the first event in the aggregated events.
Count	For aggregate events only, the number of events included in the aggregate event.
Source IP	The IP address of the device sending the event.
Source ID	The identifier of the device sending the event.
Ack'd On	The time the event was acknowledged.
Ack'd By	The name of the user who acknowledged the event.
Aggregate ID	Identifier for the aggregate event.
Cleared By	The name of the user who cleared the event.

Note that the number of rows in the events table cannot be the same as the number of events due to aggregation of events. Events that share the same Event Type, Device ID, Element Type, and Element Name are grouped together into one row representing an aggregate event in order to reduce clutter in the Event Browser.

Copyright © 2018, Juniper Networks, Inc.

Related Documentation

- Live Event Browser on page 93
- Events Count Chart on page 111

Error and Discard Chart for Interface Threshold Events

The Error and Discard Chart displays the error and discard counts relative to time for a specific interface—for example, the number of errors and inbound and outbound packets that are discarded per second. The chart is only applicable for interface threshold events.

The Error and Discard Chart in the Live Event Browser queries the error and discard counts for a specific interface of a specific device. In addition to the chart, a table is displayed that contains all the counts returned in the query result. The grid includes Timestamp, Ingress Error Count, Egress Error Count, Ingress Discard Count, and Egress Discard Count.

To display the Error and Discard Chart for interface threshold events:

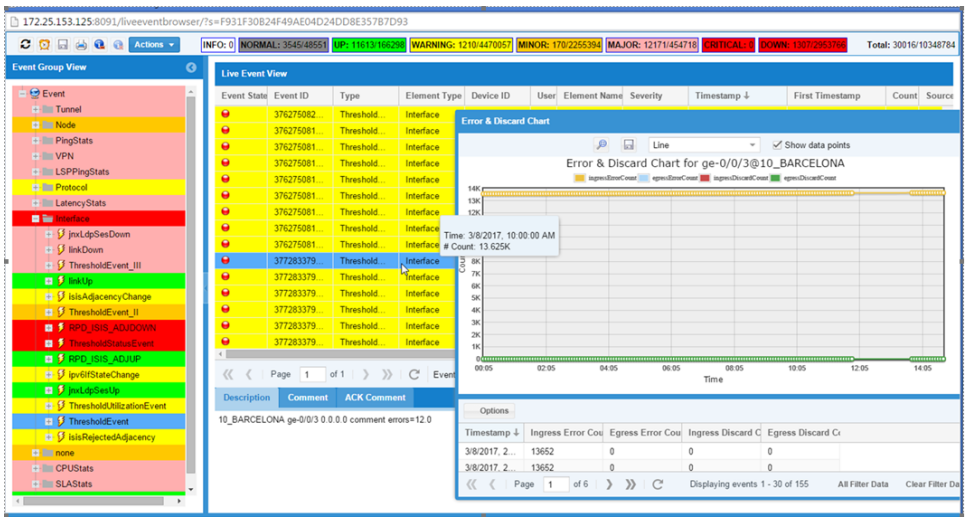
1. Select **Fault > Live Event Browser**.

   The Live Event Browser window is displayed.

2. Select the interface threshold event in the Live Event View window, right-click, and select **Show Error and Discard Chart**.

   The Error and Discard Chart for the interface is displayed. Figure 84 on page 110 shows the chart.

Figure 84: Error and Discard Chart



Copyright © 2018, Juniper Networks, Inc.

Events Count Chart

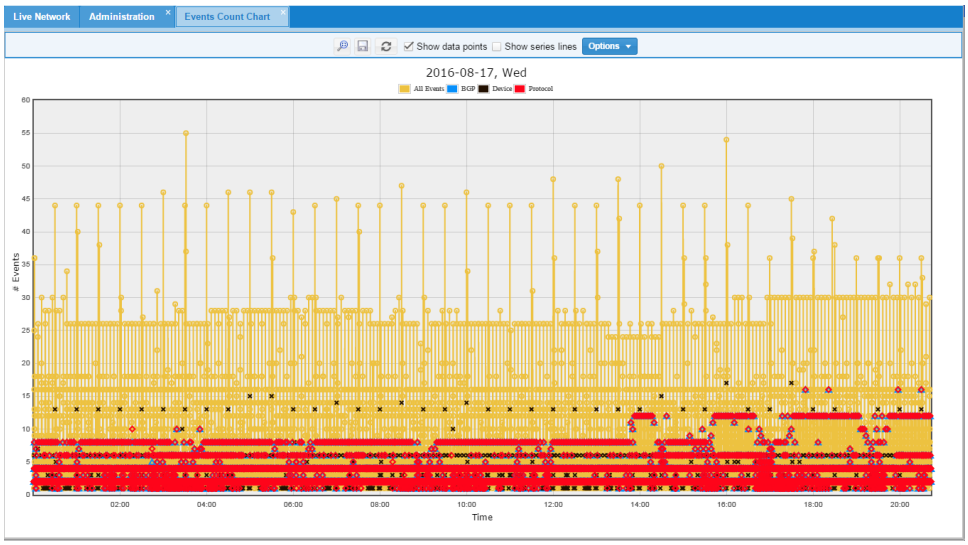
The Events Count Chart provides a graphical view for the number of events for the current day. By default, all events are displayed, but you can customize the chart view.

To display the Events Count Chart:

1. Select **Fault > Event Count Chart**.

   The Events Count Chart window is displayed. Figure 85 on page 111 shows the Event Count Chart window.

Figure 85: Event Count Chart Window



   In this example, the chart shows the event count for all events in gold, BGP events in blue, device events in black, and protocol events in red.

   In the chart window, you can use the controls at the top of the window to reset the zoom, save the chart as an image, and reload the chart. Hold your mouse pointer over a data point to display a pop-up pane that shows the event count. Drag your mouse over a section of the chart to zoom in.

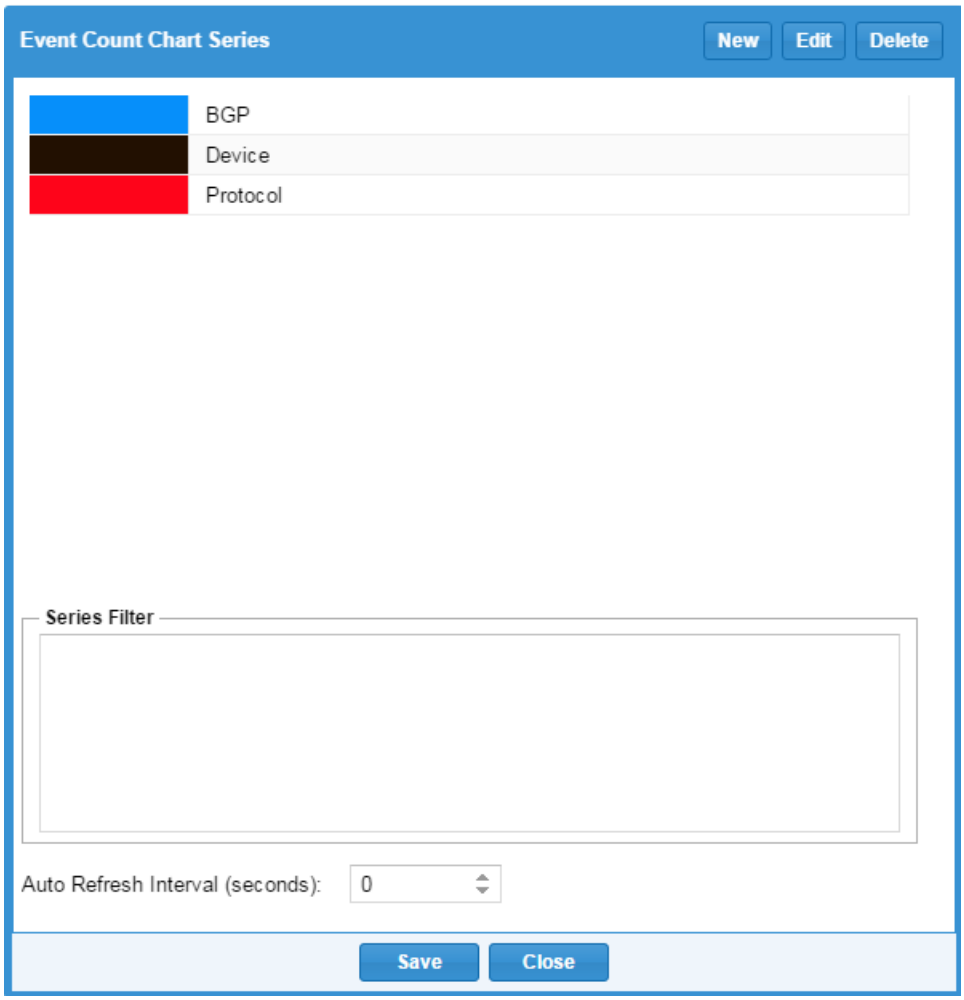
   You can also select to show or hide data points, and show or hide series lines.

   From the Options menu, you can show or hide protocol, device, and BGP events.

2. Select **Options > Manage Series**.

   The Event Count Chart Series window is displayed. Figure 86 on page 112 shows the Event Count Chart Series window.

Figure 86: Event Count Chart Series



3. Select the color and enter a different number to change the color displayed for each event series or select the color from the color selection window displayed.

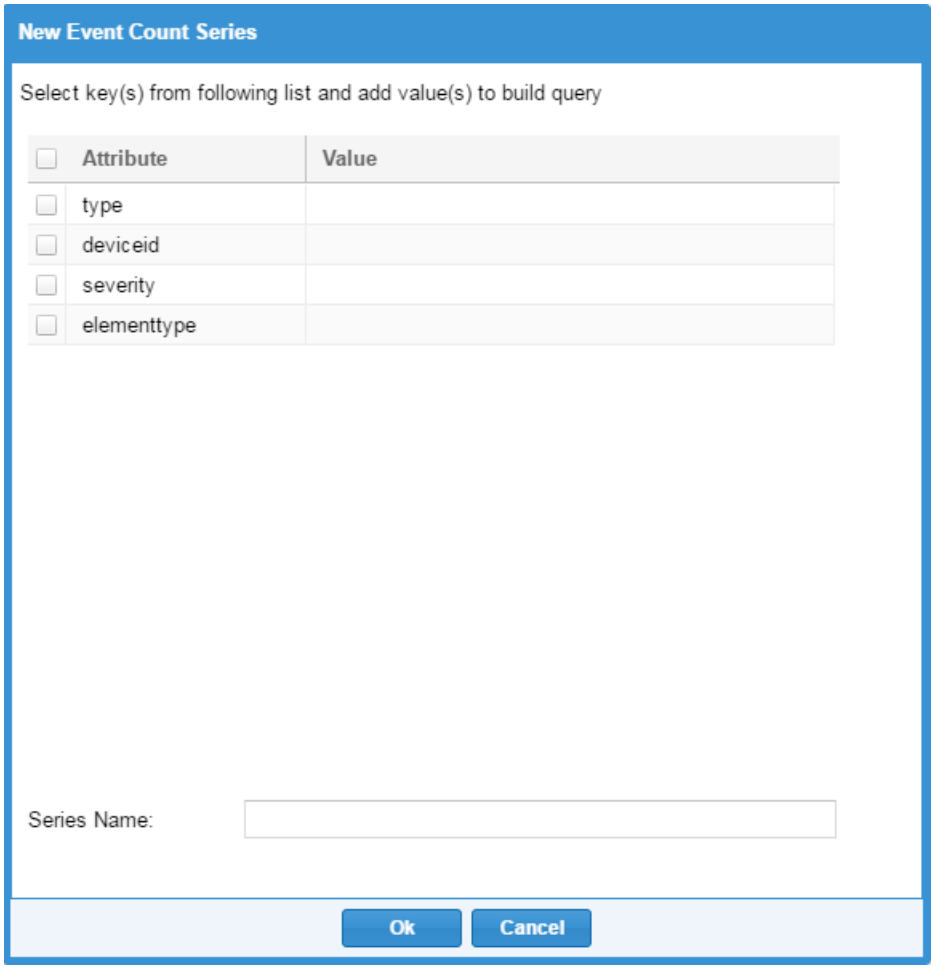
   When you select the series color, the series filter is displayed in the Series Filter pane. You can change the auto refresh rate from the Auto Refresh Interval menu. A value of 0 does not refresh.

4. To create a new series, select **New**.

   The New Event Count Series window is displayed. Figure 87 on page 113 shows the New Event Count Series window.

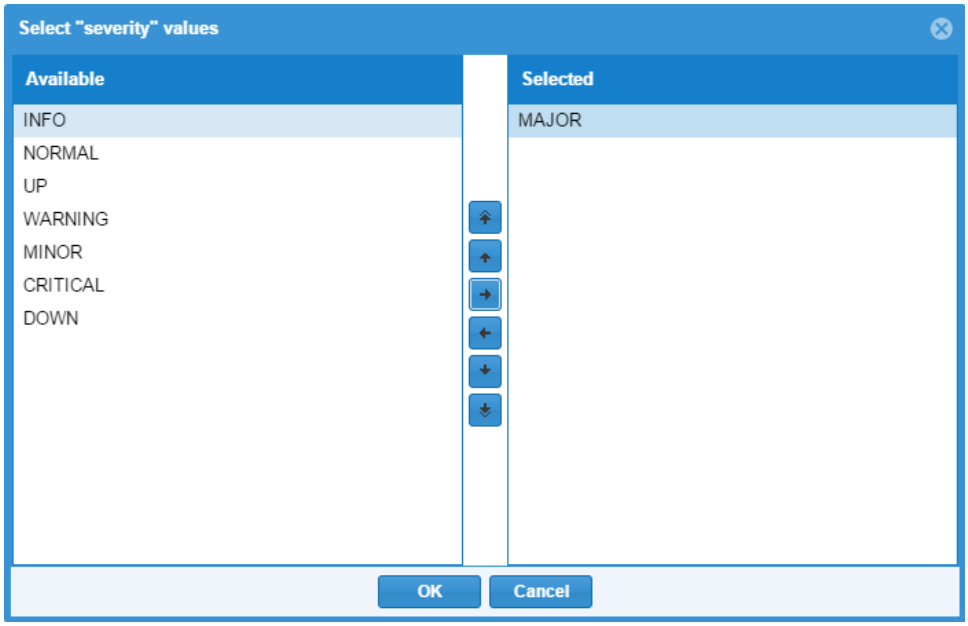
Copyright © 2018, Juniper Networks, Inc.

Figure 87: New Event Count Series Window



5. Type the name for the series in the Series Name field. Select a key in the attribute list and then click in the **Value** field. A select values window is displayed. The following figure shows the Select “severity” values window.

Figure 88: Select Severity Values Window



6. Select the value you want in the Available pane and select the right arrow to move it to the Selected pane. Select **OK**. The value is displayed in the New Event Count Series window. Continue to select the query values you want and then select **OK**. The new series is displayed in the New Event Count Series window.

   To edit a series, select **Edit**. To delete a series, select the series and select **Delete**.

Related Documentation

- Live Event Browser on page 93
- Historical Event Browser on page 107
- Event Summary Reports on page 114

Event Summary Reports

The event summary report feature displays a summary of events over a specified period of time. Daily, weekly, and last 30-day summary reports are available. Event summary reports by event type or node are also available.

To see the Event Summary Reports, make sure that the Event Server and SNMP trap server processes are running, by reading the **/u/wandl/bin/status_mplsview**. To receive trap events from network devices, the network devices should be configured to send SNMP traps with the IP/MPLSView application server as one of the target addresses.

The Event Dashboard displays the counts for various event categories. Each event category has its own window which can be edited or repositioned in your Web browser. Select **Select date range** to query a specific date, week, or the last 30 days. See Figure 89 on page 115.

Copyright © 2018, Juniper Networks, Inc.

Figure 89: Event Dashboard

Select date range

Node Type Counts

Type	Count
CollectionError	1863
authenticationFailure	213
DeviceReachable	18
UnreachableError	18
CollectionUpdate	10
jnxCmCfgChange	5

Interface Type Counts

Type	Count
ThresholdEvent	223
linkDown	10
linkUp	10

Tunnel Type Counts

Type	Count
mplsTunnelUp	780
mplsTunnelDown	750
mplsLspInfoDown	561
mplsLspInfoUp	561
mplsLspDown	554
mplsLspUp	552
ThresholdEvent	1

The event severity report displays the total number of events organized by event severity to device. Select **Select date range** to query a specific date, week, or the last 30 days. See Figure 90 on page 115.

Figure 90: Event Summary by Severity

Select date range

Device	Down	Critical	Major	Minor	Warning	Up	Normal	Info	Total
VMX10	0	0	208	2466	1275	208	2	0	4159
VMX20	0	0	294	2124	64	217	4	8	2711
VMX20(P22)	0	0	0	0	74	0	0	1	75

The event type report displays the total number of events organized by event type and severity (INFO, NORMAL, UP, WARNING, MINOR, MAJOR, CRITICAL, and DOWN). Select **Select date range** to query a specific date, week, or the last 30 days. See Figure 91 on page 115.

Figure 91: Event Summary by Event Type

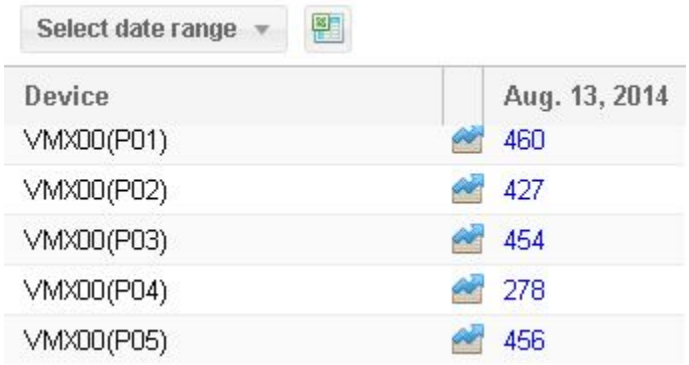
Select date range

Type	Severity	Aug. 13, 2014
CollectionError	WARNING	1902
CollectionUpdate	INFO	211
DeviceReachable	UP	18
ThresholdDurationEvent	INFO	14369

The “by node” report displays the total number of events organized by node. Select **Select date range** to query a specific date, week, or the last 30 days. See Figure 92 on page 116.

Copyright © 2018, Juniper Networks, Inc.

Figure 92: Event Summary by Node



Related Documentation

- Live Event Browser on page 93
- Events Count Chart on page 111

Event Options

Select **Fault > Event Options** to access the event settings. Use the following options to configure your event settings:

- Edit Threshold Alarms

  Threshold alarms (also known as threshold crossing alerts) help you monitor the network against any number of user defined service-level agreements (SLAs) or other production and performance requirements. When these SLAs or other requirements are breached, the event server notifies you by means of the Event Browser or by sending preconfigured notification e-mails. The Web-based Threshold Editor enables you to configure rules to trigger threshold events.

- Edit Event Subscriptions

  You can create and edit event subscriptions to notify you through e-mail or Short Message Service (SMS) text messages about network events of particular interest. To set up notifications to the events you want to monitor, you must create event subscriptions and event subscribers, and then associate event subscribers with particular subscriptions.

- Edit Event Severities

  You can change the default the severity level for an event. Possible severity levels include: INFO, NORMAL, UP, WARNING, MINOR, MAJOR, CRITICAL and DOWN.

- Enable or Disable Events

  You can enable or disable sending of SNMP traps for an event.

Copyright © 2018, Juniper Networks, Inc.

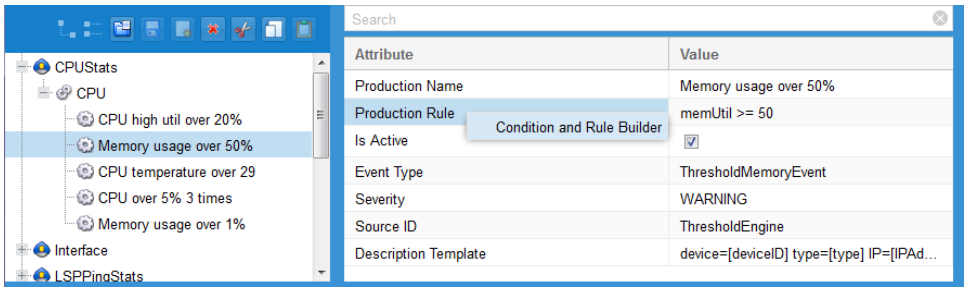
To edit a threshold alarm:

1. Select **Fault > Event Options > Edit Threshold Alarms**.

   The Threshold Editor is displayed.

2. In the left pane, navigate to and select the threshold alarm you want to edit.

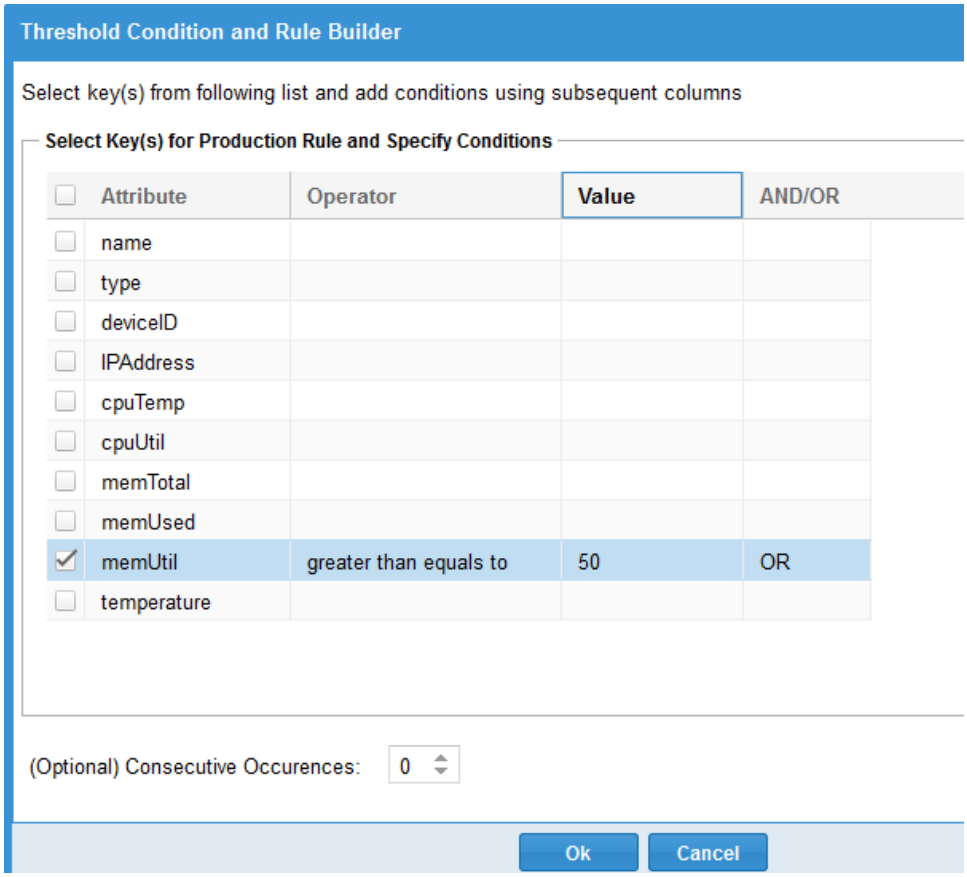
Figure 93: Edit Threshold Alarm for CPUStats



   The right pane displays the attributes configured for this threshold alarm. For example, the above figure shows the attributes for a threshold alarm that triggers an event when the CPU memory utilization is equal to or exceeds 50 percent.

3. Right-click the Production Rule to launch the Condition and Rule Builder.

Figure 94: Condition and Rule Builder for CPUStats



4. In the Threshold Condition and Rule Builder, add or modify the attributes for the threshold alarm.

   You can select one or more attributes, AND or OR from the AND/OR menu, and the operators for each value. Operators can include equals to, not equals to, matches, greater than, greater than equals to, less than, less than equals to, and between. To enter text such as the name, click in the Value field. The Add/Remove Text window is displayed. Enter the text to match and click **Add**, then click **Ok**. Click **Ok** in the Threshold Condition and Rule Builder. The new rule is displayed in the Threshold Editor window.

   To specify the number of consecutive occurrences before the alarm is triggered, you can select a value in the (Optional) Consecutive Occurences field.

To edit an event subscription:

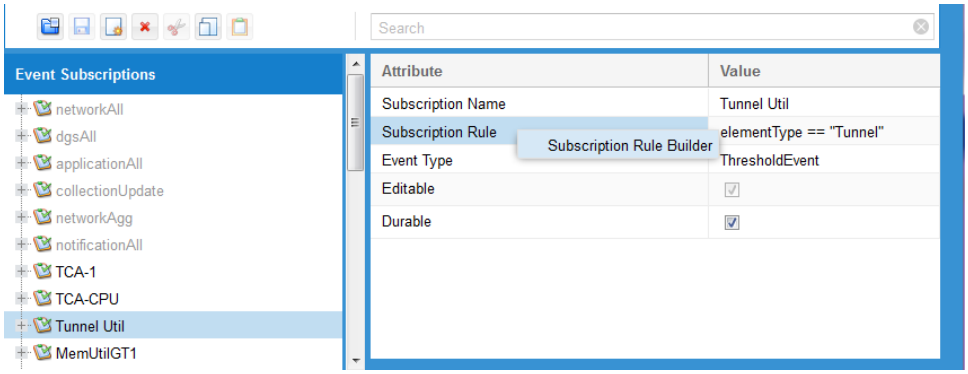
1. Select **Fault > Event Options > Edit Event Subscriptions**.

   The Subscription Editor appears.

2. In the left pane, navigate to and select the event subscription you want to edit.

Copyright © 2018, Juniper Networks, Inc.

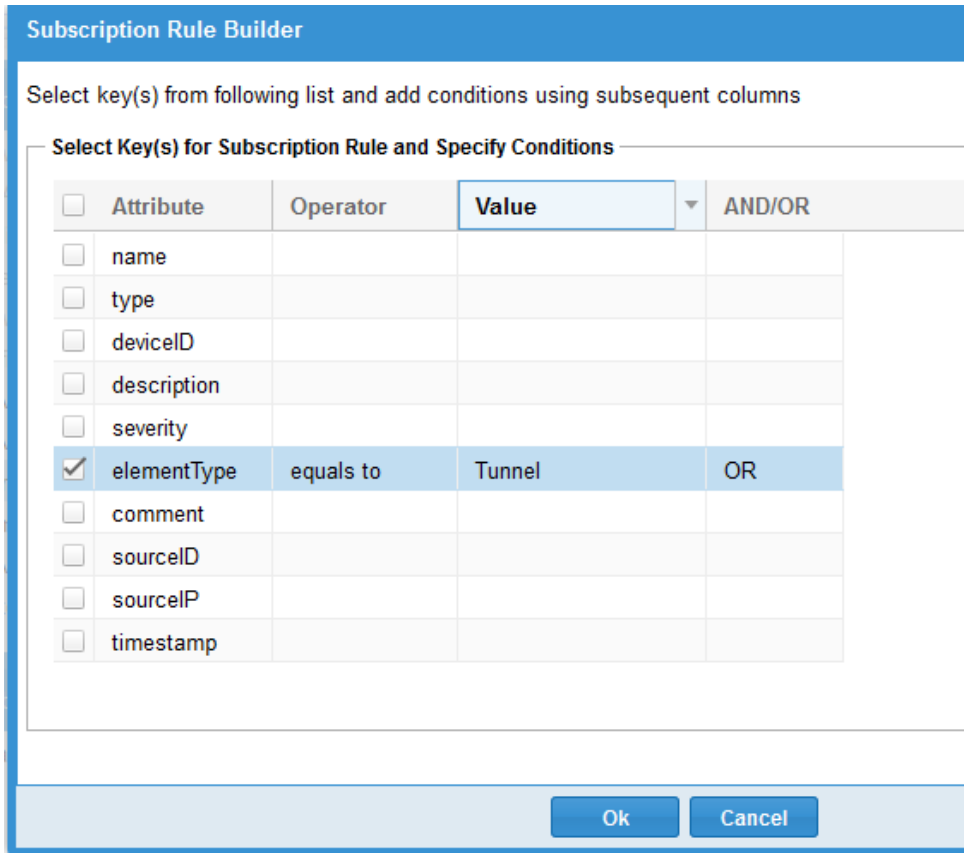
Figure 95: Edit Event Subscription for Tunnel Util



The right pane displays the attributes configured for this threshold alarm. For example, the above figure shows the attributes for an event subscription that sends notification when the element type is equal to “tunnel.”

3. Right-click the Subscription Rule to launch the Subscription Rule Builder.

Figure 96: Subscription Rule Builder for Tunnel Util



4. In the Subscription Rule Builder, add or modify the attributes for the threshold alarm.

You can select one or more attributes, AND or OR from the AND/OR menu, and the operators for each value. Operators can include equals to, not equals to, matches, greater than, greater than equals to, less than, less than equals to, and between. To enter text such as the name, click in the Value field. The Add/Remove Text window is displayed. Enter the text to match and click **Add**, then click **Ok**. Click **Ok** in the Subscription Rule Builder. The new rule is displayed in the Subscription Editor window.

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 6

Fault Management: Threshold Crossing Alerts

- Understanding Threshold Crossing Alerts on page 121
- Configuring Threshold Crossing Alerts on page 121
- Displaying Threshold Crossing Alerts on page 130
- Troubleshooting Threshold Crossing Alerts on page 135

Understanding Threshold Crossing Alerts

You can use the Threshold Editor to provide notifications when certain thresholds are exceeded. Through the threshold editor, you can configure rules, which if triggered, will create a threshold event. For example, a rule can be generated when a link exceeds a certain percentage utilization or when a node's CPU utilization exceeds a certain percentage. The threshold events will be displayed in the Event Browser and can also be subscribed to by e-mail or SMS using the Subscription Editor.

Related Documentation

- Configuring Threshold Crossing Alerts on page 121
- Displaying Threshold Crossing Alerts on page 130
- Troubleshooting Threshold Crossing Alerts on page 135

Configuring Threshold Crossing Alerts

- Threshold Editor Overview on page 121
- Interpreting the Threshold Editor on page 122
- Creating Threshold Crossing Alerts on page 124
- Triggering Threshold Alarms on page 126
- Defining Conditions and Rules on page 126

Threshold Editor Overview

Threshold alarms can be used to monitor the network against any number of user-defined SLAs or other production and performance requirements. When these SLAs or other

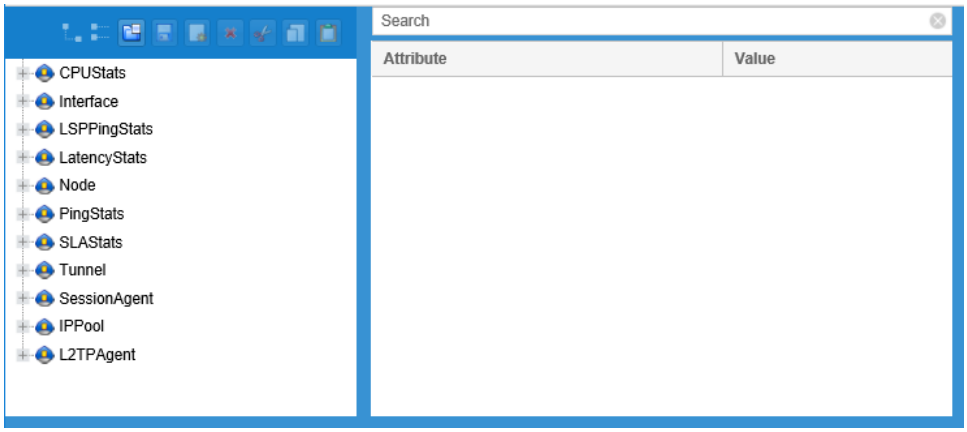
requirements are breached, you are automatically notified by the event server, either through viewing the Event Browser or by receiving preconfigured notification e-mails.

Threshold alarms can be triggered by periodic collections from the Traffic Collection Manager, or the Task Manager tasks Device SNMP Collection, Device Ping Collection, and Device SLA Collection. For each threshold alarm, the Data Gateway Server (DGS) will examine incoming data against all applicable threshold alarm rules. If any data matches a threshold alarm rule, the DGS server will post an event to the event server with the parameters specified in the threshold alarm. In the Threshold Editor, these rules are referred to as production rules. The DGS processes traffic data from the data collector. The DGS log contains detailed information about the data objects and messages from the data collector. The detail level of the log is controlled by the **dgs.log.properties** file in **/u/wandl/db/config**.

NOTE: In IP/MPLSView Release 6.3.0, Data Collector is renamed Traffic Data Collector.

To open the threshold editor, from the Live Network select **Fault > Event Options > Edit Threshold Alarms**. Figure 97 on page 122 shows the Threshold Editor window.

Figure 97: Threshold Editor



When the threshold editor is opened for the first time, the tree in the left pane is collapsed, hiding all production rules. Double-click an item or click the plus sign (+) to the left of the item to display the elements beneath it. This hierarchy is comprised of the element type, followed by group/scope, and the actual production rules.

See Also

- Displaying Threshold Crossing Alerts on page 130
- Troubleshooting Threshold Crossing Alerts on page 135

Interpreting the Threshold Editor

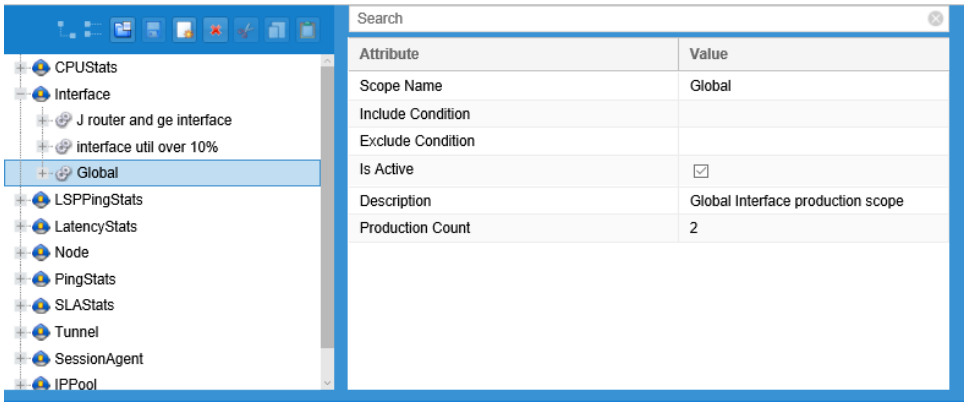
At the top level is the Element Type for which the rule will apply: Interface, Node, Tunnel, CPUStats, LSPPingStats, LatencyStats, PingStats, and SLAStats.

Copyright © 2018, Juniper Networks, Inc.

- **Interface:** Rules can be defined in this section for interface-related properties such as bandwidth and ingress and egress utilizations.
- **Node:** Rules can be defined in this section for node-related properties such as system up time, last up time, AAA, accounting, authentication, and sessions. These additional properties for AAA and sessions are related to wireless collection data and may or may not apply to all device types.
- **Tunnel:** Rules can be defined in this section for LSP tunnel-related properties such as the delta in the ingress bytes.
- **CPUStats:** Rules can be defined in this section for CPU and memory stats such as CPU temperature, CPU utilization, memory used, total memory, and memory utilization.
- **LSPPingStats:** Rules can be defined in this section for LSP ping stats on average, max, min, and standard deviation values.
- **LatencyStats:** Rules can be defined in this section for latency stats on average, max, min, and standard deviation values.
- **PingStats:** Rules can be defined in this section for ping stats on average, max, min, and loss percentage values.
- **SLAStats:** Rules can be defined in this section for SLA stats such as jitter, packet loss, packet timeout, and latency.

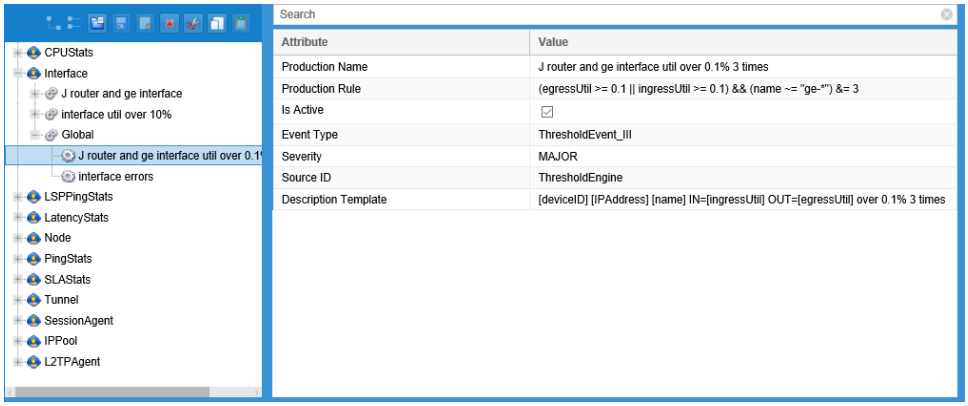
Following the element type, the next level is the scope, which defines the group of interfaces to which the threshold rule(s) will be applied. An include condition can be specified to filter for only interfaces matching some user-specified criteria. An exclude condition can additionally be specified to exclude interfaces with some user-specified criteria. If no fields are specified for the scope, the rules of this scope will be applied to all elements of the given type. For example, a scope can be created underneath the Interface element type that only considers Fast Ethernet interfaces. Figure 98 on page 123 shows the threshold editor scope window.

Figure 98: Threshold Editor Scope



Under the scope are the actual threshold rules themselves. Specify the production name, the actual rule, a severity level, and a description. For example, the rule can be created to generate a threshold event when the interface utilization exceeds a particular percentage. Figure 99 on page 124 shows an example threshold rule.

Figure 99: Example Threshold Rule



See Also

- Displaying Threshold Crossing Alerts on page 130
- Troubleshooting Threshold Crossing Alerts on page 135

Creating Threshold Crossing Alerts

To create a new threshold crossing alert:

1. For the desired element type, create a scope identifying a subgroup of elements in which to place the rule. The scope can be used, for example, to filter only Fast Ethernet interfaces, or events at a particular node. See “Creating a New Scope.”
2. Create the rule itself. See “Creating a New Rule.”

Creating a New Scope

To create a new scope, first select the upper-level tree item under which the group will be created. Then either click the **Create** button in the top toolbar, or right-click the selected item and select **Create**.

This will create a new group under that item. Select the new group and fill in the fields for the new group on the right pane. To enter text into a field, first double-click the field to enable editing of the field.

- **Scope Name** (Required)—Describes the scope of the rules contained within the group. Do not include any spaces in the name. Optionally, enter a description of the scope in the Description field.
- **Include and Exclude Conditions**—Preliminary filters for all rules within the group. Only data matching these conditions will be considered by the rules within the group. For example, you could set “name ~= fe” in the Include condition for an Interface scope to only consider Fast Ethernet interfaces. To edit these conditions, right-click at the beginning of the field to open the Condition and Rule Builder. For more information on how to define conditions, see “Defining Conditions and Rules.” If you do not require any filtering, leave these fields blank.

Copyright © 2018, Juniper Networks, Inc.

- **Is Active**—Activate or deactivate the scope and the production rules underneath it. Only if both the scope and production rule are activated will the threshold event be generated.
- **Production Count**—Number of rules within the group.

Creating a New Rule

To create a new rule underneath a scope, first select the scope under which the new rule will be created. Then either click the **Create New Production Rule** button in the top toolbar, or right-click the selected item and select **Create**. This will create a new rule under the selected group.

- **Production Name**—(Required) Describes the threshold rule. Do not include any spaces in the name.
- **Production Rule**—(Required) Defines the threshold crossing alert. If incoming data matches this rule, it will trigger the threshold event. Right-click at the beginning of the field to open the Condition and Rule Builder. An example rule for a production rule underneath the Interface scope is **ingressUtil > 75 || egressUtil > 75**. For more information about how to define conditions, see "Defining Conditions and Rules."
- **Is Active**—Activates or deactivates the production rule. Only if both the scope containing the production rule and the production rule are activated will the threshold event be generated.
- **Event Type**—Type of event triggered by this rule, which is displayed in the Event Browser when the threshold crossing alert is created. The default is **ThresholdEvent** and does not need to be changed. It is helpful to mark the events with more descriptive event types, such as **ThresholdUtilizationEvent** and **ThresholdMemoryEvent**.
- **Severity**—Configures the severity of the event. This severity can later be displayed in the Event Browser when the Threshold Event is triggered.

  The selection is used to
- **Source ID**—Displays as the source of the event triggered by this rule. This field corresponds to the Source ID field in the Event Browser.
- **Description Template**—Describes the event triggered by this threshold rule. This is the primary means of specifying threshold event details in the Event Browser. The template allows for specifying keys and dynamic values by enclosing them within square brackets []. For a list of available suggestions while typing in the Description template field, right-click in the beginning of the field. For example, for a rule that triggers an event when ingress utilization or egress utilization exceed 75 percent, the following template may be used:

  ```
  [deviceID]: [name]: ingress util [ingressUtil] or egress util [egressUtil]
  greater than 75%
  ```

See Also

- Displaying Threshold Crossing Alerts on page 130
- Troubleshooting Threshold Crossing Alerts on page 135

Triggering Threshold Alarms

Note that to trigger the threshold alarm, the corresponding collection (using the Task Manager or Traffic Collection Manager) should be scheduled on a recurring basis. For more information about scheduling the following tasks using Task Manager, see Task Manager.

- For CPUStats, see Device SNMP Collection.
- For LSPPingStats, see LSP Ping Collection.
- For LatencyStats, see Link Latency Collection.
- For PingStats, see Device Ping Collection.
- For SLAStats, see Device SLA Collection.

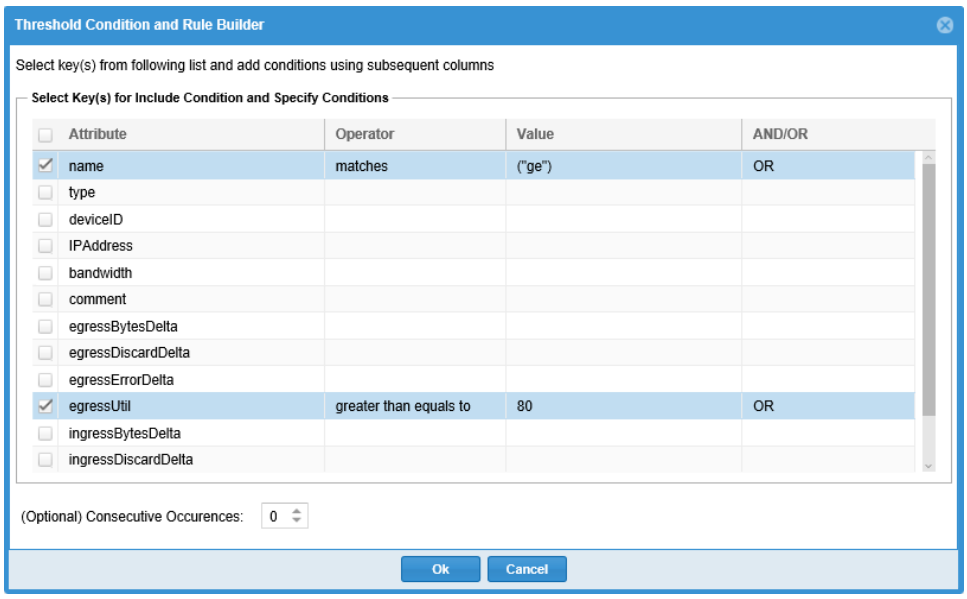
See Also

- Task Manager on page 199
- Displaying Threshold Crossing Alerts on page 130
- Troubleshooting Threshold Crossing Alerts on page 135

Defining Conditions and Rules

In the Condition and Rule Builder, select the desired key(s) in the Attribute column. Click the column header values to edit the logical operators and properties. An optional Consecutive Occurrences field allows you to specify the number of consecutive occurrences before the rule is triggered. Click **OK** to build the rule syntax. Figure 100 on page 126 shows an example for building threshold conditions and rules.

Figure 100: Threshold Conditions and Rules Builder



Copyright © 2018, Juniper Networks, Inc.

Alternatively, the Include and Exclude condition or Production rule syntax can be typed into the field instead of using the Condition and Rule Builder. Group conditions and production rules must be entered in the form of logical expressions with a predefined set of keys. For example, the following condition matches when either ingress utilization or egress utilization is greater than or equal to 75 percent: “ingressUtil >= 75 || egressUtil >= 75”.

- For a list of available keys while editing the condition or rule field, right-click for a list of suggestions, or review the Available Keys listed below. This list may be different for different types of elements. If unsure of where to start, right-click at the beginning of a field to see all possible keys. Remember that the field must first be activated for editing by double-clicking the field.
- The following are the supported logical operators for reference:== (equals), != (does not equal), ~= (equals using regular expression), && (and), || (or), < (less than), > (greater than), <= (less than or equal), and >= (greater than or equal).
- Note that all conditions and rules are case sensitive, and spaces should be used as delimiters between keywords, values, and logical operators. Additionally, quotes (“”) should be placed around string values, for example, IPAddress == “1.2.3.4.”.
- If an integer value is specified for the utilization, the traffic utilization will be compared as integers. To compare using floating numbers, specify the number as a floating number. For example, “ingressUtil > 75.0” instead of “ingressUtil > 75”.

Consecutive Occurrences

The special operator “&=” is used to test for consecutive occurrences of a condition. For example, to test that the ingress or egress utilization has been greater than 75 percent for 3 times in a row, you could use the following expression: (ingressUtil >= 75 || egressUtil >= 75) &= 3

Available Keys

Below are a list of the attributes for Interface, Node, and Tunnel elements.

Note that utilization values are specified in percentages (for example, specify 30 for 30 percent).

See “Defining Conditions and Rules” for the syntax involving brackets and units.

Common Attributes

- **deviceID:** The hostname of the device associated with the element. For the Node element type, this is the same as the name. For the Interface element type, this is the node that contains the interface. For the Tunnel element type, this is the head-end of the tunnel.
- **name:** The element’s name. For the Node element type, this is the hostname. For the Interface element type, this is the interface name. For the Tunnel element type, this is the tunnel’s name.

- **type:** The element type (Node, Interface, Tunnel).
- **IPAddress:** The IP address for the element.

Interface Attributes:

- **bandwidth:** The interface bandwidth. Here, g, m, k, are permitted to indicate the units, for example, 100m for 100 Mbps.
- **ingressBytesDelta, egressBytesDelta:** The interface ingress/egress traffic in bytes per second.
- **ingressUtil, egressUtil:** Specify an integer value for percentage, for example, 30 for 30 percent.
- **ingressErrorDelta, egressErrorDelta:** The number of inbound/outbound packets that contained errors per second.
- **ingressDiscardDelta, egressDiscardDelta:** The number of inbound/outbound packets that are discarded per second.

Node Attributes

- **nodeType:** Hardware type (for example, M5 for Juniper M5, CISCO) used for SLA status data.
- **sysUptime, lastUptime:** Unit is in hundredths of a second.

Tunnel Attributes

- **ingressBytesDelta:** The tunnel traffic in bytes per second.

CPU Stats Attributes

- **cpuTemp:** CPU temperature.
- **cpuUtil:** CPU utilization.
- **memTotal:** Total memory.
- **memUsed:** Used memory.
- **memUtil:** Memory utilization.

LSP Ping Stats Attributes

- **lsppingAvg:** Average LSP ping value.
- **lsppingMax:** Maximum LSP ping value.
- **lsppingMin:** Minimum LSP ping value.
- **lsppingSD:** Standard deviation LSP ping value.

Latency Stats Attributes

- **latencyAvg:** Average latency value.
- **latencyMax:** Maximum latency value.

Copyright © 2018, Juniper Networks, Inc.

- **latencyMin:** Minimum latency value.
- **latencySD:** Standard deviation latency value.

Ping Stats Attributes

- **pingAvg:** Average ping value.
- **pingMax:** Maximum ping value.
- **pingMin:** Minimum ping value.
- **pingLossPercent:** Ping loss percentage.

SLA Stats Attributes

- slaDNSError, slaDNSRoundTrip, slaTimeOut
- slaEgressLatencyAvg, slaEgressLatencyMax, slaEgressLatencyMin
- slaEgressNegJitterAvg, slaEgressNegJitterMax, slaEgressNegJitterMin
- slaEgressPacketLoss
- slaEgressPosJitterAvg, slaEgressPosJitterMax, slaEgressPosJitterMin
- slaEgressRoundTripAvg, slaEgressRoundTripMax, slaEgressRoundTripMin
- slaHTTPTransactionError, slaHTTPTransactionRoundTrip, slaHTTPTransactionTimeOut, slaHTTPTransactionTimeToFirstByte
- slaIngressLatencyAvg, slaIngressLatencyMax, slaIngressLatencyMin
- slaIngressNegJitterAvg, slaIngressNegJitterMax, slaIngressNegJitterMin
- slaIngressPacketLoss
- slaIngressPosJitterAvg, slaIngressPosJitterMax, slaIngressPosJitterMin
- slaIngressRoundTripAvg, slaIngressRoundTripMax, slaIngressRoundTripMin
- slaPacketOutofSequence, slaPacketTimeout
- slaRoundTripAvg, slaRoundTripMax, slaRoundTripMin
- slaTCPConnectionError, slaTCPConnectionRoundTrip, slaTCPConnectionTimeOut
- slaUnknownPacketLoss

Table 25: Additional Examples

Element Type	Scope	Production Rule	Explanation
Interface	Exclude condition: name ~= fe || name ~= ge || name ~= Ethernet	ingressUtil > 50.0 || egressUtil > 50.0	Generates alarm if non-Ethernet links have utilization over 50 percent.
CPUStats	Include condition: deviceID== “NWK”	cpuUtil > 90	Generates alarm if CPU utilization on router NWK exceeds 90 percent.

Table 25: Additional Examples (continued)

Element Type	Scope	Production Rule	Explanation
Tunnel		ingressBytesDelta > 8000	Generates alarm if traffic is over 8 KBps = 64 Kbps.

Related Documentation

- Displaying Threshold Crossing Alerts on page 130
- Troubleshooting Threshold Crossing Alerts on page 135

Displaying Threshold Crossing Alerts

- Displaying Data Triggered Threshold Crossing Alerts on page 130
- Displaying Interface Traffic Threshold Crossing Alerts on page 131
- Displaying LSP Tunnel Traffic Threshold Crossing Alerts on page 132
- Displaying Tunnel Events on page 134

Displaying Data Triggered Threshold Crossing Alerts

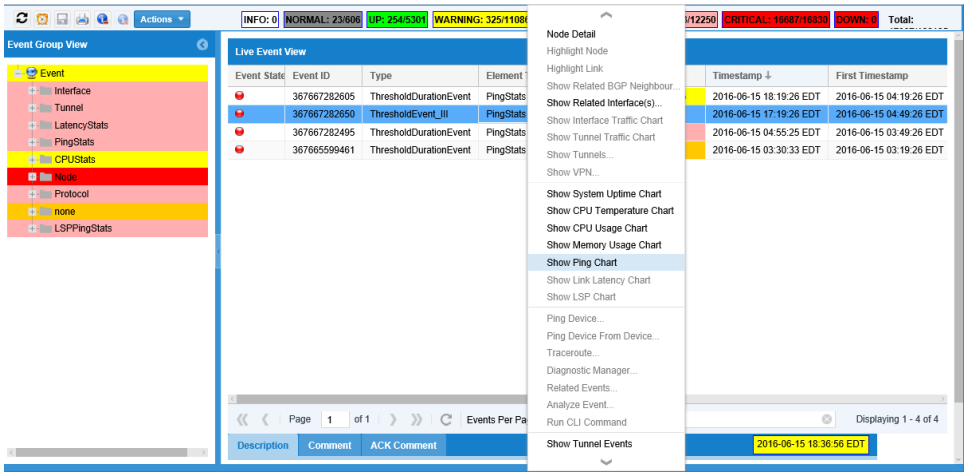
To display data-triggered threshold crossing alerts:

1. Select **Fault > Live Event Browser**.

   The Live Event View window is displayed.

2. From the Live Event View pane, select an event with a **PingStats** Element Type and right-click to display a list of applicable actions. Figure 101 on page 130 shows the actions menu.

Figure 101: Live Event View



3. Select **Show Ping Chart**.

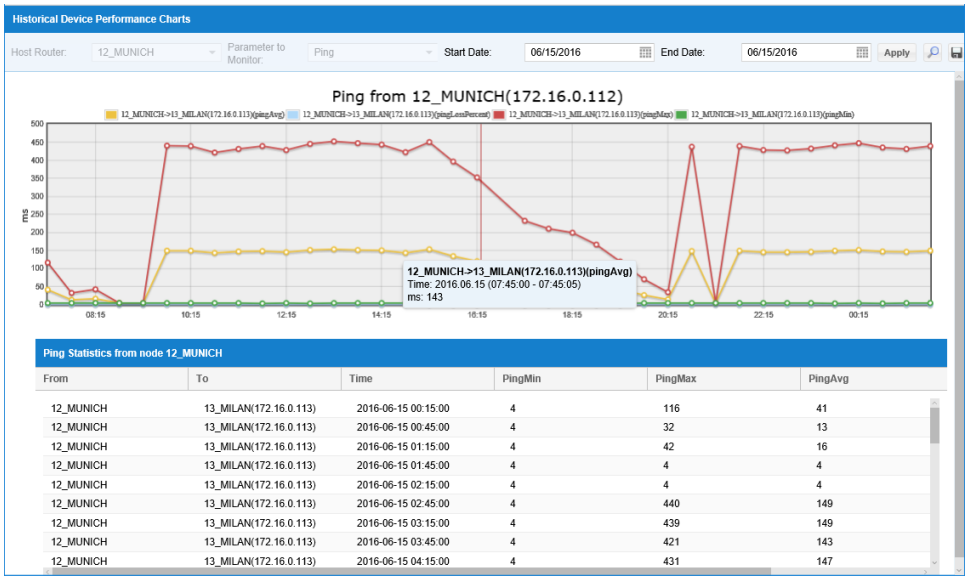
Copyright © 2018, Juniper Networks, Inc.

The Historical Device Performance Chart is displayed, showing the ping values from the source device. In the chart, the linear colors represent the following, in milliseconds, for each data point time:

- Yellow—PingAvg. Average ping time.
- Blue—PingLossPercent. Percentage of lost pings.
- Red—PingMax. Maximum ping time.
- Green—PingMin. Minimum ping time.

4. Mouse over a data point in the chart to display a pop-up pane that shows the time and traffic value. Figure 102 on page 131 shows an example ping chart. The bottom pane lists the ping values for each data point time.

Figure 102: Historical Device Performance Charts



From	To	Time	PingMin	PingMax	PingAvg
12_MUNICH	13_MILAN(172.16.0.113)	2016-06-15 00:15:00	4	116	41
12_MUNICH	13_MILAN(172.16.0.113)	2016-06-15 00:45:00	4	32	13
12_MUNICH	13_MILAN(172.16.0.113)	2016-06-15 01:15:00	4	42	16
12_MUNICH	13_MILAN(172.16.0.113)	2016-06-15 01:45:00	4	4	4
12_MUNICH	13_MILAN(172.16.0.113)	2016-06-15 02:15:00	4	4	4
12_MUNICH	13_MILAN(172.16.0.113)	2016-06-15 02:45:00	4	440	149
12_MUNICH	13_MILAN(172.16.0.113)	2016-06-15 03:15:00	4	439	149
12_MUNICH	13_MILAN(172.16.0.113)	2016-06-15 03:45:00	4	421	143
12_MUNICH	13_MILAN(172.16.0.113)	2016-06-15 04:15:00	4	431	147

See Also

- Configuring Threshold Crossing Alerts on page 121
- Troubleshooting Threshold Crossing Alerts on page 135

Displaying Interface Traffic Threshold Crossing Alerts

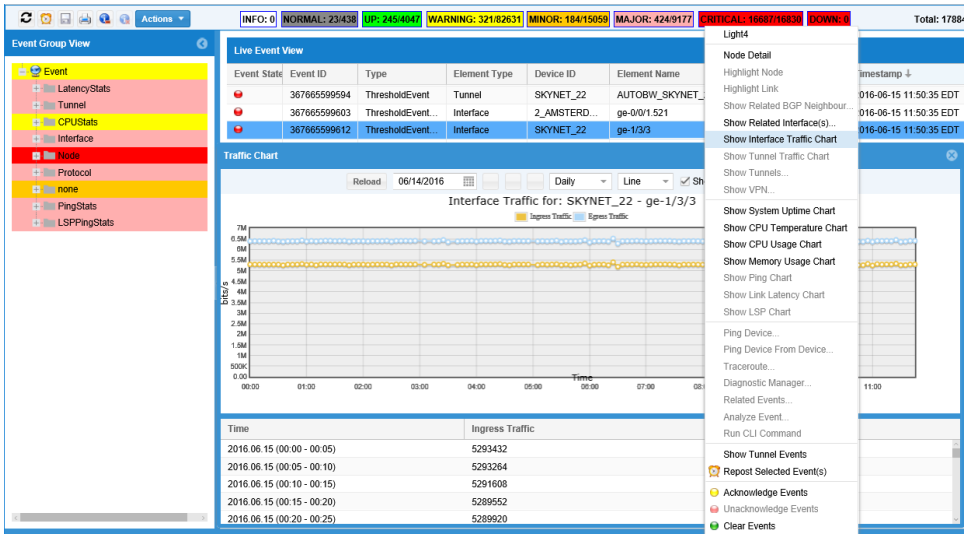
To display interface traffic threshold crossing alerts:

1. Select **Fault > Live Event Browser**.

   The Live Event View window is displayed.

2. From the Live Event View window, select an event with an **Interface** Element Type and right-click to display a list of applicable actions. Figure 39 on page 62 shows the actions menu.

Figure 103: Interface Traffic Chart



3. Select **Show Interface Traffic Chart**.

   The Traffic Chart is displayed, showing the traffic values from the source device. Figure 39 on page 62 shows the traffic chart. In the upper pane, the linear colors in the chart represent the following in bits per second, measured in units of millions (M) or thousands (K) for each data point time:

   - Ingress Traffic—Traffic originating from outside of the network and directed to a destination inside of the host network.
   - Egress Traffic—Traffic directed to an external network that originated from inside the host network.

4. Mouse over a data point in the chart to display a pop-up pane that shows the time and traffic value. The bottom pane lists the traffic values for each data point time.

See Also

- Configuring Threshold Crossing Alerts on page 121
- Troubleshooting Threshold Crossing Alerts on page 135

Displaying LSP Tunnel Traffic Threshold Crossing Alerts

To display tunnel traffic threshold crossing alerts:

1. Select **Fault > Live Event Browser**.

   The Live Event View window is displayed.

2. From the Live Event View window, select an event with a **Tunnel** Element Type and right-click to display a list of applicable actions. Figure 104 on page 133 shows the actions menu.

Copyright © 2018, Juniper Networks, Inc.

Figure 104: Tunnel Traffic Chart

3. Select **Show Tunnel Traffic Chart**.

   The Traffic Chart is displayed, showing the traffic values from the source device. Figure 104 on page 133 shows the traffic chart. In the upper pane, the linear colors in the chart represent the following in bits per second, measured in units of millions (M) or thousands (K) for each data point time:

   - Ingress Traffic—Traffic originating from outside of the network and directed to a destination inside of the host network.
   - Egress Traffic—Traffic directed to an external network that originated from inside the host network.

4. Mouse over a data point in the chart to display a pop-up pane that shows the time and traffic value. The bottom pane lists the traffic values for each data point time.

See Also

- Configuring Threshold Crossing Alerts on page 121
- Troubleshooting Threshold Crossing Alerts on page 135

Displaying Tunnel Events

To display tunnel events:

1. Select **Fault > Live Event Browser**.

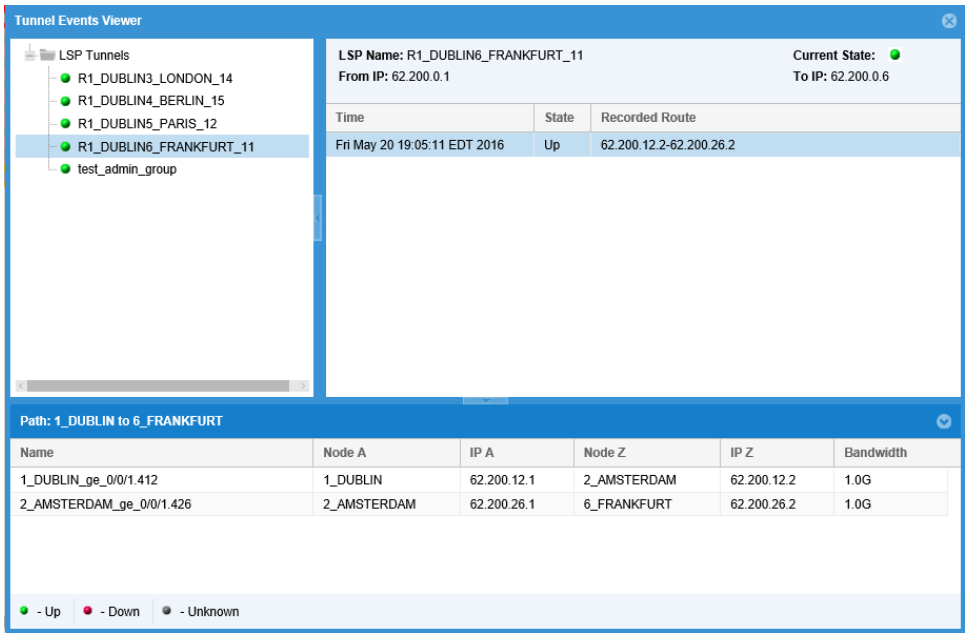
   The Live Event View window is displayed.

2. From the Live Event View window, select an event with a **Tunnel** Element Type and right-click to display a list of applicable actions.

3. Select **Show Tunnel Events**.

   The Tunnel Event Viewer is displayed, showing the LSP tunnels in the left pane and tunnel status (up, down, or unknown). Figure 105 on page 134 shows the Tunnel Events Viewer window.

Figure 105: Tunnel Events Viewer



4. Select a path from the LSP Tunnels list. The recorded route is displayed in the right pane.

5. Select an item from the right pane. The bottom pane lists the tunnel values for the selected path.

See Also

- Configuring Threshold Crossing Alerts on page 121
- Troubleshooting Threshold Crossing Alerts on page 135

Copyright © 2018, Juniper Networks, Inc.

Troubleshooting Threshold Crossing Alerts

The following items address troubleshooting threshold crossing alert behavior:

Event Severity Level—If the threshold crossing alert does not display, check that the event type is not INFO. Events of severity INFO will only be displayed when the Event Browser is opened and will not be stored.

Units—Check that you are interpreting the attribute with the correct units. For example, the utilization should be represented as a percentage (75, for 75%) rather than a fraction (0.75), and the ingressBytesDelta represents Bytes per second rather than bits per second. See Available Keys in the *IP/MPLSView Java-Based Management and Monitoring Guide* for more information about expected units. You can print the value in the description for confirmation. For example, use [ingressUtil] and [egressUtil] for interface ingress and egress utilization.

Rule ordering—If there are multiple rules within a scope, the last rule is evaluated first. In that case, rules must go from general to specific. It might be safer to add in both > and < checks for safety. For example, suppose we have the following settings. Then a memUtil of 75 will use rule c, not rule a or b. This is the expected rule behavior.

- **Rule a:** memUtil > 50, MINOR
- **Rule b:** memUtil > 60, MAJOR
- **Rule c:** memUtil > 70, CRITICAL

- If a rule d is added, which is more general than the preceding rules, then rules a, b, and c will never get used.
- **Rule d:** memUtil > 5, Severity WARNING
- To get around this, you can qualify rules with both < and > checks.
- **Rule d:** memUtil > 5 && memUtil < 50

Whole Numbers—Be careful with whole numbers, as the fraction may get ignored. For example, better to use 1.0 instead of 1. If the rule > 60 should include 60.3, then it should be changed either to > 60.0 or >= 60. This should be changed in the memUtil rules. Otherwise, 60.3 will fail the > 60 rule but succeed the >50 rule. This is because if you specify an integer, our software will evaluate in terms of integers, and truncates any floating point to integer before doing the evaluation. Thus, 60.3 is truncated to 60, and then fails rule > 60.

Timestamps—Note that the time stamp of a threshold event can differ by up to two collection cycles, depending upon when the event is processed by IP/MPLSView.

- If no threshold crossing alerts are displayed as expected, rerun the Scheduling Live Network Collection task. It is possible that some information regarding interface bandwidth needs to be updated.

Copyright © 2018, Juniper Networks, Inc.

- Read the **/u/wandl/log/threshold.log.0** file and verify that there are no diagnostic error messages.

Related Documentation

- Configuring Threshold Crossing Alerts on page 121
- Displaying Threshold Crossing Alerts on page 130

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 7

Performance Management

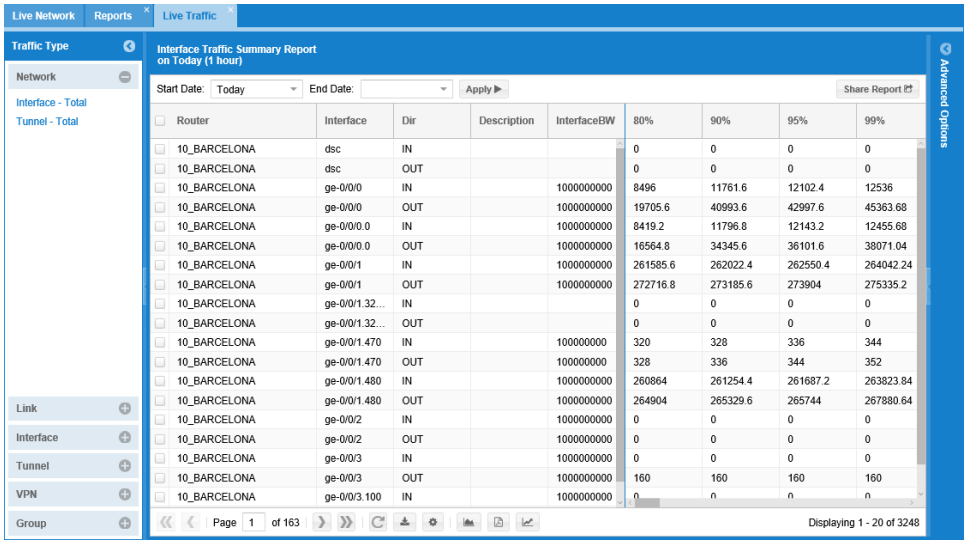
- Understanding Live Traffic on page 137
- Live Traffic on page 140
- Aggregated Traffic Reports on page 147
- Live VPN Traffic on page 148
- Monitoring the Status of Your Network on page 149
- Monitoring Real-Time Traffic and Device Performance on page 152
- Monitoring Any OID in Real Time on page 155
- Diagnostics on page 157
- Running the CLI on page 162
- Diagnostic Manager on page 166
- Traffic Collection Manager on page 178
- Viewing Device Performance on page 181
- Viewing Network Performance on page 185
- Viewing Miscellaneous Reports and Charts on page 187
- Network Performance Data Chart Report on page 188
- Archived Reports on page 189

Understanding Live Traffic

The IP/MPLSView main window has a Performance menu used to display live traffic, aggregated traffic, real-time status and usage, device and network performance, diagnostics, and manage the Traffic Collector.

Figure 106 on page 138 shows the Live Traffic window.

Figure 106: Live Traffic Window



Router	Interface	Dir	Description	InterfaceBW	80%	90%	95%	99%
10_BARCELONA	dsc	IN			0	0	0	0
10_BARCELONA	dsc	OUT			0	0	0	0
10_BARCELONA	ge-0/0/0	IN		1000000000	8496	11761.6	12102.4	12536
10_BARCELONA	ge-0/0/0	OUT		1000000000	19705.6	40993.6	42997.6	45363.68
10_BARCELONA	ge-0/0/0.0	IN		1000000000	8419.2	11796.8	12143.2	12455.68
10_BARCELONA	ge-0/0/0.0	OUT		1000000000	16564.8	34345.6	36101.6	38071.04
10_BARCELONA	ge-0/0/1	IN		1000000000	261585.6	262022.4	262550.4	264042.24
10_BARCELONA	ge-0/0/1	OUT		1000000000	272716.8	273185.6	273904	275335.2
10_BARCELONA	ge-0/0/1.32...	IN			0	0	0	0
10_BARCELONA	ge-0/0/1.32...	OUT			0	0	0	0
10_BARCELONA	ge-0/0/1.470	IN		100000000	320	328	336	344
10_BARCELONA	ge-0/0/1.470	OUT		100000000	328	336	344	352
10_BARCELONA	ge-0/0/1.480	IN		1000000000	260864	261254.4	261687.2	263823.84
10_BARCELONA	ge-0/0/1.480	OUT		1000000000	264904	265329.6	265744	267880.64
10_BARCELONA	ge-0/0/2	IN		1000000000	0	0	0	0
10_BARCELONA	ge-0/0/2	OUT		1000000000	0	0	0	0
10_BARCELONA	ge-0/0/3	IN		1000000000	0	0	0	0
10_BARCELONA	ge-0/0/3	OUT		1000000000	160	160	160	160
10_BARCELONA	ge-0/0/3.100	IN		1000000000	0	0	0	0

Live traffic reports are organized by traffic type.

Network

Interface Total—Displays the total interface ingress and egress traffic collected for the entire day.

Tunnel Total—Displays the total tunnel traffic collected for the entire day.

Link

Link Summary—Displays link traffic between two routers.

Interface

Interface Router—Displays total interface ingress and egress traffic on a router at the last collection time interval. Clicking a specific router will display all interfaces on that router. Clicking a specific interface will display historical traffic for that interface.

Interface Individual—Displays single interface ingress and egress traffic on a router.

Interface Summary—Displays interface ingress and egress traffic on a router.

Interface Total Ingress—Displays aggregated interface ingress traffic. Requires running the Traffic Summary Report task in Task Manager.

Interface Total Egress—Displays aggregated interface egress traffic. Requires running the Traffic Summary Report task in Task Manager.

Tunnel

Tunnel Network Level—Displays tunnel traffic by tunnel name at the last collection time interval. Clicking a specific tunnel will display historical status states and traffic for that tunnel.

Copyright © 2018, Juniper Networks, Inc.

Tunnel Router—Displays tunnel ingress and egress traffic on a router at the last collection time interval. Clicking a specific router will display all tunnels on that router. Clicking a specific tunnel will display historical status states and traffic for that tunnel.

Tunnel Individual—Displays single tunnel traffic on a router.

Tunnel Summary—Displays tunnel traffic on a router.

Tunnel Total Ingress—Displays aggregated tunnel traffic. Requires running the Traffic Summary Report task in Task Manager.

Tunnel Traffic Matrix—Displays the total tunnel traffic originating and terminating at each router.

VPN

VPN Summary—Displays VPN ingress and egress traffic on a router.

VPN Total Ingress—Displays aggregated VPN ingress traffic. Requires running the Traffic Summary Report task in Task Manager.

VPN Total Egress—Displays aggregated VPN egress traffic. Requires running the Traffic Summary Report task in Task Manager.

Customer Service—Displays total traffic per Customer Service VPN.

Group

Live Chart—Displays interface traffic charts by report groups. The report group must defined in Admin > Report Groups.

Live Report—Displays interface traffic reports by report groups. The report group must defined in Admin > Report Groups.

Single Day—Displays total tunnel traffic between groups for a single day. The group is defined in the client.

Multiple Days—Displays total tunnel traffic between groups for multiple days. The group is defined in the client.

Tunnel Traffic Matrix—Displays the total tunnel traffic originating and terminating between groups. The group is defined in the client.

Status—Displays the traffic data collector's status, assigned traffic collection groups, and routers. Click on the Group ID to display details of the routers and collected tables. The traffic collection group is defined in the client Traffic Collection Manager.

Related Documentation

- Live Traffic on page 140

Live Traffic

- Displaying a Live Traffic Network Tunnel Chart on page 140
- Displaying a Link Traffic Summary Report on page 141
- Saving and Sharing a Live Traffic Report on page 142
- Displaying a Router Ingress Interface Traffic Summary Report on page 143
- Displaying a Router Ingress Tunnel Traffic Summary Report on page 144
- Displaying LSP Bandwidth on page 145
- Displaying a VPN Egress Traffic Summary Report on page 146

Displaying a Live Traffic Network Tunnel Chart

To display a live traffic network tunnel chart:

1. Select **Performance > Live Traffic**.

   The Live Traffic window is displayed.

2. In the Traffic Type pane, select **Network > Tunnel - Total**.

   The default display is for the current date, as shown in Figure 107 on page 140.

Figure 107: Total Network Tunnel Traffic Chart

   The upper pane shows the tunnel traffic chart. The bottom pane lists the traffic values for each data point time.

3. (Optional) In the Network Tunnel Traffic Chart window, you can use the controls at the top of the window to reload the chart, select the day, week, month, or year, reset the zoom, save the chart as an image, export to Excel, select the time period, select the chart style, show or hide the data points, and enable auto refresh. Hold your mouse

Copyright © 2018, Juniper Networks, Inc.

pointer over a data point to display a pop-up pane that shows the time and traffic value.

See Also

- Understanding Live Traffic on page 137
- Aggregated Traffic Reports on page 147
- Monitoring the Status of Your Network on page 149
- Monitoring Real-Time Traffic and Device Performance on page 152

Displaying a Link Traffic Summary Report

To display a link traffic summary report:

1. Select **Performance > Live Traffic**.

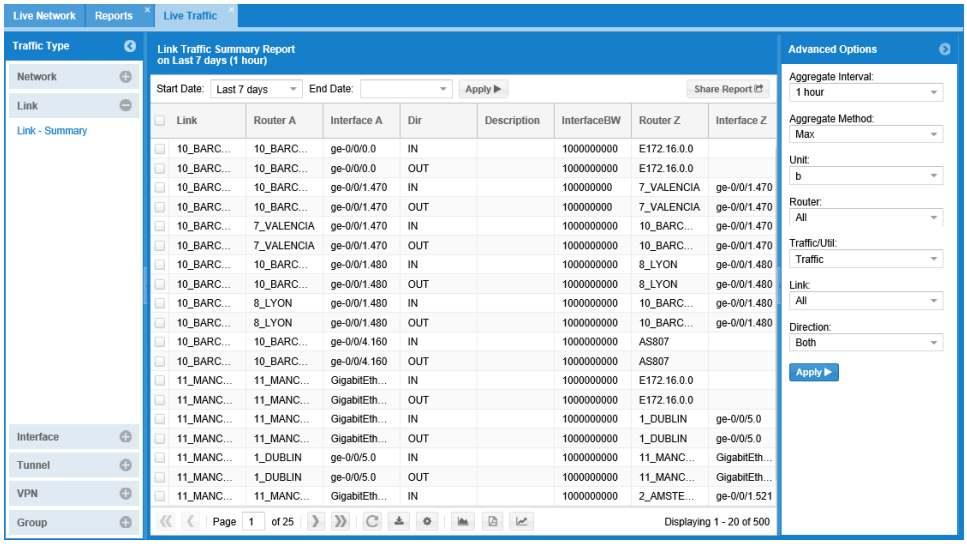
   The Live Traffic window is displayed.

2. In the Traffic Type pane, select **Link > Link - Summary**.

3. From the drop-down lists, select the Start Date and End Date, then click **Apply**.

   The Link Traffic Summary Report is displayed. See Figure 108 on page 141.

Figure 108: Link Traffic Summary Report



4. (Optional) Expand the Advanced Options pane and select from the drop-down lists to change the following:

   - **Aggregate Interval**—Select the interval in increments of minutes or hours.
   - **Aggregate Method**—Select maximum, average, or percentage.
   - **Unit**—Select b (bytes), kb (kilobytes), Mb (megabytes), or Gb (gigabytes).

- **Router**—Select all or filter by specific router.
- **Traffic\Util**—Select to filter by all, traffic only, or utility only.
- **Link**—Select all or filter by specific link.
- **Direction**—Select traffic in both directions, traffic coming in, or traffic going out.

See Also
- Monitoring Real-Time Traffic and Device Performance on page 152

Saving and Sharing a Live Traffic Report

To share a live traffic report:

1. Select **Performance > Live Traffic**.

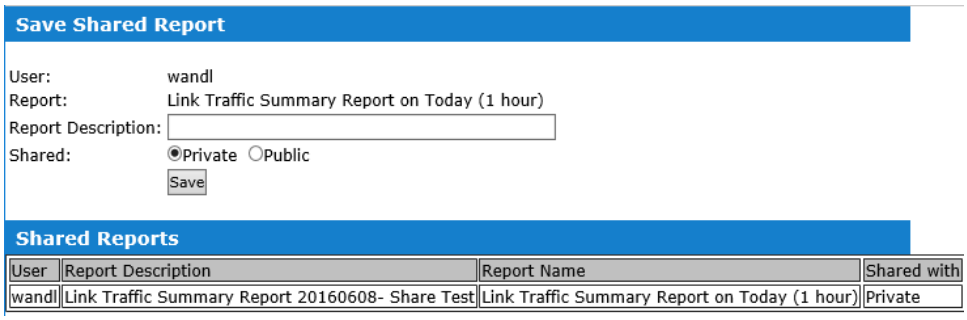
   The Live Traffic window is displayed.

2. After running a Live Traffic report, click **Share Report** in the upper-right corner of the report window.

   This option applies to the link, interface, tunnel, VPN, and group reports.

3. In Report Description, type a description and click **Save**. Figure 109 on page 142 shows an example of a saved shared report that is displayed in the Shared Reports table.

Figure 109: Save Shared Report



4. To view the Shared Report, from the Live Network window, select **Reports > Shared Reports**.

5. Click the report link to view the full report.

See Also
- Monitoring Real-Time Traffic and Device Performance on page 152

Copyright © 2018, Juniper Networks, Inc.

Displaying a Router Ingress Interface Traffic Summary Report

To display a router ingress interface traffic summary report:

1. Select **Performance > Live Traffic**.

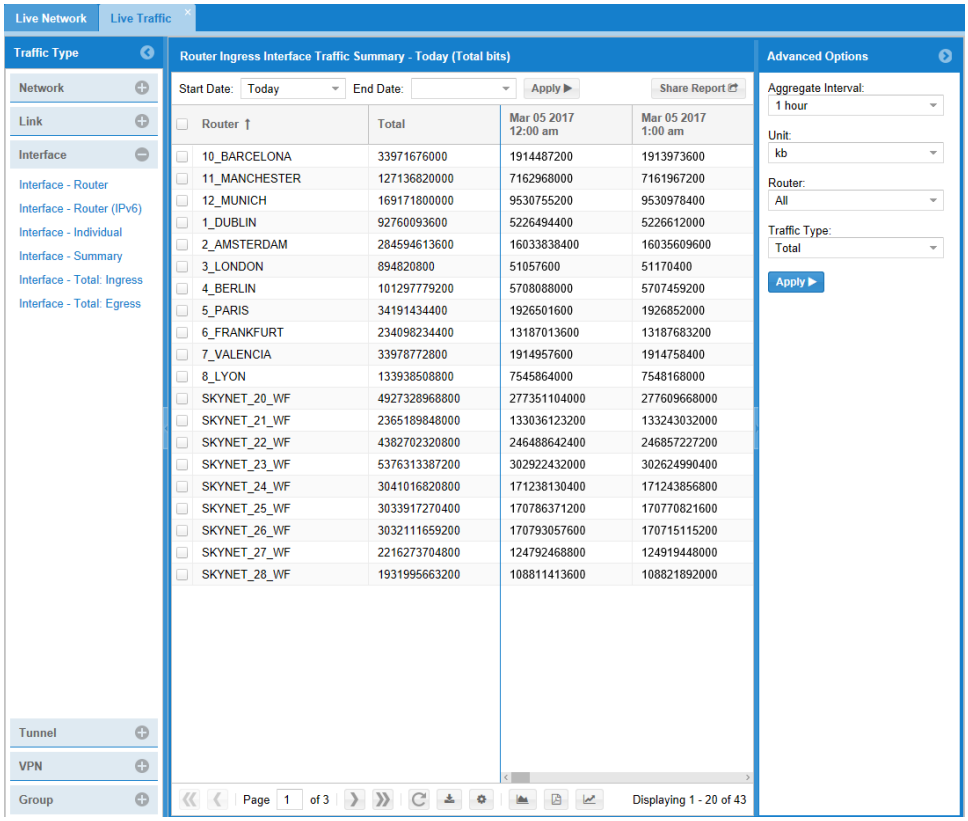
   The Live Traffic window is displayed.

2. In the Traffic Type pane, select **Interface > Interface - Total: Ingress.**

3. From the drop-down lists, select the Start Date and End Date, then click **Apply.**

   The Router Ingress Interface Traffic Summary Report is displayed, as shown in Figure 110 on page 143.

Figure 110: Router Ingress Interface Traffic Summary



4. (Optional) Expand the Advanced Options pane and select from the drop-down lists to change the following:

   Aggregate Interval—Select the interval in increments of minutes or hours.

   Unit—Select b (bytes), kb (kilobytes), Mb (Megabytes), or Gb (gigabytes).

   Traffic Type—Select Total or Average.

See Also • Monitoring Real-Time Traffic and Device Performance on page 152

Displaying a Router Ingress Tunnel Traffic Summary Report

To display a router ingress tunnel traffic summary report:

1. Select **Performance > Live Traffic**.

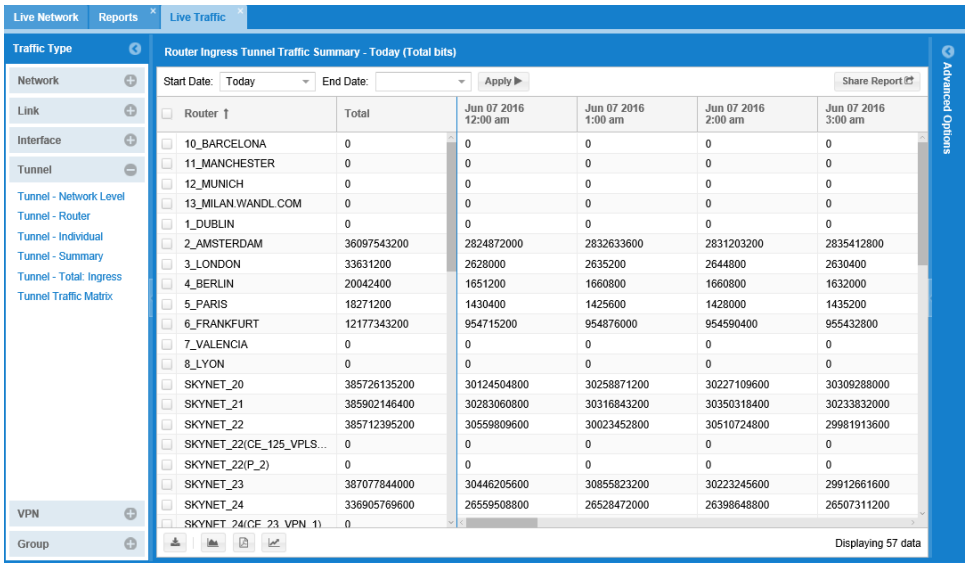
   The Live Traffic window is displayed.

2. In the Traffic Type pane, select **Tunnel > Tunnel - Total: Ingress.**

3. From the drop-down lists, select the Start Date and End Date, then click **Apply.**

   The Router Ingress Tunnel Traffic Summary Report is displayed, as shown in Figure 111 on page 144.

Figure 111: Router Ingress Tunnel Traffic Summary



Router	Total	Jun 07 2016 12:00 am	Jun 07 2016 1:00 am	Jun 07 2016 2:00 am	Jun 07 2016 3:00 am
10_BARCELONA	0	0	0	0	0
11_MANCHESTER	0	0	0	0	0
12_MUNICH	0	0	0	0	0
13_MILAN.WANDL.COM	0	0	0	0	0
1_DUBLIN	0	0	0	0	0
2_AMSTERDAM	36097543200	2824872000	2832633600	2831203200	2835412800
3_LONDON	33631200	2628000	2635200	2644800	2630400
4_BERLIN	20042400	1651200	1660800	1660800	1632000
5_PARIS	18271200	1430400	1425600	1428000	1435200
6_FRANKFURT	12177343200	954715200	954876000	954590400	955432800
7_VALENCIA	0	0	0	0	0
8_LYON	0	0	0	0	0
SKYNET_20	385726135200	30124504800	30258871200	30227109600	30309288000
SKYNET_21	385902146400	30283060800	30316843200	30350318400	30233832000
SKYNET_22	385712395200	30559809600	30023452800	30510724800	29981913600
SKYNET_22(CE_125_VPLS...	0	0	0	0	0
SKYNET_22(P_2)	0	0	0	0	0
SKYNET_23	387077844000	30446205600	30855823200	30223245600	29912661600
SKYNET_24	336905769600	26559508800	26528472000	26398648800	26507311200
SKYNET_24(CE_23_VPN_1)	0				

4. (Optional) Expand the Advanced Options pane and select from the drop-down lists to change the following:

   Aggregate Interval—Select the interval in increments of minutes or hours.

   Unit—Select b (bytes), kb (kilobytes), Mb (Megabytes), or Gb (gigabytes).

   Router—Select all or filter by specific router.

   Traffic Type—Select Total or Average.

See Also • Monitoring Real-Time Traffic and Device Performance on page 152

 Copyright © 2018, Juniper Networks, Inc.

Displaying LSP Bandwidth

To display the LSP bandwidth:

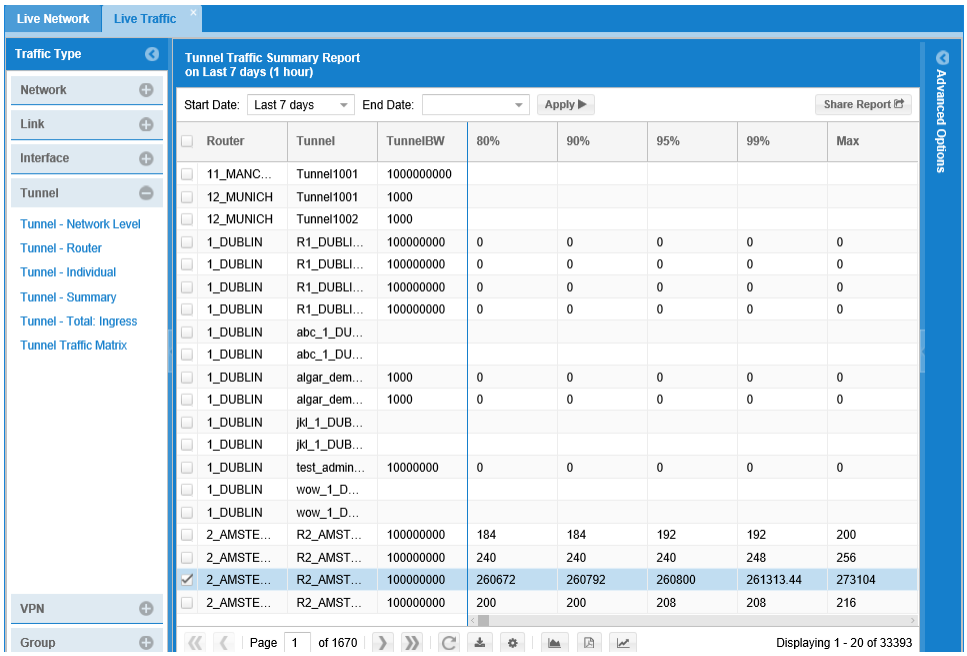
1. Select **Performance > Live Traffic**.

   The Live Traffic window is displayed.

2. In the Traffic Type pane, select **Tunnel > Tunnel - Summary**.

   The Tunnel Traffic Summary Report is displayed. Figure 112 on page 145 shows the Tunnel Traffic Summary Report.

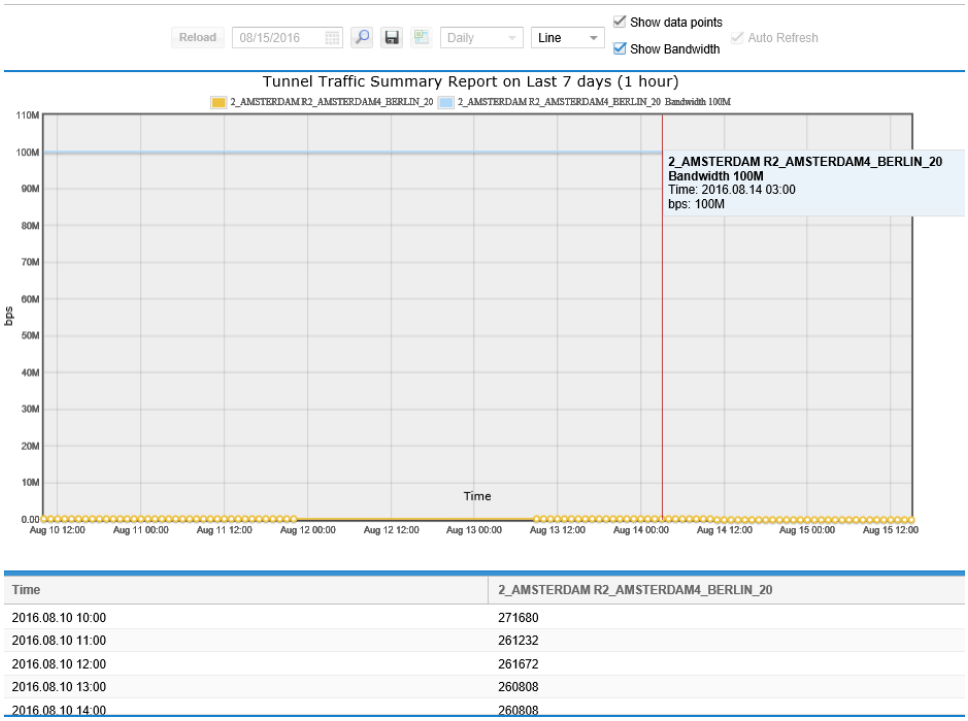
Figure 112: Tunnel Traffic Summary Report



Router	Tunnel	TunnelBW	80%	90%	95%	99%	Max
11_MANC...	Tunnel1001	1000000000					
12_MUNICH	Tunnel1001	1000					
12_MUNICH	Tunnel1002	1000					
1_DUBLIN	R1_DUBLI...	100000000	0	0	0	0	0
1_DUBLIN	R1_DUBLI...	100000000	0	0	0	0	0
1_DUBLIN	R1_DUBLI...	100000000	0	0	0	0	0
1_DUBLIN	R1_DUBLI...	100000000	0	0	0	0	0
1_DUBLIN	abc_1_DU...						
1_DUBLIN	abc_1_DU...						
1_DUBLIN	algar_dem...	1000	0	0	0	0	0
1_DUBLIN	algar_dem...	1000	0	0	0	0	0
1_DUBLIN	jkl_1_DUB...						
1_DUBLIN	jkl_1_DUB...						
1_DUBLIN	test_admin...	10000000	0	0	0	0	0
1_DUBLIN	wow_1_D...						
1_DUBLIN	wow_1_D...						
2_AMSTE...	R2_AMST...	100000000	184	184	192	192	200
2_AMSTE...	R2_AMST...	100000000	240	240	240	248	256
2_AMSTE...	R2_AMST...	100000000	260672	260792	260800	261313.44	273104
2_AMSTE...	R2_AMST...	100000000	200	200	208	208	216

3. Select the **Chart** icon in the lower pane, then select **Show Bandwidth** at the top of the displayed bandwidth chart.

Figure 113: LSP Bandwidth Chart



4. Mouse over the chart to display the LSP bandwidth for a specific time, as shown in Figure 113 on page 146.

See Also

- Monitoring Real-Time Traffic and Device Performance on page 152

Displaying a VPN Egress Traffic Summary Report

To display a VPN Egress Traffic Summary Report:

1. Select **Performance > Live Traffic**.

   The Live Traffic window is displayed.

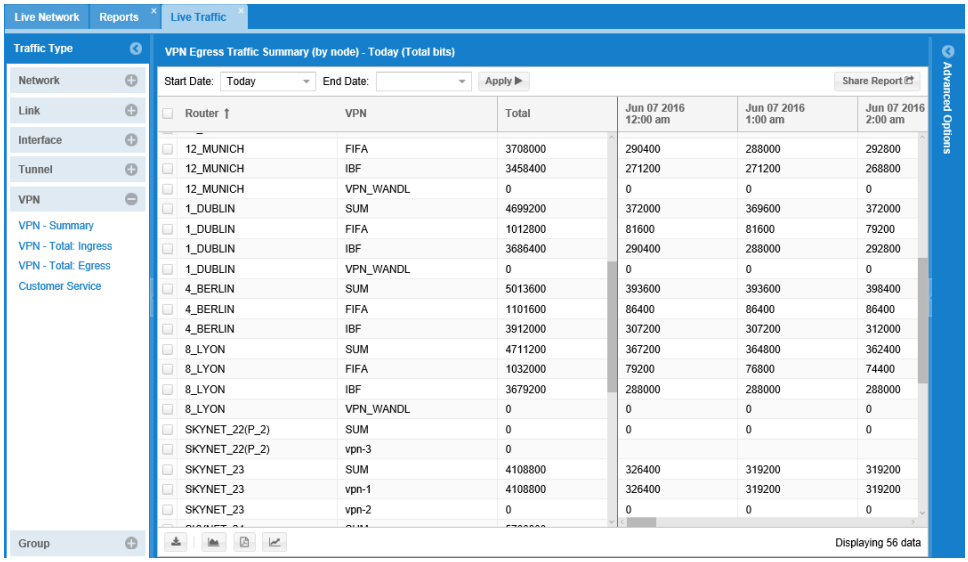
2. In the Traffic Type pane, select **VPN > VPN - Total: Egress.**

3. From the drop-down lists, select the Start Date and End Date, then click **Apply.**

   The VPN Egress Traffic Summary Report is displayed, as shown in Figure 114 on page 147.

Copyright © 2018, Juniper Networks, Inc.

Figure 114: VPN Egress Traffic Summary Report



Router	VPN	Total	Jun 07 2016 12:00 am	Jun 07 2016 1:00 am	Jun 07 2016 2:00 am
12_MUNICH	FIFA	3708000	290400	288000	292800
12_MUNICH	IBF	3458400	271200	271200	268800
12_MUNICH	VPN_WANDL	0	0	0	0
1_DUBLIN	SUM	4699200	372000	369600	372000
1_DUBLIN	FIFA	1012800	81600	81600	79200
1_DUBLIN	IBF	3686400	290400	288000	292800
1_DUBLIN	VPN_WANDL	0	0	0	0
4_BERLIN	SUM	5013600	393600	393600	398400
4_BERLIN	FIFA	1101600	86400	86400	86400
4_BERLIN	IBF	3912000	307200	307200	312000
8_LYON	SUM	4711200	367200	364800	362400
8_LYON	FIFA	1032000	79200	76800	74400
8_LYON	IBF	3679200	288000	288000	288000
8_LYON	VPN_WANDL	0	0	0	0
SKYNET_22(P_2)	SUM	0	0	0	0
SKYNET_22(P_2)	vpn-3	0			
SKYNET_23	SUM	4108800	326400	319200	319200
SKYNET_23	vpn-1	4108800	326400	319200	319200
SKYNET_23	vpn-2	0	0	0	0

4. (Optional) Expand the Advanced Options pane and select from the drop-down lists to change the following:

   Aggregate Interval—Select the interval in increments of minutes or hours.

   Unit—Select b (bytes), kb (kilobytes), Mb (Megabytes), or Gb (gigabytes).

   Traffic Type—Select Total or Average.

   Show Traffic—Select All or SUM only.

   Show—Select to filter by VPN or by node.

See Also

- Monitoring Real-Time Traffic and Device Performance on page 152

Aggregated Traffic Reports

The following aggregated traffic reports are organized by traffic type and are aggregated either hourly or daily.
General column filtering and sorting capabilities apply to all aggregated traffic reports.

Link

Link—Displays link traffic between two routers.

Interface

Interface—Displays summary interface traffic at each router.

Interface CoS—Displays summary interface CoS traffic at each router.

Interface Multicast—Displays summary interface multicast traffic at each router.

Packet Errors—Provides the number of inbound and outbound packets that could not be transmitted because of errors.

Packet Discards—Provides the number of inbound and outbound packets that were chosen to be discarded even though no errors had been detected. One possible reason for discarding such a packet could be to free up buffer space.

Tunnel

- Tunnel—Displays summary tunnel traffic at each router.

VPN

VPN—Provides the total in and out traffic per VPN.

VPN CoS—Provides the total in and out CoS traffic per VPN.

VPN Multicast—Provides the total in and out multicast traffic per VPN.

Customer Service—Provides the total in and out traffic per Customer Service VPN.

Customer Service CoS—Provides the total in and out CoS traffic per Customer Service VPN.

Customer Service Multicast—Provides the total in and out multicast traffic per Customer Service VPN.

Group

Interface Group—Provides the total in and out traffic for the interfaces in a group. These groups are defined in Admin > Report Groups.

Interface Group CoS—Provides the total in and out CoS traffic for the interfaces in a group. These groups are defined in Admin > Report Groups.

Interface Group Multicast—Provides the total in and out multicast traffic for the interfaces in a group. These groups are defined in Admin > Report Groups.

AS—Provides the total in and out traffic for the interfaces in an autonomous system.

Related Documentation

- Live Traffic on page 140

Live VPN Traffic

You can display live VPN traffic from the Performance tab in the IP/MPLSView main window.

To display live VPN traffic:

1. Select **Performance > Live VPN traffic**.

Copyright © 2018, Juniper Networks, Inc.

The IP VPN window is displayed.

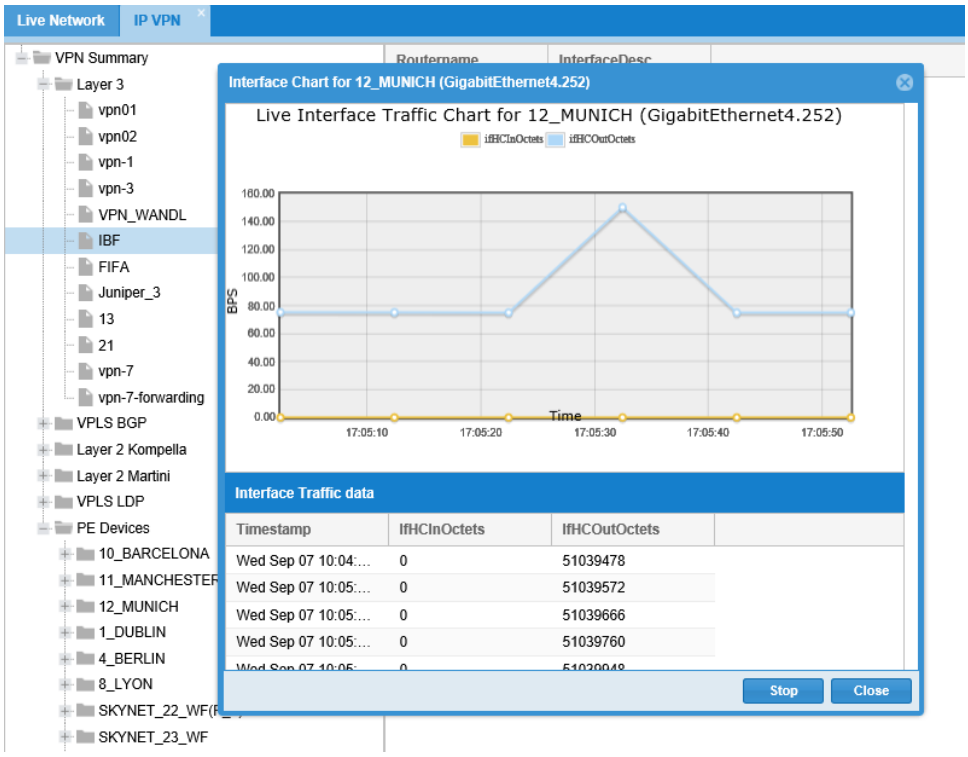
2. Expand the menu and select a VPN instance in the left tree view to list the available VPN interfaces.

   The router names and interface descriptions are displayed in the right pane.

3. Select a router name and interface description, then right-click and select **Open Live Interface Traffic Chart**.

   The Live Interface Traffic Chart is displayed. Figure 115 on page 149 shows the Live Interface Traffic Chart.

Figure 115: Live VPN Traffic



Related Documentation

- Live Traffic on page 140

Monitoring the Status of Your Network

- Real-Time Network Status on page 150
- Monitoring Real-Time Network Status on page 150
- Monitoring Real-Time Status for LSPs (Tunnels) on page 151
- Monitoring Real-Time Status for BGP Neighbors on page 152

Real-Time Network Status

You can display real-time status for the following network elements from the IP/MPLSView Web interface:

- Live links
- Live label-switched paths (LSPs)
- Live BGP neighbors
- Live OSPF neighbors
- Live IS-IS adjacencies

Monitoring Real-Time Network Status

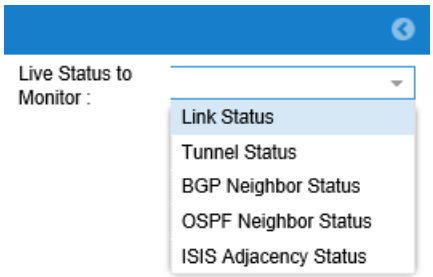
To monitor real-time network status:

1. Select **Performance > Real Time Status**.

   The Real Time Status window is displayed.

2. Select the type of live status you want to monitor from the Live Status to Monitor menu.

Figure 116: Live Status to Monitor Menu



3. Review the results in the Live Status window that appears for the selected network element.

   Each column head has a menu. From the menu within each column you can sort the element information in ascending or descending order. You can also select which columns are displayed or hidden, resize columns, and rearrange the column order.

Copyright © 2018, Juniper Networks, Inc.

Monitoring Real-Time Status for LSPs (Tunnels)

To monitor real-time status for LSPs (tunnels):

1. Select **Performance > Real Time Status**.

   The Real Time Status window is displayed.

2. Select **Tunnel Status** from the Live Status to Monitor menu.

3. Display the live Tunnel Status window in one of the following ways:

   - To view an unfiltered status display for all nodes, select **No Filtering** in the Set Filters field.
   - To view a display filtered by node, select **Filter by Node** in the Set Filters field, select a node name from the Select Nodes menu, and click **Apply Node Filter**.

   For example, Figure 118 on page 151 shows the Live Tunnel Status window filtered by the node named VMX101.

Figure 117: Live Tunnel Status Window with Filtered Display

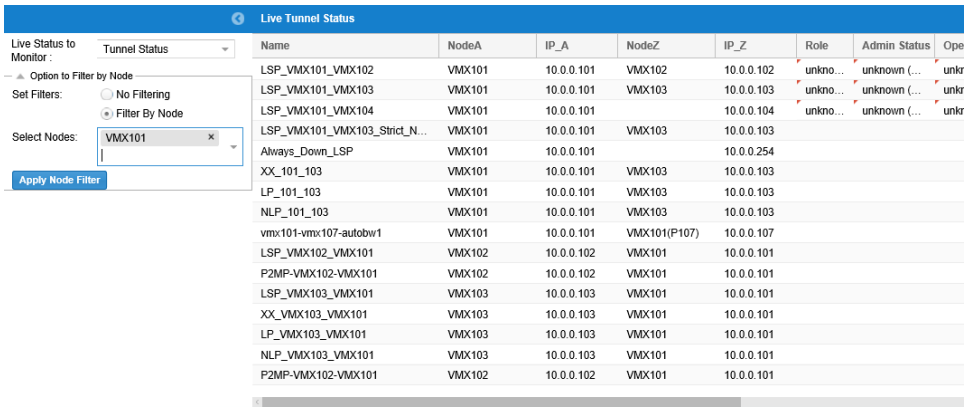
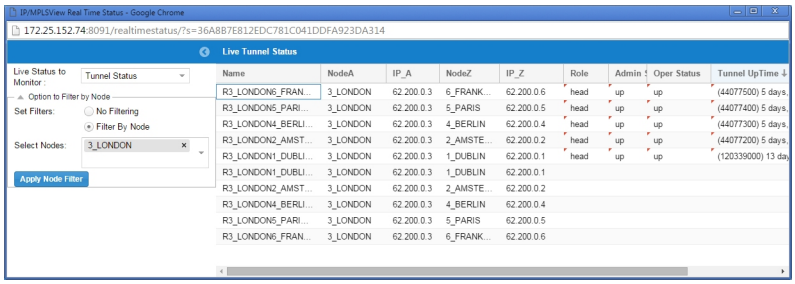


Figure 118: Live Tunnel Status Window with Filtered Display



4. Review the results in the Live Tunnel Status window.

   Make sure the administrative status (Admin Status) and operational status (Oper Status) are both reported as **up** for each tunnel.

Monitoring Real-Time Status for BGP Neighbors

To monitor real-time status for BGP neighbors:

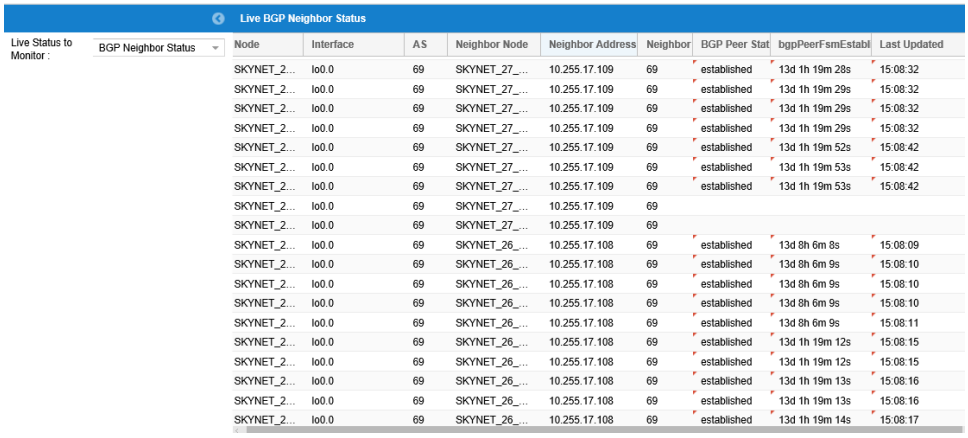
1. Select **Performance > Real Time Status**.

   The Real Time Status window is displayed.

2. Select **BGP Neighbor Status** from the Live Status to Monitor menu.

   The Live BGP Neighbor Status window is displayed. Figure 119 on page 152 shows the Live BGP Neighbor Status window.

Figure 119: Live BGP Neighbor Status Window



Node	Interface	AS	Neighbor Node	Neighbor Address	Neighbor	BGP Peer Stat	bgpPeerFsmEstabl	Last Updated
SKYNET_2...	lo0.0	69	SKYNET_27_...	10.255.17.109	69	established	13d 1h 19m 28s	15:08:32
SKYNET_2...	lo0.0	69	SKYNET_27_...	10.255.17.109	69	established	13d 1h 19m 29s	15:08:32
SKYNET_2...	lo0.0	69	SKYNET_27_...	10.255.17.109	69	established	13d 1h 19m 29s	15:08:32
SKYNET_2...	lo0.0	69	SKYNET_27_...	10.255.17.109	69	established	13d 1h 19m 29s	15:08:32
SKYNET_2...	lo0.0	69	SKYNET_27_...	10.255.17.109	69	established	13d 1h 19m 52s	15:08:42
SKYNET_2...	lo0.0	69	SKYNET_27_...	10.255.17.109	69	established	13d 1h 19m 53s	15:08:42
SKYNET_2...	lo0.0	69	SKYNET_27_...	10.255.17.109	69	established	13d 1h 19m 53s	15:08:42
SKYNET_2...	lo0.0	69	SKYNET_27_...	10.255.17.109	69			
SKYNET_2...	lo0.0	69	SKYNET_27_...	10.255.17.109	69			
SKYNET_2...	lo0.0	69	SKYNET_26_...	10.255.17.108	69	established	13d 8h 6m 8s	15:08:09
SKYNET_2...	lo0.0	69	SKYNET_26_...	10.255.17.108	69	established	13d 8h 6m 9s	15:08:10
SKYNET_2...	lo0.0	69	SKYNET_26_...	10.255.17.108	69	established	13d 8h 6m 9s	15:08:10
SKYNET_2...	lo0.0	69	SKYNET_26_...	10.255.17.108	69	established	13d 8h 6m 9s	15:08:10
SKYNET_2...	lo0.0	69	SKYNET_26_...	10.255.17.108	69	established	13d 8h 6m 9s	15:08:11
SKYNET_2...	lo0.0	69	SKYNET_26_...	10.255.17.108	69	established	13d 1h 19m 12s	15:08:15
SKYNET_2...	lo0.0	69	SKYNET_26_...	10.255.17.108	69	established	13d 1h 19m 12s	15:08:15
SKYNET_2...	lo0.0	69	SKYNET_26_...	10.255.17.108	69	established	13d 1h 19m 13s	15:08:16
SKYNET_2...	lo0.0	69	SKYNET_26_...	10.255.17.108	69	established	13d 1h 19m 13s	15:08:16
SKYNET_2...	lo0.0	69	SKYNET_26_...	10.255.17.108	69	established	13d 1h 19m 14s	15:08:17

3. Review the results in the Live BGP Neighbor Status window.

   Make sure the BGP Peer Status is reported as **established** for each BGP neighbor.

Related Documentation

- Monitoring Real-Time Traffic and Device Performance on page 152

Monitoring Real-Time Traffic and Device Performance

- Real-Time Usage for Traffic and Device Performance on page 152
- Monitoring Real-Time Usage for Link Traffic on page 153
- Monitoring Real-Time Usage for Device Performance on page 154

Real-Time Usage for Traffic and Device Performance

You can display real-time usage information for the following types of network traffic from the IP/MPLSView Web interface by selecting **Performance Management > Real Time Usage** or by right-clicking a node or link on the live network topology map:

- Interface traffic
- Label-switched path (LSP) traffic

Copyright © 2018, Juniper Networks, Inc.

- Link traffic

You can also display real-time usage information for device performance.

Monitoring Real-Time Usage for Link Traffic

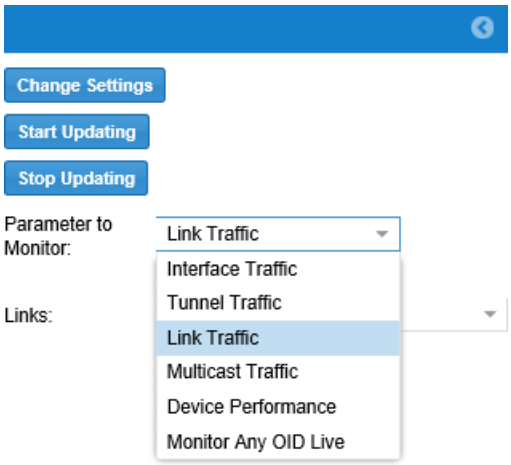
To monitor real-time usage for link traffic:

1. Select **Performance > Real Time Usage**, or click a link on the live network topology map.

   The Real Time Usage window is displayed.

2. Select **Link Traffic** from the Parameter to Monitor menu. Figure 120 on page 153 shows the Parameter to Monitor menu.

Figure 120: Parameter to Monitor Menu

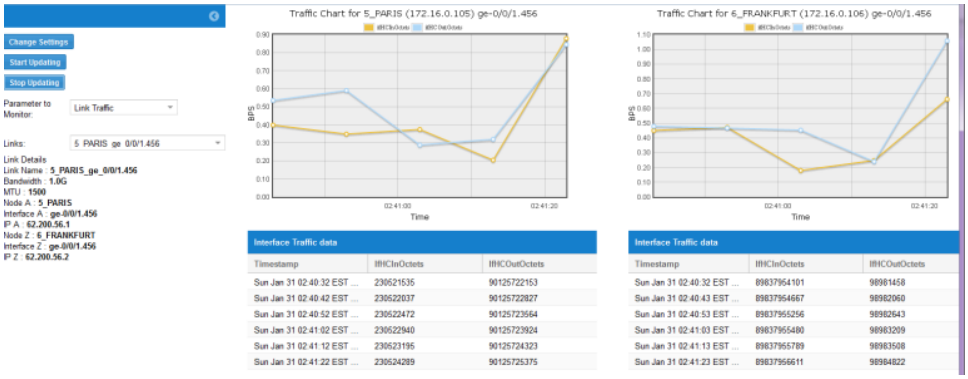


3. Select a live link to monitor in the Links menu.

   The Link Traffic Chart for the selected link is displayed.

   Figure 121 on page 154 shows the real-time usage display for live link traffic between node 5_PARIS (Node A) and 6_FRANKFURT (Node Z).

Figure 121: Link Traffic Chart



4. Click **Start Updating** to begin polling the data, and click **Stop Updating** when you are ready to stop polling the data.

   The usage information for link traffic is calculated by polling the two ends of the link side-by-side every 10 seconds.

5. Review the real-time usage results in the Link Traffic Chart.

   Make sure the inbound traffic (ifHCInOctets, represented by the yellow line) and outbound traffic ((ifHCOutOctets, represented by the blue line) for each end of the link look more or less consistent with each other, and with the traffic at the other end of the link.

Monitoring Real-Time Usage for Device Performance

To monitor real-time usage for device performance:

1. Select **Performance > Real Time Usage**, or click a device on the live network topology map.

   The Real Time Usage window appears.

2. Select **Device Performance** from the Parameter to Monitor menu.

3. Specify the name of the host (node) for which you want to monitor device performance usage.

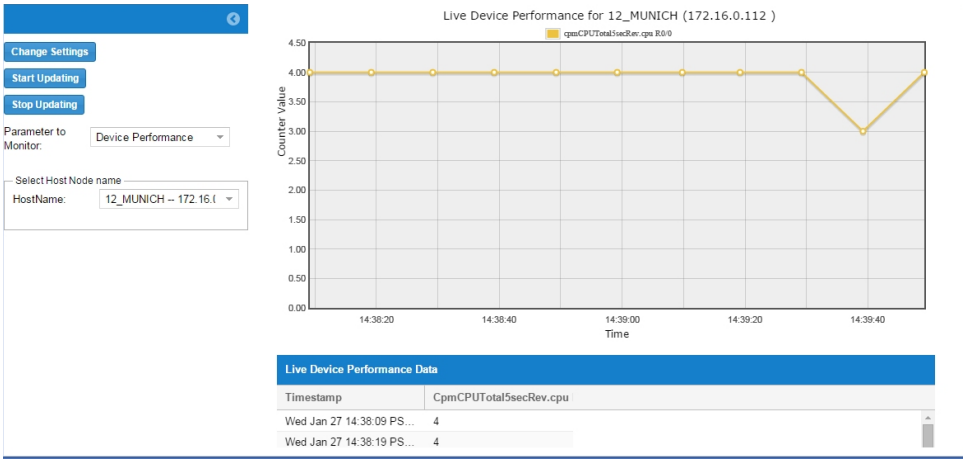
   The Select Device Perf Counters window appears.

4. Use the arrow keys to move the device object you want to monitor from the Available Objects list to the Selected Objects list, and click **Apply**.

   The Live Device Performance Chart window for the selected object appears.

Copyright © 2018, Juniper Networks, Inc.

Figure 122: Live Device Performance Chart Window



5. Click **Start Updating** to begin polling the data, and click **Stop Updating** when you are ready to stop polling the data.

   The usage information for device performance includes information about CPU utilization, memory, and temperature.

6. Review the real-time usage results in the Live Device Performance Chart.

Related Documentation

- Monitoring the Status of Your Network on page 149

Monitoring Any OID in Real Time

- Real-Time Usage for Any OID on page 155
- Monitoring Any OID Live on page 156

Real-Time Usage for Any OID

Using IP/MPLSView, you can display real-time usage information to monitor any object identifier (OID) in your network and view the results in tabular or chart format. This feature is useful if you want to monitor a specific OID continuously for a particular node in your live network.

Initially, you must manually specify the inputs for monitoring, including the node (host) name and the OID to monitor, in the Inputs for Monitor Any OID window. If you want to reuse these monitoring inputs later to monitor this OID for the same node or for a different node, you can conveniently save the monitoring inputs as a template for future use. IP/MPLSView saves these templates as CSV files in the **/u/wandl/data/monitorAnyOID** directory.

When you monitor an OID live, IP/MPLSView uses SNMP to monitor the OID in real time by polling the specified OID every 10 seconds and displaying the continuously updated

results in charts or tabular reports. The tabular report format displays the OID descriptions in columns.

Monitoring Any OID Live

To monitor any OID live:

1. Select **Performance > Real Time Usage**.

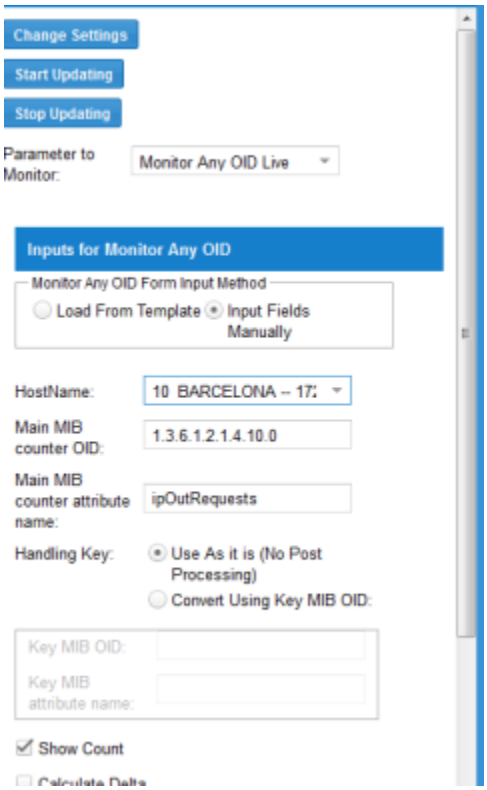
   The Real Time Usage window is displayed.

2. Select **Monitor Any OID Live** from the Parameter to Monitor menu.

   The Inputs for Monitor Any OID window are displayed in the left pane.

3. Specify the monitoring inputs.

Figure 123: Inputs for Monitor Any OID Window



Select a parameter to monitor and a hostname. Select whether to have the data processed using the key MIB OID. If post-processing is enabled, a key MIB OID is specified to link the main counter to a name or description, and to specify a utilization OID to compute utilization. Enter the main MIB counter OID and counter attribute name. Scroll down the left pane and select whether to show the calculate delta and calculate rate. Select the counter unit for representation. If calculate rate is enabled, the system computes the delta divided by the time difference and plots it on the chart.

Copyright © 2018, Juniper Networks, Inc.

4. (Optional) Save the monitoring inputs as a template If you want to reuse them later.

   At the bottom of the Inputs for Monitor Any OID window, select the **Save Form as Template** check box, specify a template name and description, and click **Save Form As Template**. A message appears confirming that the template has been saved.

   The next time you monitor any OID live, the Load from Template button appears in the Inputs for Monitor Any OID window. To load a previously saved template, click **Load from Template** and select the name of your template file from the Template Name menu. The Inputs for Monitor Any OID window is automatically populated with the settings in your template.

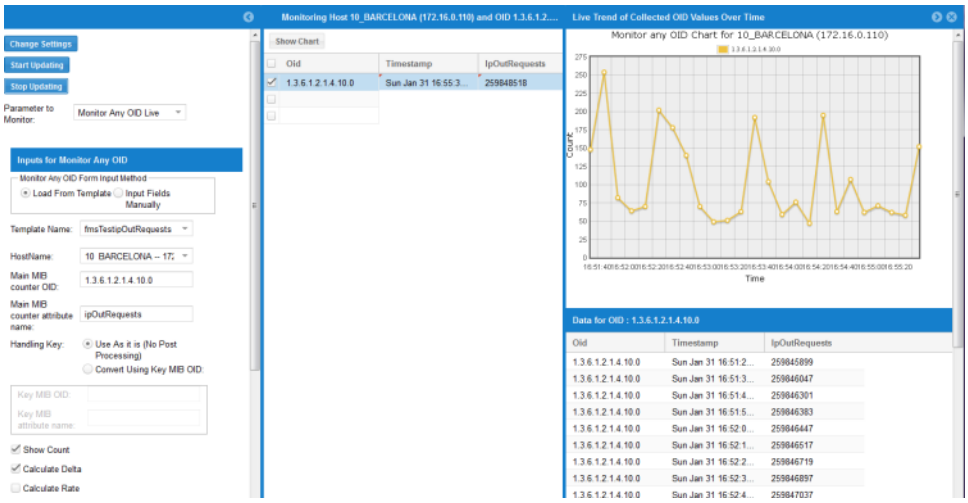
5. Click **Apply**.

   A list of monitored OIDs appears in the middle pane. Select the OID you want and click **Show Chart**.

   The Monitor Any OID Chart window appears for the device and OID you selected.

   Figure 124 on page 157 shows an example of the Monitor Any OID Chart window for the ipOutRequests OID on device 10_BARCELONA. In this example, the monitoring inputs were loaded from a previously saved template named fmsTestipOutRequests.

Figure 124: Monitor Any OID Chart Window from Template



Related Documentation

- Monitoring Real-Time Traffic and Device Performance on page 152

Diagnostics

The Diagnostics Manager feature enables you to run network diagnostic tools such as ping, CLI commands, test connectivity, and traceroute. Adobe Flash needs to be installed to run certain tools.

Diagnostics Manager

Diagnostics Manager provides the capability to perform basic and advanced ping commands as well as checking router connectivity.

The Run CLI feature provides the capability to run multiple CLI commands on a selected device.

Run CLI and Diagnostic Tool

To use the Run CLI tool in the IP/MPLSView interface:

1. Select **Performance > Diagnostics > Run CLI**.

2. Select the name of the device from the Device pane.

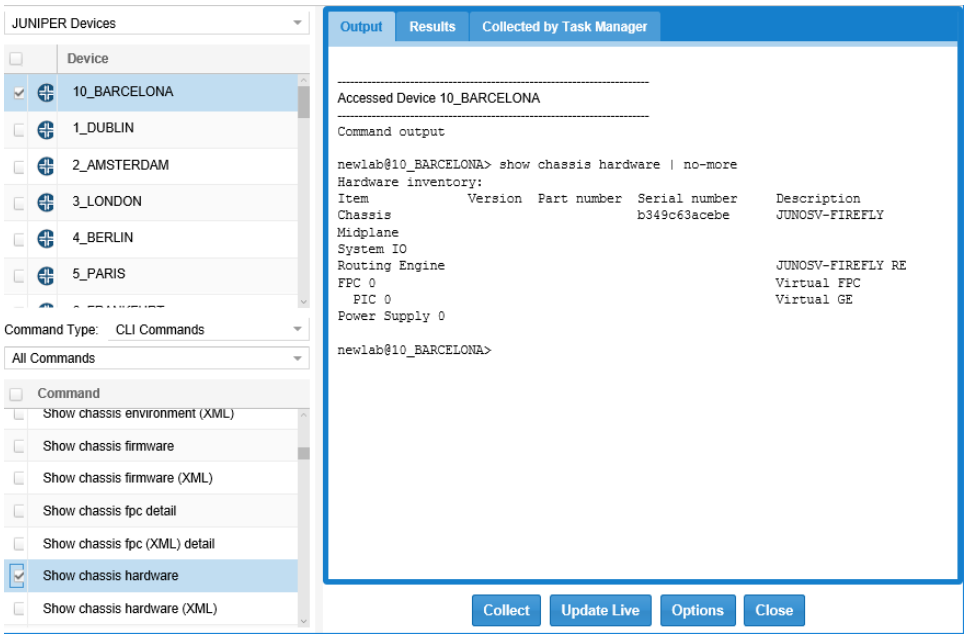
3. From the CLI Commands pane, expand the command category for the command you want to run.

4. Select the check box for the specific CLI command you want to run, and click **Collect**.

5. Specify the appropriate parameters for your command, and click **Run CLI**.

   The Output pane displays the command output for the selected CLI command, as shown in Figure 125 on page 158.

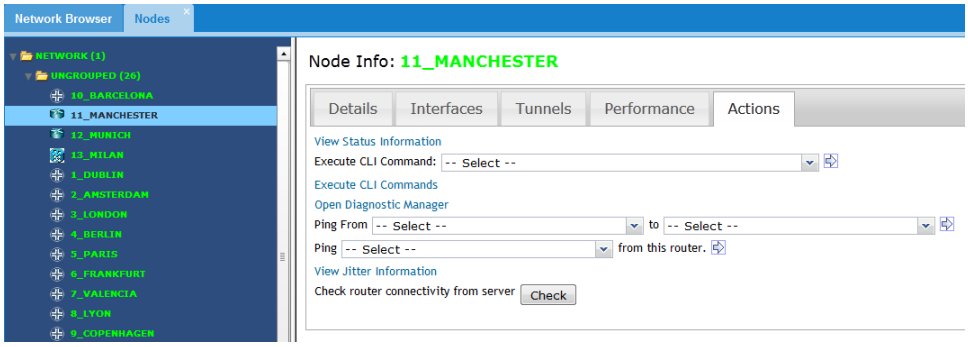
Figure 125: Run CLI Window for Selected Device



You can also execute CLI commands and open the Diagnostics Manager by selecting the Actions tab from the Node Info pane. See Figure 126 on page 159.

Copyright © 2018, Juniper Networks, Inc.

Figure 126: Run CLI from Actions Tab of Node Info Pane



Take any of the following actions:

- To run a single CLI command, select the command from the **Execute CLI Command** drop-down menu.
- To execute multiple CLI commands in a batch, select **Execute CLI Commands**.
- To access the Diagnostics Manager, select **Open Diagnostic Manager**.

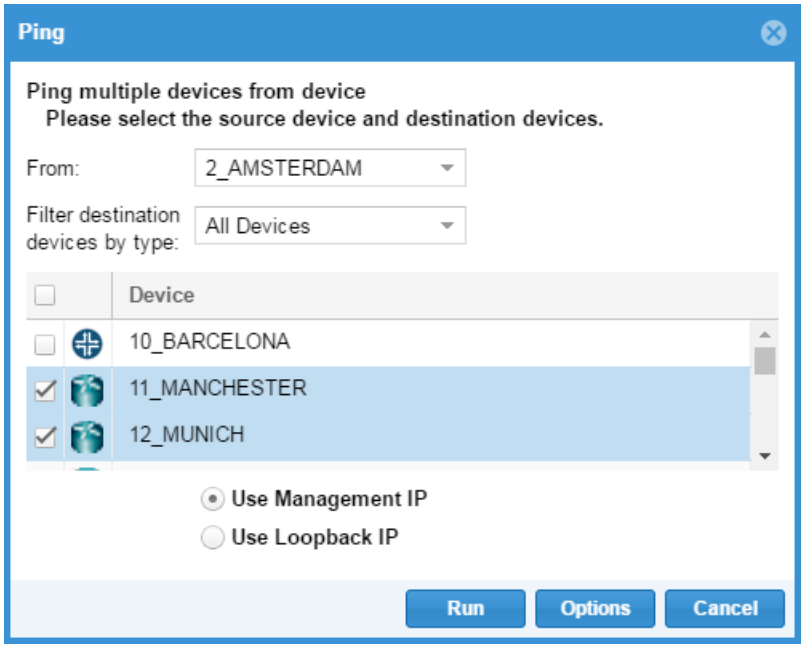
For more detailed information about running CLI commands and accessing the Diagnostics Manager from the Node Info page, see Nodes.

Ping Multiple Routers

Use the Ping Multiple Routers function to check the connectivity between multiple routers in the network, and measure latency and packet loss. Ping results are generated, displaying the ping times between all possible pairs of the selected routers. Ping time refers to the time it takes for a small packet of data to travel from one device to another and back.

Select multiple routers from the list. Then, click **Run** and wait until all the results have populated in the table. This might take a few minutes. Figure 127 on page 160 shows the Ping window.

Figure 127: Ping Multiple Routers



NOTE: The designation “n/a” (not available) may signify that the ping operation timed out. If there are VPNs in your network, it may signify that the two devices are not in the same VPN.

The default color codings and ping thresholds are described in Table 26 on page 160. These values can be adjusted by the administrator.

Table 26: Default Color Codings

Color	Meaning
Green	Acceptable. The ping operation took less than 150 ms.
Yellow	Problematic. The ping operation took between 150 ms and 400 ms.
Red	Unacceptable. The ping operation timed out or took longer than 400 ms. There may not be any connectivity between the two devices.

NOTE: Each outcome displayed in the table is actually the result of multiple pings. The Ping Count, or number of pings actually issued between devices, depends upon the diagnostics settings configured by the Web administrator in Admin > Diagnostics Settings. Ping parameter settings are described in Diagnostic Configuration Settings.

Copyright © 2018, Juniper Networks, Inc.

In the ping results table (Table 27 on page 161), the default view shows the average (avg) ping results, in milliseconds. You can also choose to display the minimum, maximum, or loss percent of the pings by clicking on the respective word(s) following the table. See Table 27 on page 161 for ping results descriptions.

Table 27: Ping Results

Feature	Description
min/max/avg	Displays the minimum, maximum, or average ping time experienced, respectively. (Multiple pings are actually issued.)
loss %	Displays the percentage of pings that are lost or dropped between each device pair.

Ping Router from Router

The Ping Router from Router function is similar to the Ping Multiple Routers diagnostic described in *Ping Multiple Routers*. It allows you to check the connectivity between one particular router and several other routers in the network. Select one router from the list. Then in the second router list, select one or more routers, and click **Run**.

Check Router Connectivity

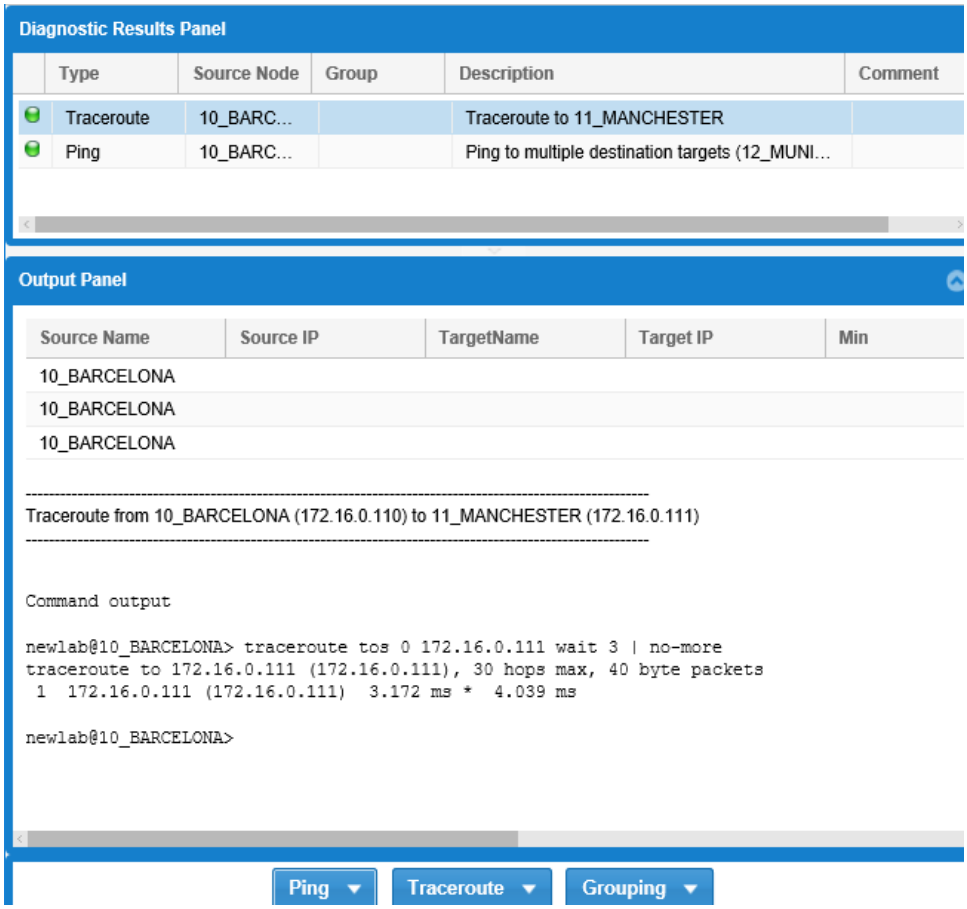
The Check Router Connectivity function allows you to check the connectivity status between the IP/MPLSView server and a particular device in the network. Select the router from the list, and click **Run**. The program will ping the device and report whether it is UP or DOWN.

Traceroute

The Traceroute function allows you to trace the route that an IP packet follows from one device to another in the Live network. Select the source and destination routers from the two selection boxes, and click **Run**. Figure 128 on page 162 shows an example traceroute output.

Copyright © 2018, Juniper Networks, Inc.

Figure 128: Traceroute Output



If the traceroute times out, the message **No route to host** is displayed.

NOTE: Traceroute parameter settings can be changed in Admin > Diagnostic Settings. These parameters are described in Diagnostic Configuration Settings.

Related Documentation

- Running the CLI on page 162
- Diagnostic Manager on page 166
- Nodes on page 57

Running the CLI

- Running CLI Commands on page 163
- Running CLI Commands on Multiple Devices on page 163
- Displaying Collected Data from the Task Manager on page 165
- Running Live Network Updates for Selected Devices on page 166

Copyright © 2018, Juniper Networks, Inc.

Running CLI Commands

When running CLI commands you can:

- Run commands on multiple devices.
- Filter commands that are organized by categories.
- Cache outputs and organize the outputs by devices.
- Display collected data from the Task Manager.

See Also

- Diagnostic Manager on page 166

Running CLI Commands on Multiple Devices

To run CLI commands on multiple devices:

1. Select **Performance > Run CLI**.

   The Run CLI Commands window is displayed.

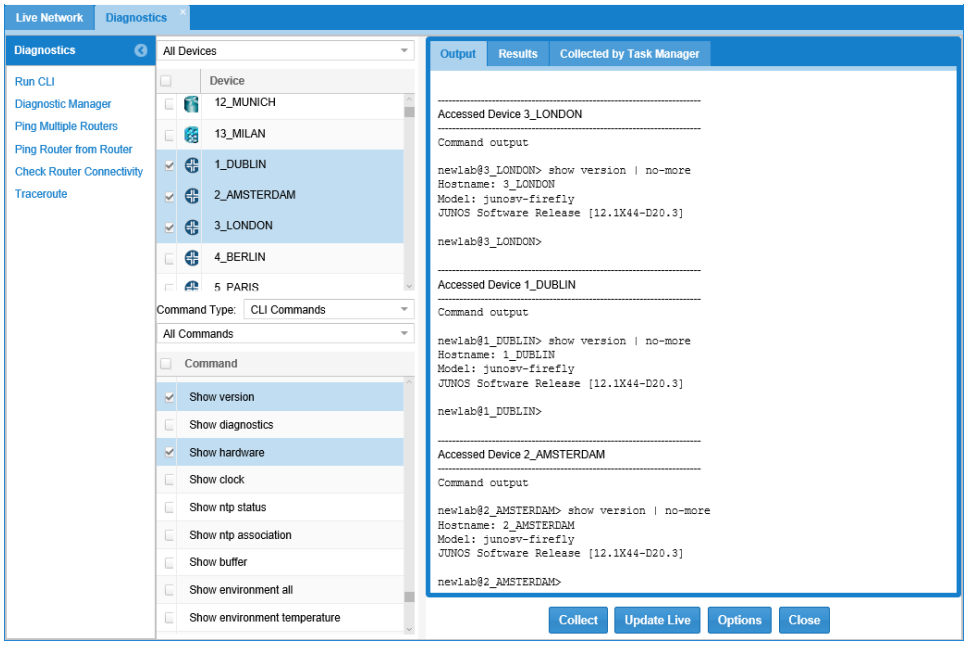
2. In the Device Selection pane, select one or more devices, and in the Command Selection pane, filter and select commands to run on the devices.

   To filter the devices view to a subset of devices of a particular hardware vendor, select the vendor from the All Devices menu. Similarly, to narrow down the commands listed to a category of commands, type the category of command, and then click the arrow next to Command. Note that when changing the view, the previous selections will be lost and only the devices and commands within the current view can be selected. You can also select Command Types.

3. Click **Collect** to display the collected data in the Output tab pane. Figure 129 on page 164 shows the RUN CLI window populated with the results of **show versions** and **show chassis environment** CLI commands for a single device.

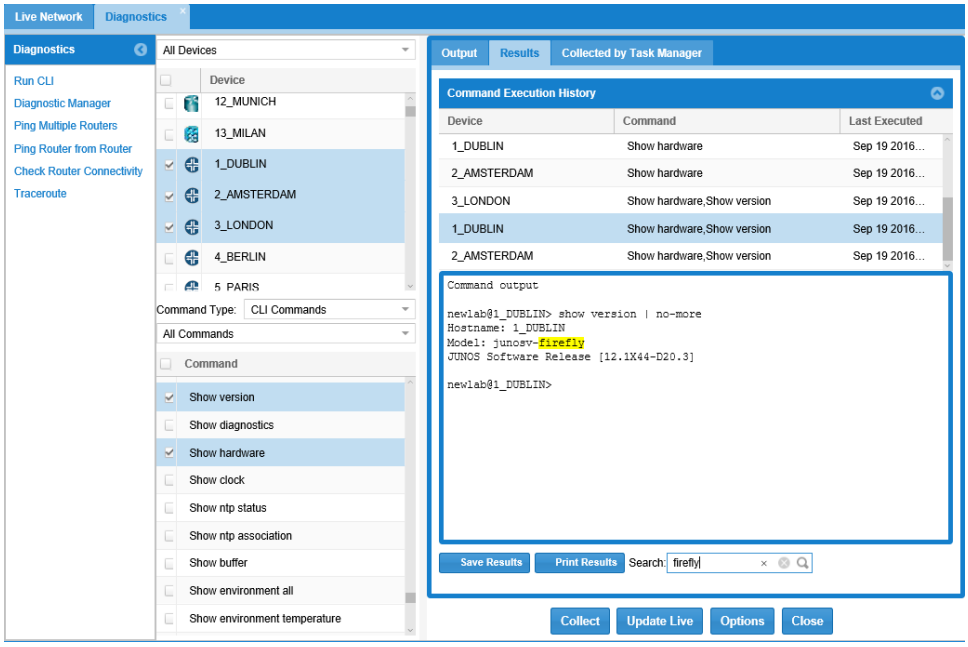
   Certain commands require that you specify an additional parameter. Only one such command can be selected at a time, and you are prompted to enter the parameter when collecting the data for that command. When applicable, the parameter request displays as (OPTION) in the Command Input Parameters window.

Figure 129: Run CLI Window



4. Select the **Results** tab to view the Command Execution History pane, that displays the dates and commands run on the listed devices. Figure 130 on page 164 shows the Results pane with the Command Execution History list to display the output.

Figure 130: Command Execution History and Output



Copyright © 2018, Juniper Networks, Inc.

5. (Optional) From the Results tab, select **Save Results** or **Print Results**.

6. (Optional) From the Results tab, in the Search field, type a text string to find and highlight that specific string in the CLI output.

See Also • Diagnostic Manager on page 166

Displaying Collected Data from the Task Manager

To display command output that has been collected by a task in the Task Manager:

1. Select **Performance > Run CLI**.

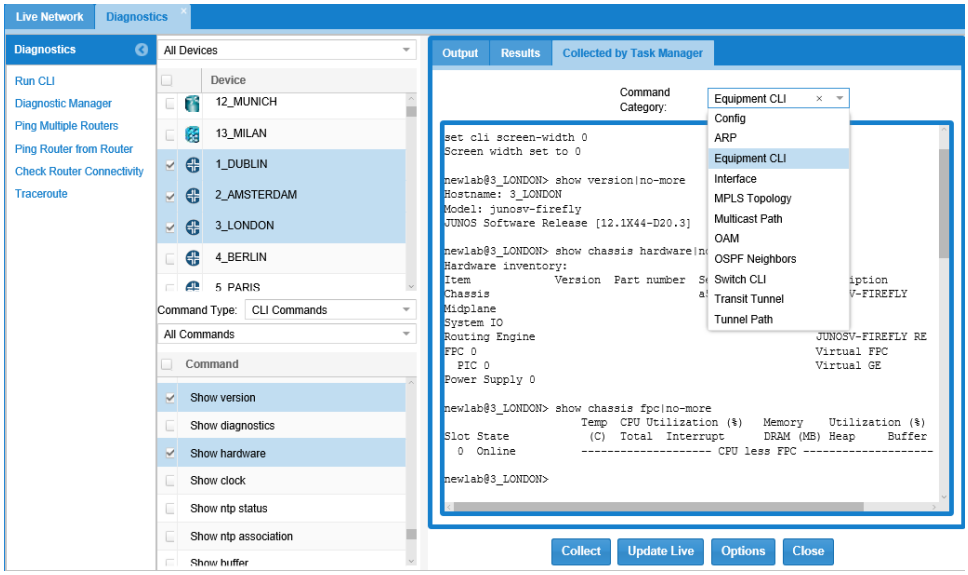
   The Run CLI Commands window is displayed.

2. From the **Collected by Task Manager** tab and in the Command Category list, select the category of command.

3. Select a device from the Device Selection pane.

   The collected data for the selected device is displayed automatically in the Collected by Task Manager pane. Figure 131 on page 165 shows the Collected by Task Manager command category menu and command output display.

Figure 131: Command Output Collected by Task Manager



See Also • Diagnostic Manager on page 166

Running Live Network Updates for Selected Devices

To run live network updates for selected devices:

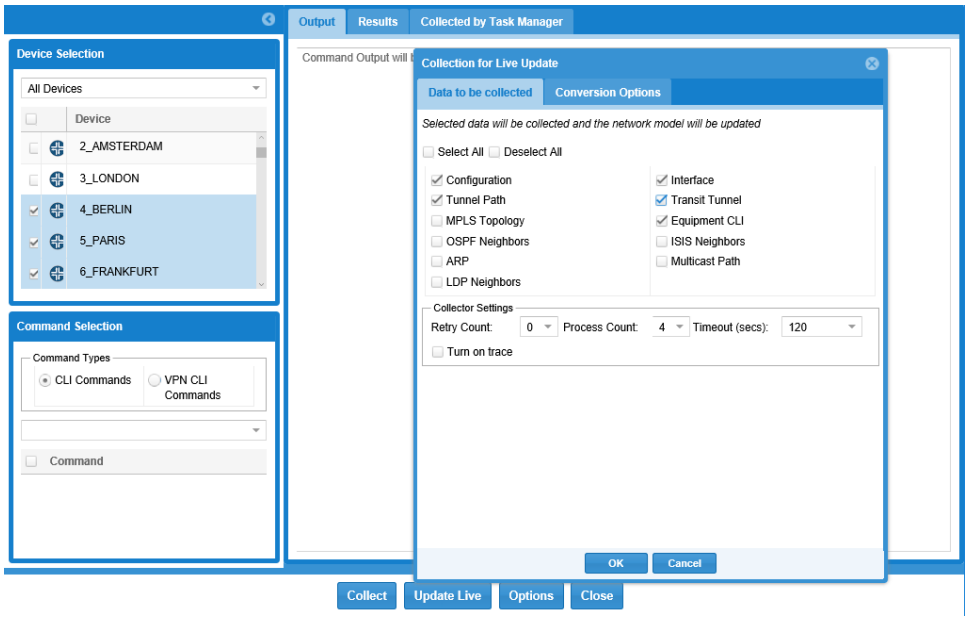
1. Select **Performance > Run CLI**.

   The Run CLI window is displayed.

2. In the Device Selection pane, select one or more devices, and then click **Update Live**.

   The Collection for Live Update dialog box is displayed, as shown in Figure 132 on page 166.

Figure 132: Collection for Live Update



3. Select the data to be collected, then click **OK**.

   Incremental updates are displayed as the tasks are completed. Check the Task Manager to see the detailed status.

Related Documentation

- Task Manager on page 199

Diagnostic Manager

- Understanding the Diagnostic Manager on page 167
- Pinging from Device to Device on page 169
- Pinging Multiple Devices from a Device on page 169
- Pinging Multiple Devices from a Server on page 171

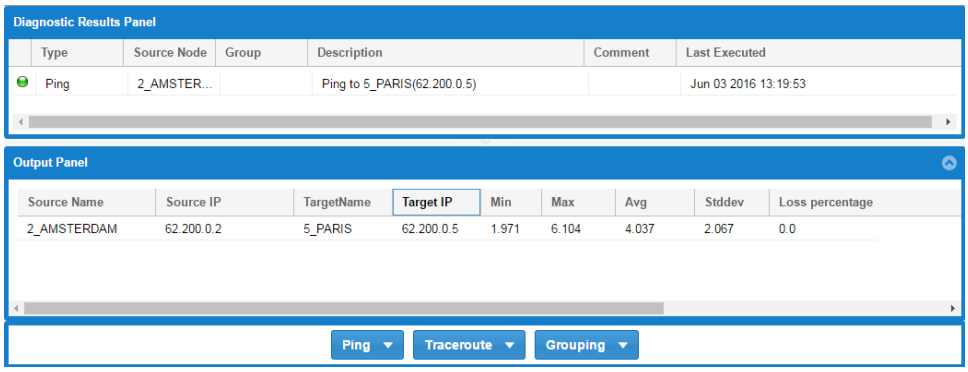
Copyright © 2018, Juniper Networks, Inc.

- Performing a Continuous Ping on page 172
- Running Traceroute from Device to Device on page 172
- Running Traceroute on Multiple Devices from a Device on page 173
- Pinging and Traceroute for Device Groups on page 174
- Pinging and Traceroute for a Customized Advanced Group on page 175

Understanding the Diagnostic Manager

The Diagnostic Manager provides an interface to keep track of ping and traceroute operations performed on the live network. To open Diagnostic Manager, select **Performance > Diagnostics > Diagnostic Manager**. Figure 133 on page 167 shows the Diagnostic Manager window populated with the results of a ping test.

Figure 133: Diagnostic Manager Window



The ping and traceroute features provide the following options:

Ping > Device From Device—Ping from one device to another device. The Advanced option provides a selection of ping commands for the device.

Ping > Multiple Devices From Device—Ping from one device to multiple devices.

Ping > Devices from Server—Ping from the IP/MPLSView server to multiple devices.

Ping > Devices to Device/Server—Ping from multiple devices to a device or to the IP/MPLSView server. Note that even if the server can ping a device by its loopback address, this does not guarantee that the device can also ping the server. It is possible that the source interface that the device uses to ping the server is unreachable to the server, so that the ping response never returns to the device.

Ping > Continuous Ping—Ping at regular intervals between two devices and display the result graphically. The Advanced option provides a selection of ping commands available for the device.

Traceroute > Device From Device—Traceroute between two devices and display the path on the map (right-click menu option). The Advanced option provides a selection of traceroute commands available for the device.

Copyright © 2018, Juniper Networks, Inc.

Traceroute > Multiple Devices From Device—Traceroute from one device to multiple devices.

The grouped pings feature provides the following options:

Ping/Traceroute within Device Group—Perform a ping between each pair of routers in the group.

Ping/Traceroute between Device Groups—Perform a ping from routers in the first group to routers in the second group.

Ping/Traceroute from Device Group to Multiple Devices—Ping from routers in the first group to selected routers.

Ping within Devices of VPN—For a given Layer 3 VPN, ping from PE to CE, CE to PE, or PE to CE loopback. This VPN group must be predefined by selecting **Grouping > Customized VPN Diagnostics**.

Ping/Traceroute by Customized Advanced Group—Perform a ping between each designated pair of source router/interface and destination router/interface. This option is useful if you need to specify a particular source interface to use for the ping. This group must be predefined by selecting **Grouping > Customized Advanced Group**.

For each ping or traceroute operation performed from the Ping and Traceroute buttons or from the **Tools > Diagnostics** menus, an entry is added to the Diagnostic Results Panel window, describing the operation and the time it was performed. Click on a row to display the results in the Output Panel window.

- For each entry, a green circle indicates a successful operation, a timer glass indicates an operation in progress, and a red circle indicates a failed operation.
- Right-clicking a row in the Diagnostic Results Panel window, as shown in Figure 133 on page 167, provides options to rerun a ping or traceroute, show the path for a traceroute, stop a continuous ping and turn off the chart view for continuous ping, or delete an entry.
- The buttons in the lower left of the window allow the user to save a single entry or all entries to a text file on the client machine, and to view details of an item in a separate window.

TIP: For diagnostic configuration settings, see “Configuration Revision Manager.”

See Also

- Configuration Revision Manager on page 84
- Running the CLI on page 162

Copyright © 2018, Juniper Networks, Inc.

Pinging from Device to Device

To measure connectivity, round-trip time (RTT), delay, and packet loss, you can use a ping operation from one device to another device, or from one device to multiple devices. The round-trip time (RTT) is the time from the moment the ping packet is sent to the time a reply is received. After a number of pings, the minimum, maximum, and average round-trip time, in milliseconds, is collected, as well as the standard deviation and percentage packet loss.

1. Select **Performance > Diagnostics > Diagnostic Manager**.

2. In the Diagnostic Manager window, click **Ping > Device from Device**.

   The Ping dialog box is displayed.

3. Select the source device and destination device from the lists.

4. (Optional) Select any of the following options:

   Use Management IP—Ping the destination device's management IP address, where the management IP address is the IP address defined in the router profile that is used by the IP/MPLS server to collect information from the router. This option is the default.

   Use Loopback IP—Ping the destination device's loopback IP address.

   Choose Source Interface—Choose the source interface from a list.

   Choose Destination IP—Type a specific IP address for the destination device.

5. (Optional) Click **Options** to change the diagnostic timeout from the default of 30 seconds.

6. Click **Run** to execute the ping request.

   The ping results are displayed in the Output Panel, as shown in Figure 133 on page 167.

See Also

- Running the CLI on page 162

Pinging Multiple Devices from a Device

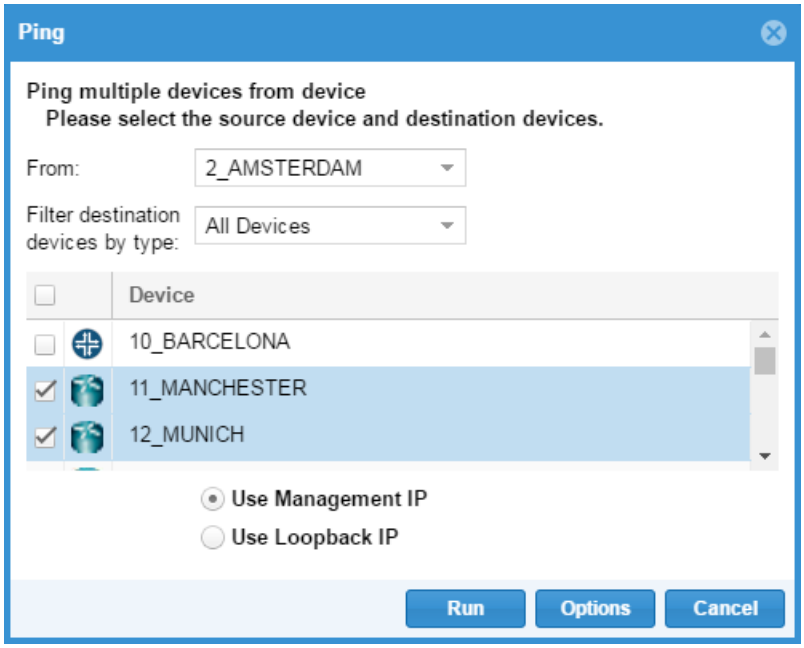
To perform a ping test from a single device to multiple devices:

1. Select **Performance > Diagnostics > Diagnostic Manager**.

2. In the Diagnostic Manager window, click **Ping > Multiple Devices from Device**.

   The Ping dialog box Figure 134 on page 170 is displayed, as shown in Figure 134 on page 170.

Figure 134: Ping Multiple Devices from Device



3. In the From list, select the source device to ping from.

4. (Optional) From the Filter destination devices by type list, select All Devices or a specific vendor.

5. Select the devices to ping from the source device, or select **Device** to ping all devices.

6. (Optional) Select any of the following options:

   Use Management IP—Ping the destination device's management IP address, where the management IP address is the IP address defined in the router profile that is used by the IP/MPLS server to collect information from the router. This option is the default.

   Use Loopback IP—Ping the destination device's loopback IP address.

7. (Optional) Click **Options** to change the diagnostic timeout from the default of 30 seconds.

8. Click **Run** to execute the ping request.

   The ping results are displayed in the Output Panel, as shown in Figure 133 on page 167.

See Also

- Running the CLI on page 162

Copyright © 2018, Juniper Networks, Inc.

Pinging Multiple Devices from a Server

To ping multiple devices from the server:

1. Select **Performance** > **Diagnostics** > **Diagnostic Manager**.

2. In the Diagnostic Manager window, click **Ping** > **Multiple Devices from Server**.

   The Ping dialog box is displayed.

3. (Optional) From the list, select All Devices or a specific vendor.

4. Select the devices to ping from the server or select **Device** to ping all devices.

5. (Optional) Select any of the following options:

   Use Management IP—Ping the destination device's management IP address, where the management IP address is the IP address defined in the router profile that is used by the IP/MPLS server to collect information from the router. This option is the default.

   Use Loopback IP—Ping the destination device's loopback IP address.

6. (Optional) Click **Options** to change the diagnostic timeout from the default of 30 seconds.

7. Click **Run** to execute the ping request.

   The ping results are displayed in a table in the Output Panel and indicate the round-trip time and packet loss information for each device being pinged. Table 28 on page 171 shows the items and descriptions.

Table 28: Multiple Ping Results

Item	Description
Target Name	The destination router.
Target IP	The destination IP address of the ping.
Min/Max/Avg/Stddev	The smallest, largest, and average round trip, respectively, in milliseconds, and the standard deviation.
Loss Percentage	The packet loss percentage experienced during the ping operation.

See Also

- Running the CLI on page 162

Performing a Continuous Ping

To chart the results of continuous pings between one router and another:

1. Select **Performance > Diagnostics > Diagnostic Manager**.

2. In the Diagnostic Manager window, click **Ping > Continuous Ping**.

   The Ping dialog box is displayed.

Running Traceroute from Device to Device

To use the traceroute utility to trace the route of an IP packet from one device to another:

1. Select **Performance > Diagnostics > Diagnostic Manager**.

2. In the Diagnostic Manager window, click **Traceroute > Device from Device**.

   TheTraceroute dialog box is displayed.

3. Select the source and destination devices from the lists.

4. (Optional) Select any of the following options:

   Use Management IP—Ping the destination device's management IP address, where the management IP address is the IP address defined in the router profile that is used by the IP/MPLS server to collect information from the router. This option is the default.

   Use Loopback IP—Ping the destination device's loopback IP address.

   Choose Source Interface—Choose the source interface from a list.

   Choose Destination IP—Type a specific IP address for the destination device.

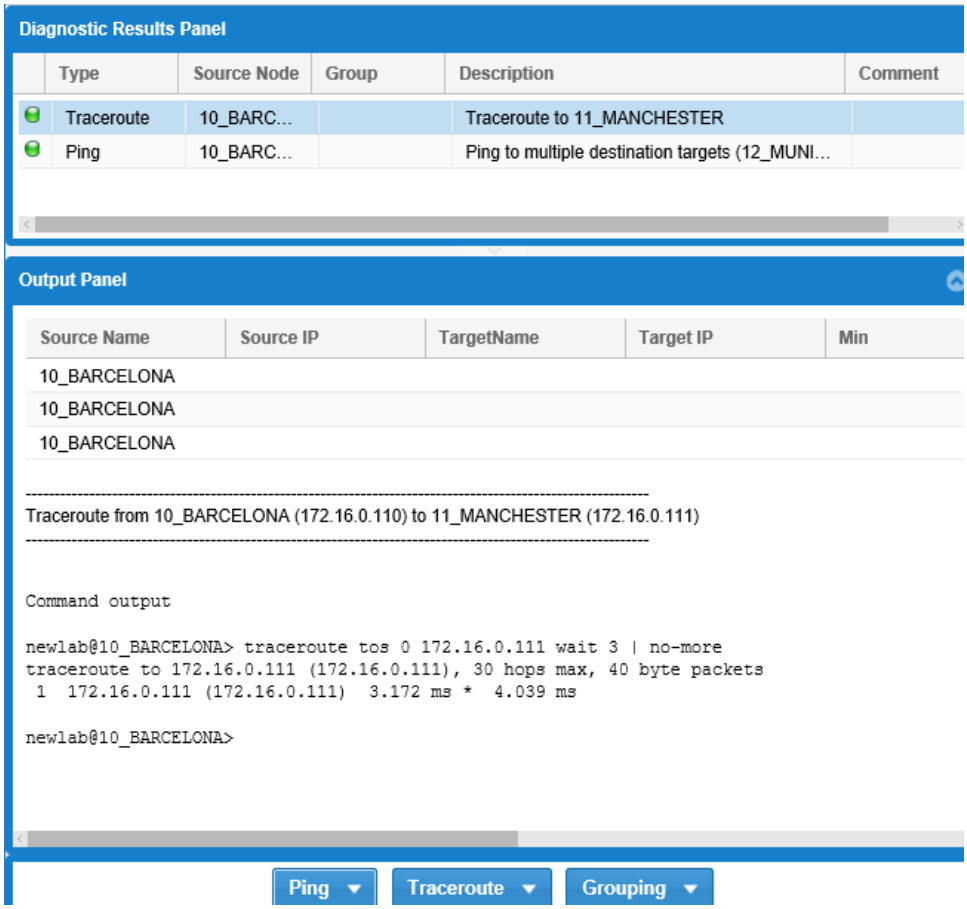
5. (Optional) Click **Options** to change the diagnostic timeout from the default of 30 seconds.

6. Click **Run** to start the trace.

   The trace results are displayed in the Output Panel. The results indicate the IP addresses at each hop of the path and the time it took for the IP trace packet to travel along this hop. Figure 128 on page 162 shows an example traceroute output result for device to device.

Copyright © 2018, Juniper Networks, Inc.

Figure 135: Example Traceroute Output for Device to Device



See Also

- Running the CLI on page 162

Running Traceroute on Multiple Devices from a Device

To perform a traceroute to multiple devices from one device:

1. Select **Performance > Diagnostics > Diagnostic Manager**.

2. In the Diagnostic Manager window, click **Traceroute > Multiple Devices from Device**.

   The Traceroute dialog box is displayed.

3. In the From list, select the source device to ping from.

4. (Optional) From Filter destination devices by type list, select All Devices or a specific vendor.

5. Select the devices to ping from the source device or select **Device** to ping all devices.

6. (Optional) Select any of the following options:

   Use Management IP—Ping the destination device's management IP address, where the management IP address is the IP address defined in the router profile that is used by the IP/MPLS server to collect information from the router. This option is the default.

   Use Loopback IP—Ping the destination device's loopback IP address.

7. (Optional) Click **Options** to change the diagnostic timeout from the default of 30 seconds.

8. Click **Run** to start the ping.

   The traceroute results are displayed in the Output Panel. The results indicate the IP addresses at each hop of the path and the time it took for the IP trace packet to travel along this hop. Figure 128 on page 162 shows an example of traceroute results.

See Also

- Running the CLI on page 162

Pinging and Traceroute for Device Groups

To perform a ping or traceroute within a group, between groups, or between a group and selected routers, a group of devices must first be created.

To create a group and then perform a ping or traceroute for that group:

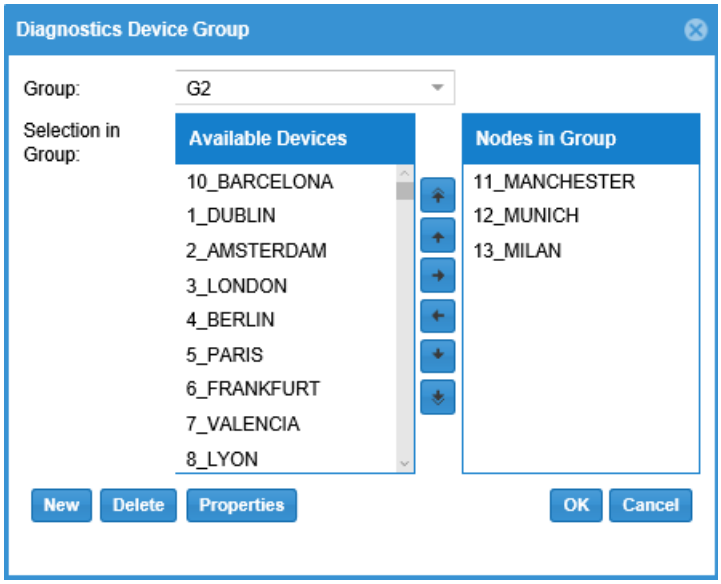
1. Select **Performance > Diagnostics > Diagnostic Manager**.

2. In the Diagnostic Manager window, click **Grouping > Device Group**.

   The Diagnostics Device Group window is displayed, as shown in Figure 136 on page 175.

Copyright © 2018, Juniper Networks, Inc.

Figure 136: Diagnostic Device Group Window



3. Click **New** and enter the name of the new group.

4. Select from the list of available devices in the left and click the arrow to move them into the group. Then click **OK**.

See Also

- Running the CLI on page 162

Pinging and Traceroute for a Customized Advanced Group

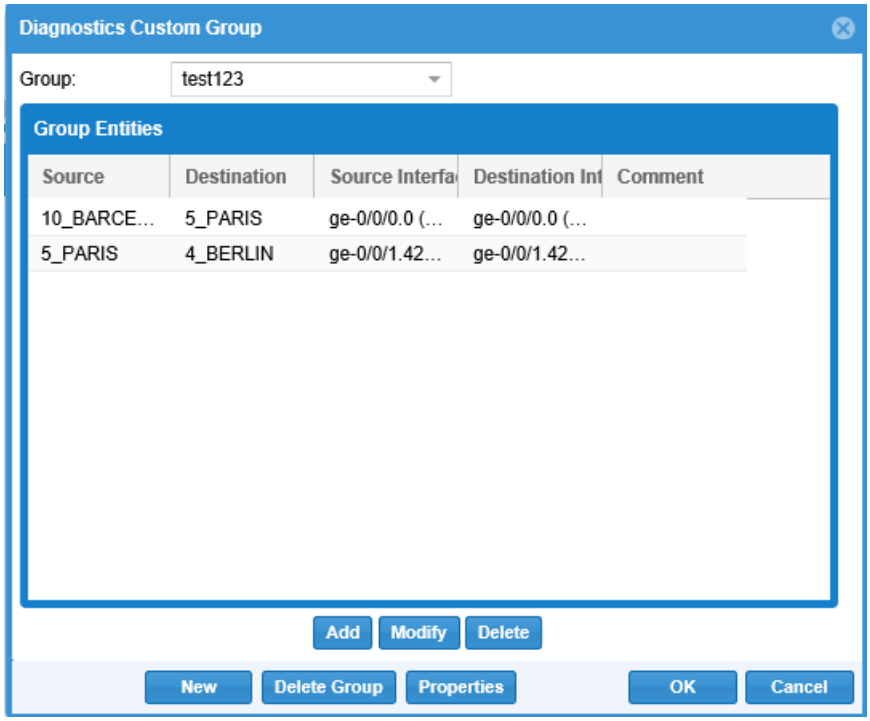
To use ping or traceroute and specify greater detail for the device groups, including the specific interface to use, create a customized advanced group:

1. Select **Performance > Diagnostics > Diagnostic Manager**.

2. In the Diagnostic Manager window, click **Grouping > Customized Advanced Group**.

3. The Diagnostics Custom Group window is displayed, as shown in Figure 137 on page 176.

Figure 137: Diagnostics Custom Group

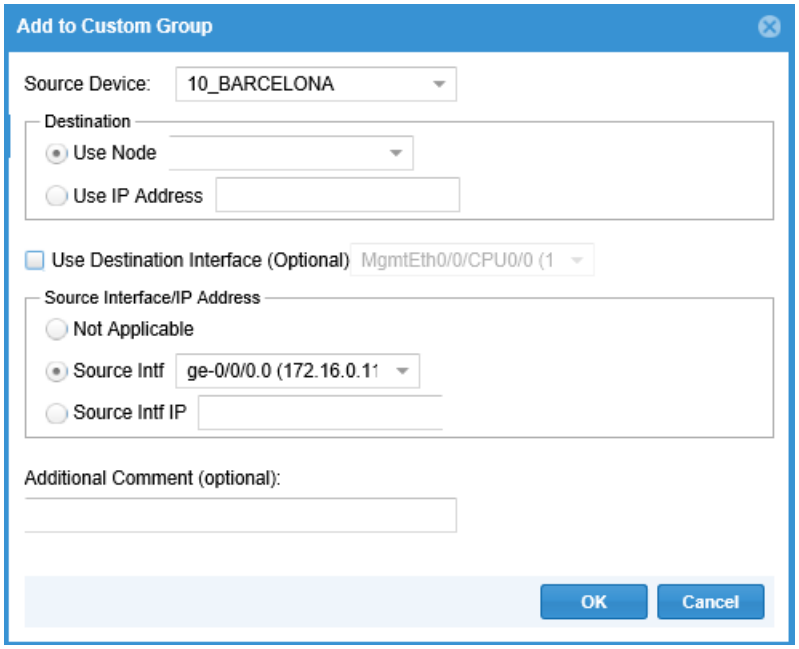


4. Click **New** and enter the name of the new group.

5. Select and existing group or click **Add** to display the Add to Custom Group window, as shown in Figure 138 on page 177.

Copyright © 2018, Juniper Networks, Inc.

Figure 138: Customized Advanced Group



6. From the Add to Custom Group window, add a new Source Device/Source Interface and Destination Device/Destination Interface pair, then click **OK**.

7. To execute the ping pairs, select **Ping > Ping by Customized Advanced Group** and select the group. The option to select either Management IP address or Loopback IP address is still available in case the destination device's interface was not specified in the Customized Advanced Group.

   One entry is created for each source/destination pair from the Customized Advanced Group.

Traffic Collection Manager

The Traffic Collection Manager enables you to manage traffic data collectors and configure the type of traffic data that IP/MPLSView collects from the devices in your network. By viewing the collected information in various ways in the Traffic Collection Manager, you can monitor your network interface and tunnel traffic.

You can access the Traffic Collection Manager from either the Web interface or Java client interface in IP/MPLSView. The Web version of the Task Manager provides essentially the same features as the Java client version, with only minor variations in the appearance of the GUI.

To access the Traffic Collection Manager from the IP/MPLSView Web interface, select **Performance > Traffic Collection Manager** from the window's main menu. The Web version of the Traffic Collection Manager enables you to perform the following tasks:

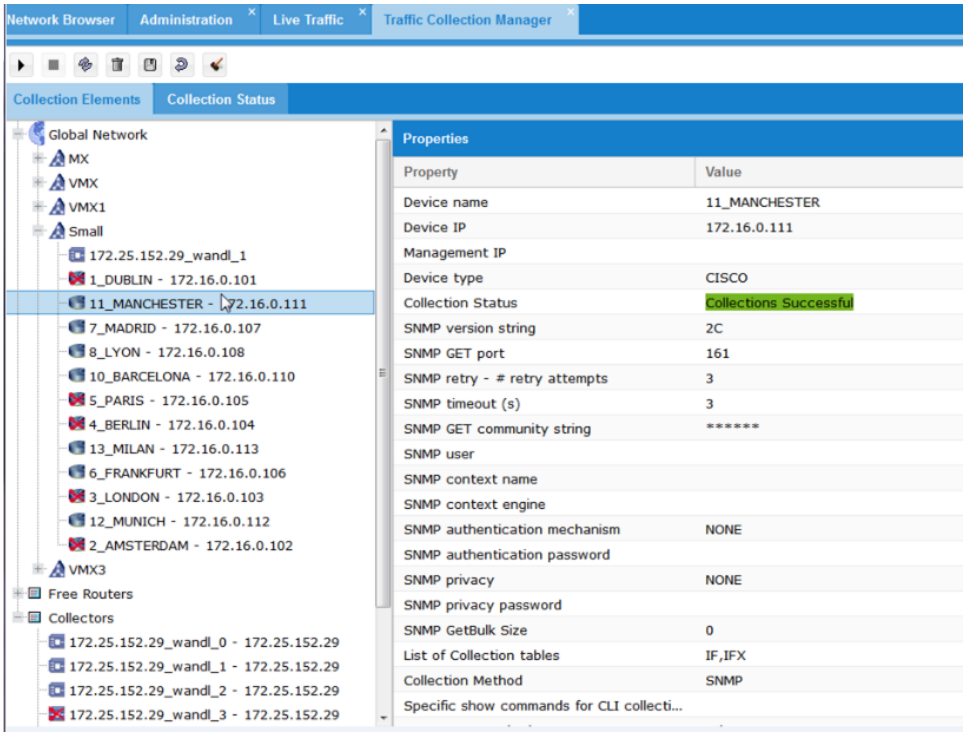
- Create, modify, and delete router groups from which data is collected.
- Assign devices and traffic data collectors to router groups.
- Select the collection tables that you want to use for data collection.
- Modify device profile properties for data collection.
- Manage the collection status.
- Test network connectivity to one or more devices in a router group.

NOTE: **To configure collection settings for the Master Collection Panel and the Collection Manager, you must access and use Traffic Collection Manager from the Java client interface. All other tasks are supported in both the Web version and Java version of the Traffic Collection Manager.**

In the sample Traffic Collection Manager window in Figure 139 on page 179, the left pane of the Collection Elements tab shows a router group named Small to which traffic data collector 172.25.152.29_wandl_1 is assigned. The right pane displays the properties for the device named 11_MANCHESTER - 172.16.0.11, which belongs to the Small router group.

Copyright © 2018, Juniper Networks, Inc.

Figure 139: Traffic Collection Manager and Router Groups



To enable collection of IPv6 interface traffic, click List of Collection tables and select **IPV6** in the List of Collection Tables window that appears, as shown in Figure 140 on page 180. When you enable IPv6 interface traffic collection, IP/MPLSView polls various object identifiers (OIDs) in the **ipv6IfTable** (to retrieve the index, description, administrative status, and operating status), **ipv6StatsEntry** table, and the Juniper Networks **jnxipv6IfStatsEntry** table. You can display the collection results by viewing the IPv6 Interface Traffic Report.

Figure 140: Choose Collection Tables

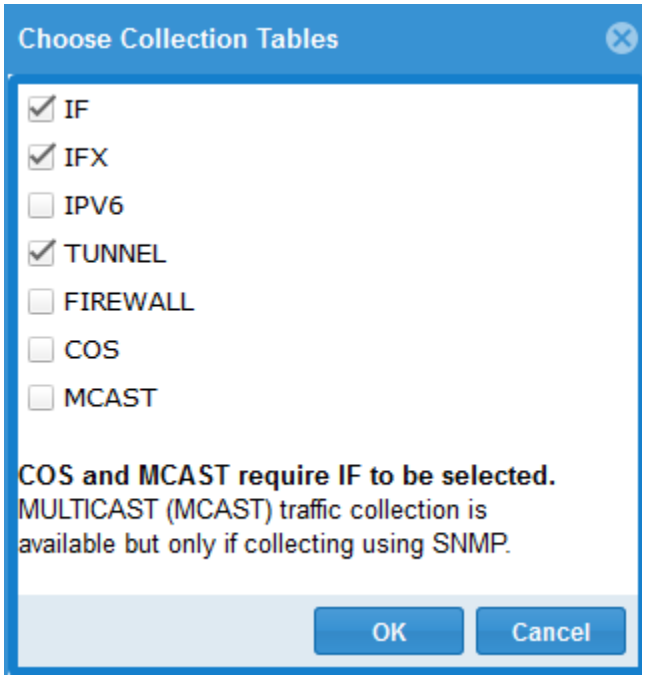


Figure 141 on page 180 displays the collection status in the Traffic Collection Manager. After traffic collection has started, you can select the Collection Status tab to view and monitor collection events. The display includes any errors, warnings, and updates that may occur.

Figure 141: Traffic Collection Manager Collection Status

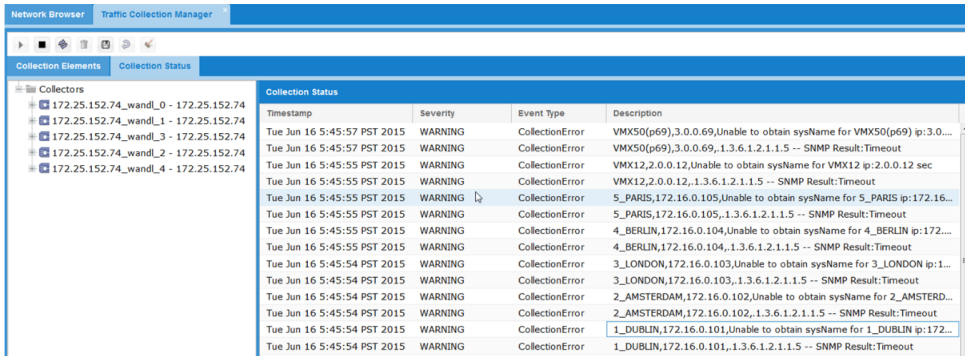
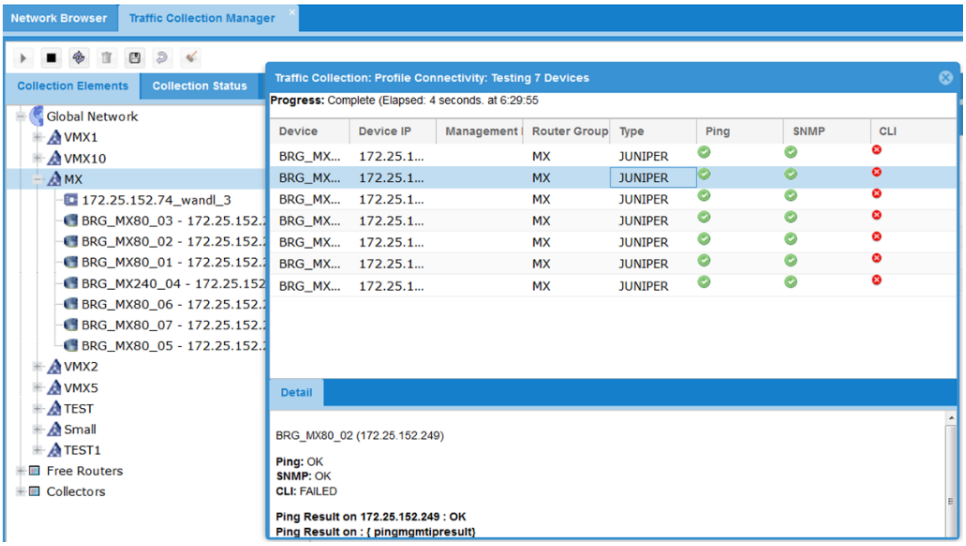


Figure 142 on page 181 displays the profile connectivity test for the seven devices that belong to the MX router group. The connectivity test runs Ping, SNMP, and CLI tests on the devices to verify reachability, SNMP configuration, and CLI login access, respectively. You can run the connectivity test only for devices that belong to a complete router group to which a traffic data collector is assigned.

Copyright © 2018, Juniper Networks, Inc.

Figure 142: Traffic Collection Manager Profile Connectivity Test



For more information about traffic collection, see the *IP/MPLSView Java-Based Management and Monitoring Guide*.

Viewing Device Performance

The Device Performance feature enables you to view device reports on system uptime, CPU temperature, CPU usage, CPU load, and memory usage. To prepare this data, schedule the Device SNMP Collection task, as described in *Device SNMP Collection*.

To display statistics information in the Device Performance report about interface modules (also known as line cards) installed in Juniper Networks devices in your network, select the **Collect Line Card Information (Juniper Only)** option when you configure the parameters for the Device SNMP Collection task.

To view the CPU load report and chart:

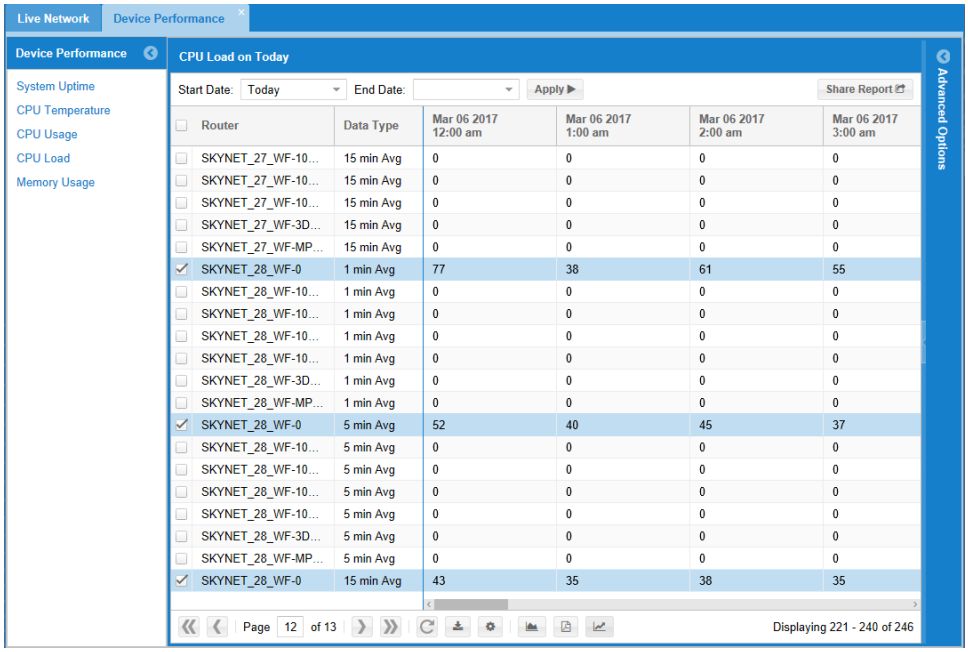
1. Select **Performance > Device Performance**.

   The Device Performance window is displayed. The CPU load averages are shown in increments of 1 minute, 5 minutes, and 15 minutes.

2. In the Device Performance pane, select **CPU Load**.

   The CPU Load report is displayed, as shown in Figure 143 on page 182. The default display is for the current date.

Figure 143: CPU Load Report



Router	Data Type	Mar 06 2017 12:00 am	Mar 06 2017 1:00 am	Mar 06 2017 2:00 am	Mar 06 2017 3:00 am
SKYNET_27_WF-10...	15 min Avg	0	0	0	0
SKYNET_27_WF-10...	15 min Avg	0	0	0	0
SKYNET_27_WF-10...	15 min Avg	0	0	0	0
SKYNET_27_WF-3D...	15 min Avg	0	0	0	0
SKYNET_27_WF-MP...	15 min Avg	0	0	0	0
SKYNET_28_WF-0	1 min Avg	77	38	61	55
SKYNET_28_WF-10...	1 min Avg	0	0	0	0
SKYNET_28_WF-10...	1 min Avg	0	0	0	0
SKYNET_28_WF-10...	1 min Avg	0	0	0	0
SKYNET_28_WF-10...	1 min Avg	0	0	0	0
SKYNET_28_WF-3D...	1 min Avg	0	0	0	0
SKYNET_28_WF-MP...	1 min Avg	0	0	0	0
SKYNET_28_WF-0	5 min Avg	52	40	45	37
SKYNET_28_WF-10...	5 min Avg	0	0	0	0
SKYNET_28_WF-10...	5 min Avg	0	0	0	0
SKYNET_28_WF-10...	5 min Avg	0	0	0	0
SKYNET_28_WF-10...	5 min Avg	0	0	0	0
SKYNET_28_WF-3D...	5 min Avg	0	0	0	0
SKYNET_28_WF-MP...	5 min Avg	0	0	0	0
SKYNET_28_WF-0	15 min Avg	43	35	38	35

3. Select devices in the Router column, then click the chart icon to show the CPU load for the selected devices on the specified dates in a chart. See Figure 144 on page 183.

Copyright © 2018, Juniper Networks, Inc.

Figure 144: CPU Load Chart

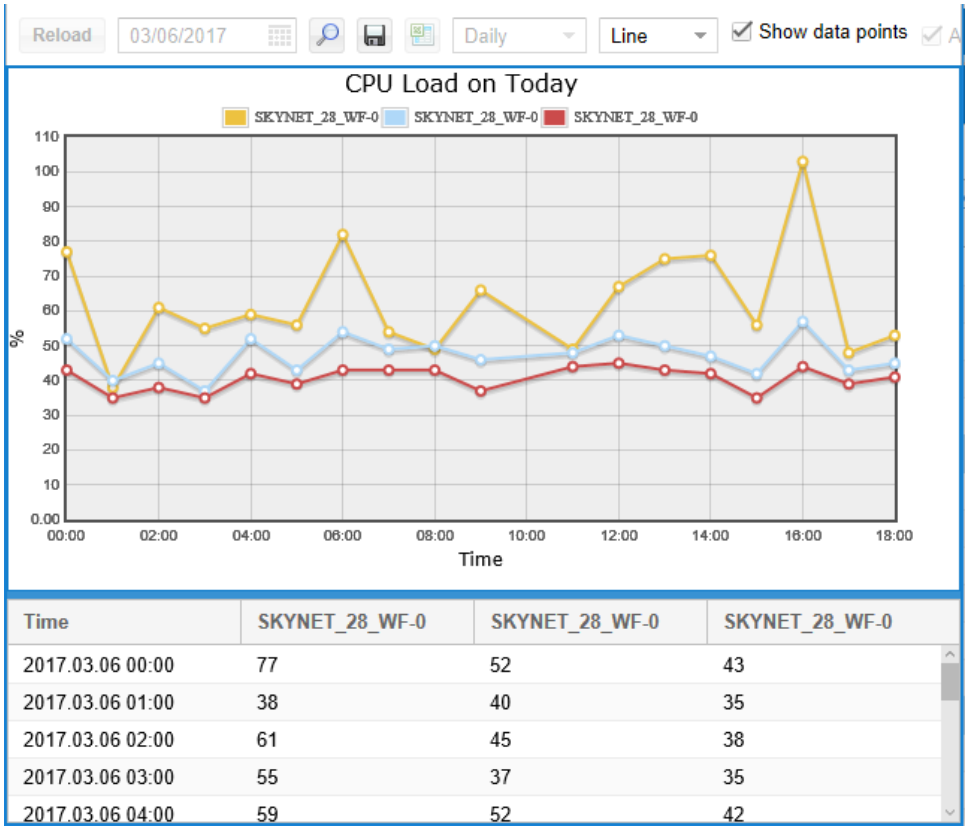


Figure 145 on page 183 shows a System Uptime report.

Figure 145: System Uptime Report

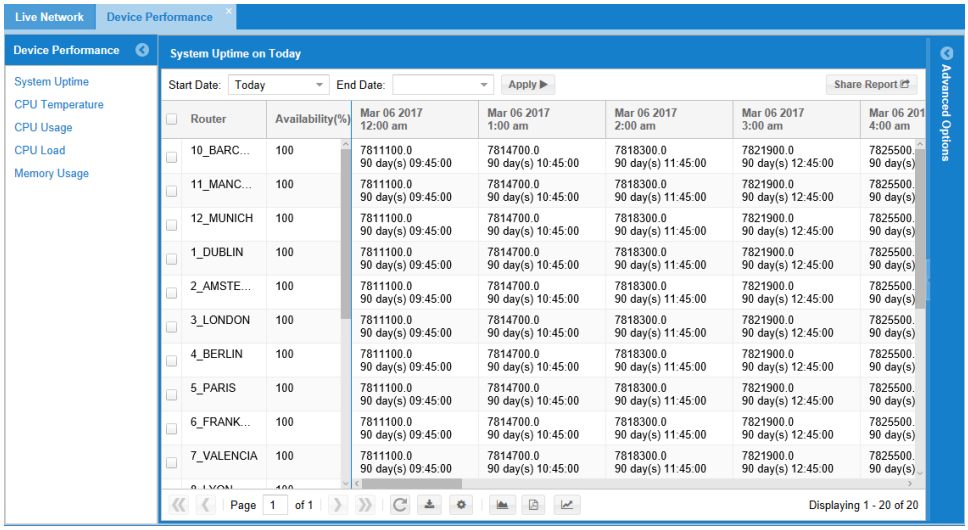
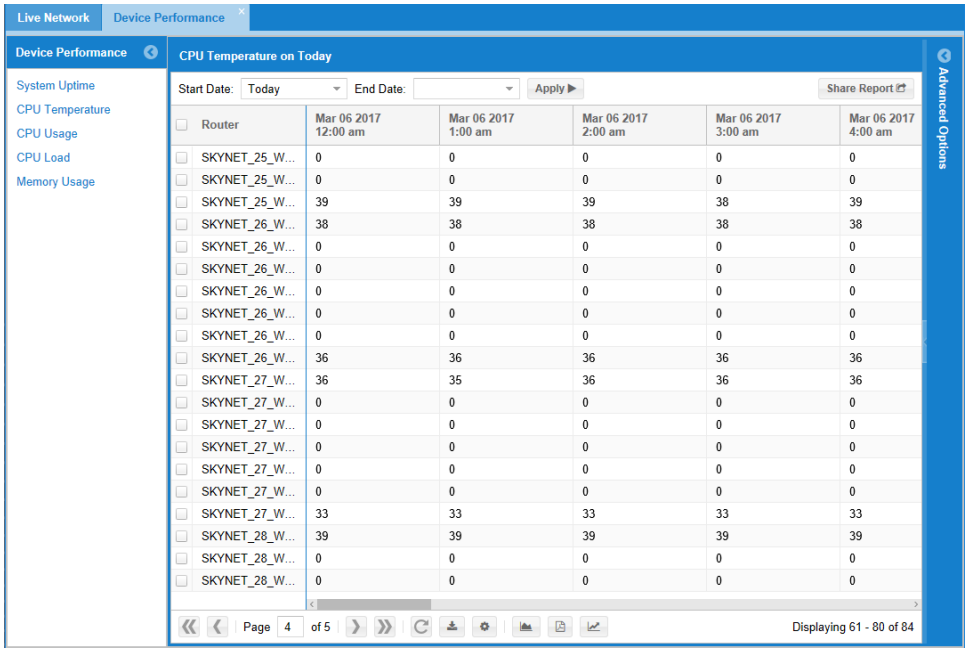


Figure 146 on page 184 shows a CPU Temperature report.

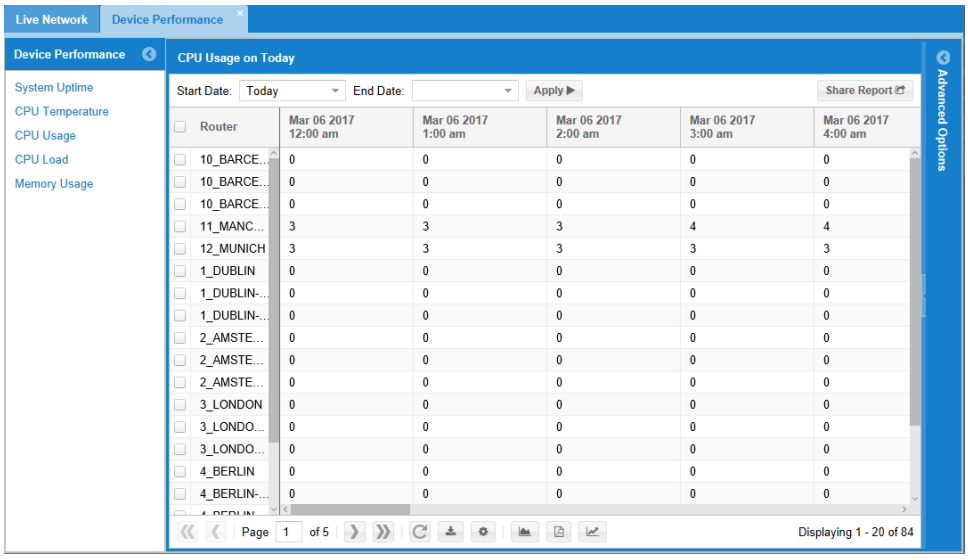
Figure 146: CPU Temperature Report



Router	Mar 06 2017 12:00 am	Mar 06 2017 1:00 am	Mar 06 2017 2:00 am	Mar 06 2017 3:00 am	Mar 06 2017 4:00 am
SKYNET_25_W...	0	0	0	0	0
SKYNET_25_W...	0	0	0	0	0
SKYNET_25_W...	39	39	39	38	39
SKYNET_26_W...	38	38	38	38	38
SKYNET_26_W...	0	0	0	0	0
SKYNET_26_W...	0	0	0	0	0
SKYNET_26_W...	0	0	0	0	0
SKYNET_26_W...	0	0	0	0	0
SKYNET_26_W...	0	0	0	0	0
SKYNET_26_W...	36	36	36	36	36
SKYNET_27_W...	36	35	36	36	36
SKYNET_27_W...	0	0	0	0	0
SKYNET_27_W...	0	0	0	0	0
SKYNET_27_W...	0	0	0	0	0
SKYNET_27_W...	0	0	0	0	0
SKYNET_27_W...	0	0	0	0	0
SKYNET_27_W...	33	33	33	33	33
SKYNET_28_W...	39	39	39	39	39
SKYNET_28_W...	0	0	0	0	0
SKYNET_28_W...	0	0	0	0	0

Figure 147 on page 184 shows a CPU Usage report.

Figure 147: CPU Usage Report

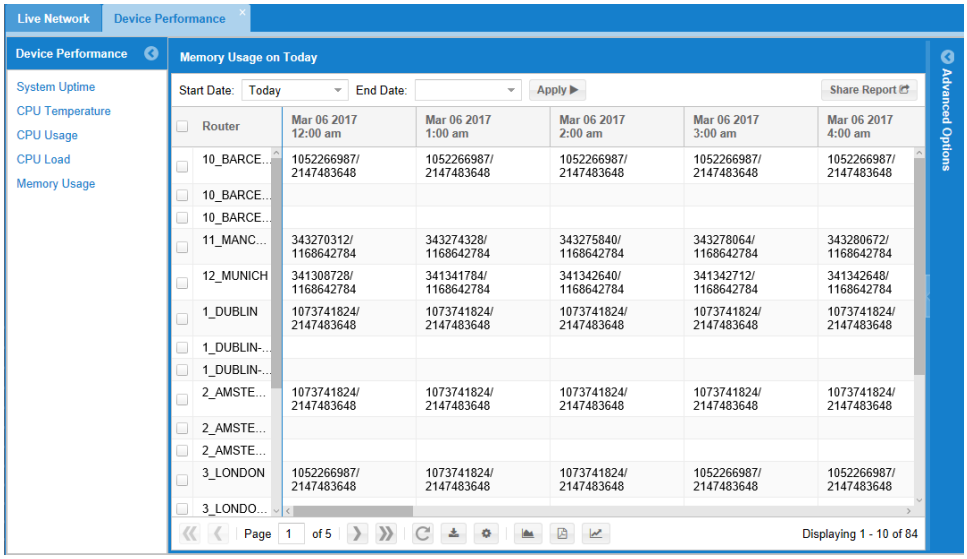


Router	Mar 06 2017 12:00 am	Mar 06 2017 1:00 am	Mar 06 2017 2:00 am	Mar 06 2017 3:00 am	Mar 06 2017 4:00 am
10_BARCE...	0	0	0	0	0
10_BARCE...	0	0	0	0	0
10_BARCE...	0	0	0	0	0
11_MANC...	3	3	3	4	4
12_MUNICH	3	3	3	3	3
1_DUBLIN	0	0	0	0	0
1_DUBLIN-...	0	0	0	0	0
1_DUBLIN-...	0	0	0	0	0
2_AMSTE...	0	0	0	0	0
2_AMSTE...	0	0	0	0	0
2_AMSTE...	0	0	0	0	0
3_LONDON	0	0	0	0	0
3_LONDO...	0	0	0	0	0
3_LONDO...	0	0	0	0	0
4_BERLIN	0	0	0	0	0
4_BERLIN-...	0	0	0	0	0

Figure 148 on page 185 shows a Memory Usage report.

Copyright © 2018, Juniper Networks, Inc.

Figure 148: Memory Usage Report



Related Documentation

- Viewing Network Performance on page 185

Viewing Network Performance

The network performance menu enables you to view network reports on ping, LSP ping, SLA, and link latency. To prepare this data, schedule the Device Ping Collection, LSP Ping Collection, Device SLA Collection, and Link Latency Collection tasks, respectively.

Figure 149 on page 185 shows a ping report.

Figure 149: Ping Report

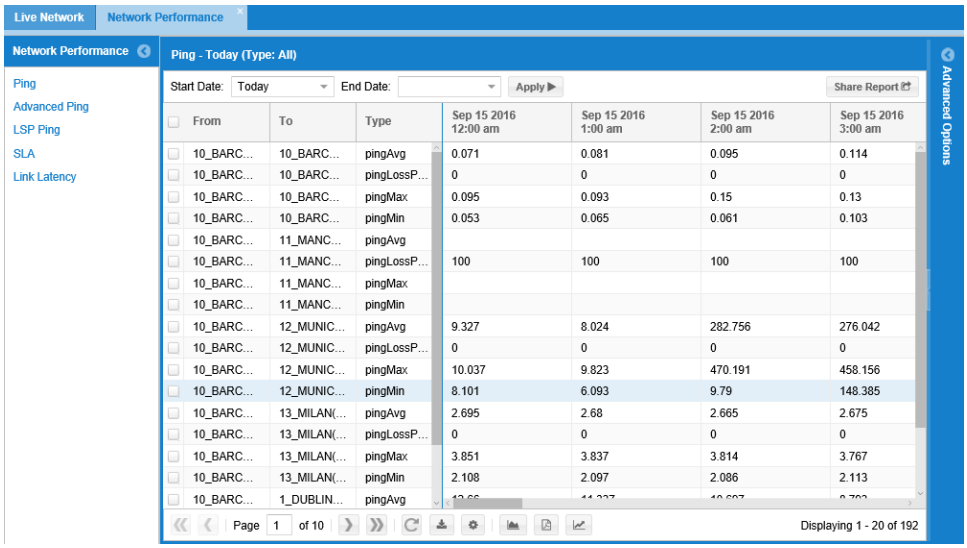


Figure 150 on page 186 shows a LSP ping report.

Figure 150: LSP Ping Report

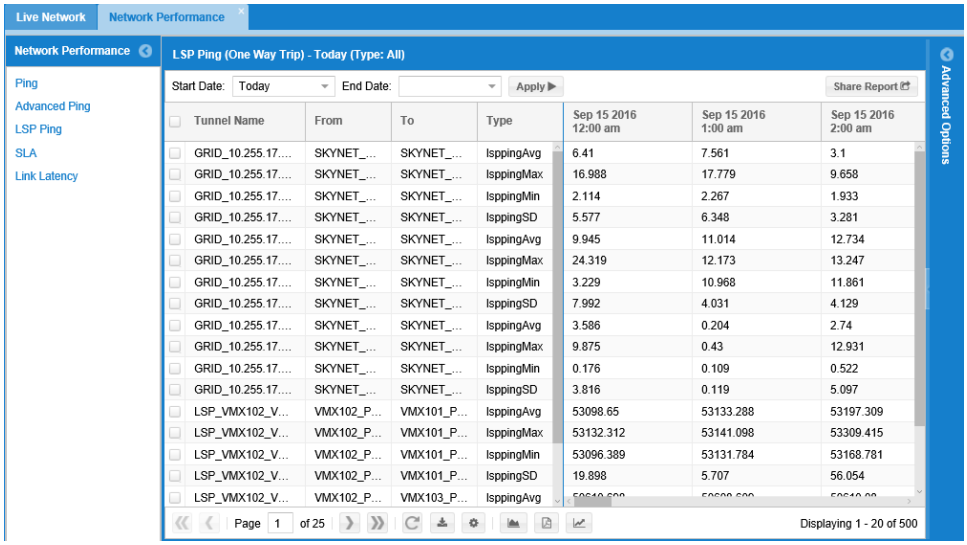


Figure 151 on page 186 shows a SLA report.

Figure 151: SLA Report

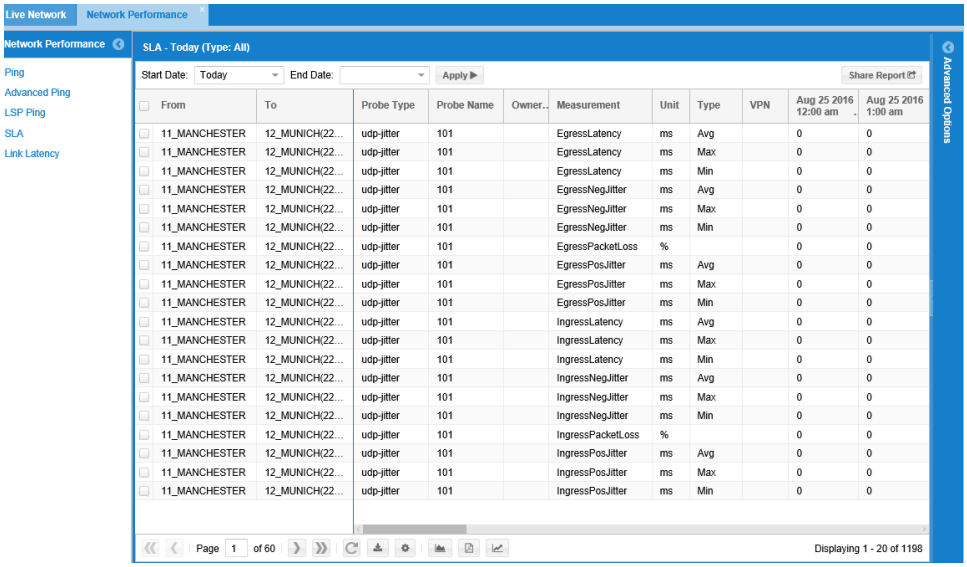
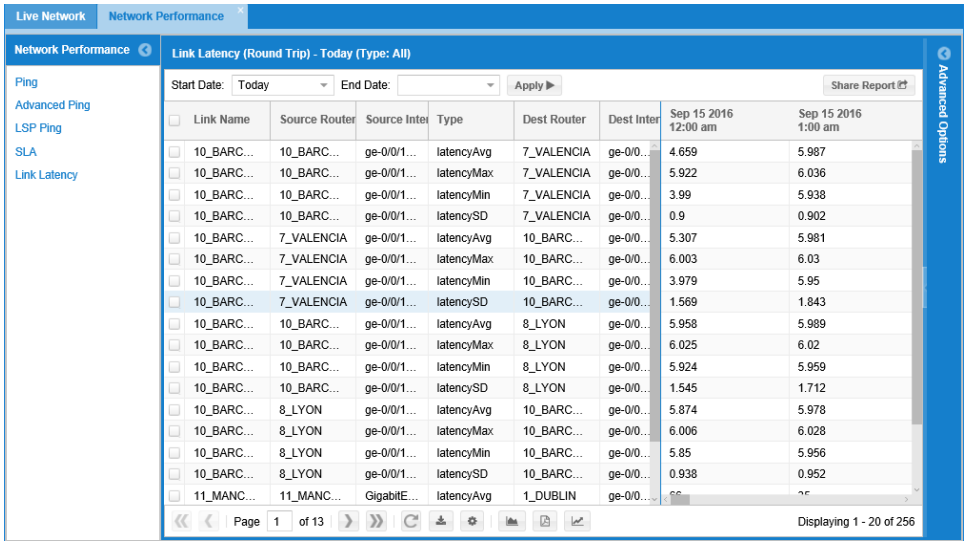


Figure 152 on page 187 shows a link latency report.

Copyright © 2018, Juniper Networks, Inc.

Figure 152: Link Latency Report



Viewing Miscellaneous Reports and Charts

This section describes the following miscellaneous and vendor-specific reports and charts related to performance and traffic data:

- **Network Performance Data Report from Task Manager:** To view this report, see *Network Performance Data Report*.
- **Aggregated Traffic Reports:** To view this report, run the Aggregated Traffic Report task from the Task Manager. The resulting report is saved to **/u/wandl/data/task_reportsummary/** and can be viewed from this Web menu. You should wait at least one day from the beginning of traffic collection. There is a cron job that runs once daily to perform the aggregation.
- **LDP Traffic Summary Report:** To view this report, run the LDP Traffic Collection task (for Juniper only) from the Task Manager, and specify the same LDP Traffic Directory here that was used when scheduling the task.
- **LSP Tunnel Traffic Summary Report:** To view this report, run the LSP Tunnel Traffic Collection task (for Juniper only) from the Task Manager, and specify the same LSP Traffic Directory here that was used when scheduling the task.
- **User Defined Group Traffic Summary Report (Hourly Aggregation):** Given the router groups defined through the IP/MPLSView client, this report provides total in and out traffic for the interfaces in a group aggregated by hourly intervals. Click **Show** to display the Group hierarchy. Click **Report** to display the report. Only the Web Admin can add or remove reports. The default topology group is from the file **/u/wandl/data/.network/group.x**.
- **Group / Device / Interface Traffic Summary Reports (Live Traffic):** To view this report, create groups from the IP/MPLSView client. This report provides traffic summary reports organized by the groupings.

Related Documentation

- Live Traffic on page 140
- Network Performance Data Chart Report on page 188

Network Performance Data Chart Report

How to Prepare the Data

A report group is a group containing the router interfaces that will be reported on in the resulting traffic report. From the Web, create report groups from **Admin > Report Groups**. Select the created report group to add the desired router interface(s) one by one.

After creating the report group, schedule the Network Performance Data Report task as described in *Network Performance Data Report*. On the Report Parameters tab, include at least the format Data Chart and a report title. On the Report Attributes tab, specify the report group defined from the Web, and select the desired attributes to report on, for example, the Egress utilization. If you have not yet collected one days' worth of traffic, you will not see data from a query of the last day, for example, Query data over the last 1 Day. Instead, you can query over the last few hours, for example, Query data over the last 5 Hours. Alternatively, you can specify a specific date/time range by using the option Specify the report query date range.

Viewing the Reports

Once the report is created, select the title of the report and then select the date/time that it was generated. Reports are provided for CPU, Memory, Ingress and Egress Traffic, and Error Count. After selecting the report name, click on the link corresponding to the day that you would like to view:

- **Network_Data_Report:** This report will provide CPU and memory information, one chart per device.
- **Device:** This report will provide CPU and memory information, one chart per device.

Network Performance PDF Chart Report

This is similar to the Network Performance Data Chart Report above, except that the chart is provided in PDF format. The difference during setup is that the format PDF Chart should be selected as the output from the Report Parameters tab of the Network Performance Data Report task.

Copyright © 2018, Juniper Networks, Inc.

Archived Reports

You can use the Archived Reports feature from the IP/MPLSView Web interface to display preprocessed traffic reports that you can view on a daily, weekly, monthly, or yearly basis. Because the reports are generated from preprocessed aggregated traffic data stored in the database on a daily, weekly, monthly, or yearly basis, you can perform report queries more quickly to retrieve the data.

The following archived reports are available:

Traffic reports—Archived Interface Traffic or Archived Tunnel Traffic.

Device performance reports—Archived System Uptime, Archived CPU Temperature, Archived CPU Usage, or Archived Memory Usage.

Network performance reports—Archived Ping, Archived Advanced Ping, Archived LSP Ping, Archived SLA, or Archived Link Latency.

The daily and weekly reports use hourly aggregated data. The monthly and yearly reports use daily aggregated data. You can specify display options for the average, maximum (max), or 80th, 90th, 95th, and 99th percentiles. IP/MPLSView prepares the data every day at 11:30 AM by running the **/u/wandl/bin/genAggTrafDB.sh** script.

To generate and display archived reports from the Web interface:

1. (Optional) Configure the IP/MPLSView server to set the maximum number of days to store performance management data.

   By default, you can store data collected from live traffic, aggregated traffic, and archived traffic for a maximum of 35 days. In most cases, using the default value should be adequate for your data storage needs, However, you can increase or decrease this value according to the available storage space in your network and how long you need to retain the historical data.

   If necessary, you can set a nondefault value for the maximum data storage capacity in either of the following ways:

   - During the IP/MPLSView installation, change the default value (35) for Maximum Traffic Capacity in Days in the installation script.

     ```
     Server Configuration Settings:
     (A) Overall Settings
     (B) IP Address
     (C) Memory Settings
     (D) Port Settings (Server to Client)
     (E) Port Settings (Advanced)
     (F) Online Performance Management Settings
     (G) Online Fault Management Settings
     (H) Advanced Configuration

     Please select a number to modify.
     [<CR>=accept, q=quit]:F

     (F) Online Performance Management Settings
     ```

```
Aggregation Settings:
   1.) Maximum Traffic Capacity in Days......:35
```

- After the IP/MPLSView installation, change the default value by running the **/u/wandl/bin/changeconfig.sh** script.

2. Collect the data to be generated for the archived reports by running the appropriate collection task from Task Manager.

   Table 29 on page 190 lists the collection tasks you need to run to provide data for the associated archived reports. For example, to generate data for the Archived Ping report, you must first schedule the Device Ping Collection task from the Task Manager to run on a recurring basis.

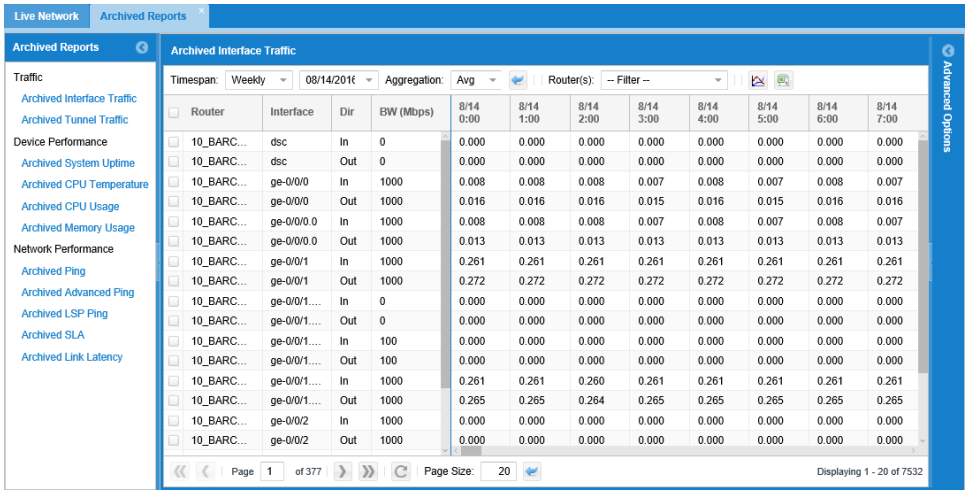
Table 29: IP/MPLSView Collection Tasks and Associated Archived Reports

Collection Task	Associated Archived Reports
Traffic Collection	Archived Interface Traffic, Archived Tunnel Traffic
Device SNMP Collection	Archived System Uptime, Archived CPU Temperature, Archived CPU Usage, Archived Memory Usage
Device Ping Collection	Archived Ping
Advanced Ping Collection	Archived Advanced Ping
LSP Ping Collection	Archived LSP Ping
SLA Collection	Archived SLA
Link Latency Collection	Archived Link Latency

3. Select **Performance > Archived Reports** from the main menu to access the Archived Reports.

Copyright © 2018, Juniper Networks, Inc.

Figure 153: Example of Archived Reports



Router	Interface	Dir	BW (Mbps)	8/14 0:00	8/14 1:00	8/14 2:00	8/14 3:00	8/14 4:00	8/14 5:00	8/14 6:00	8/14 7:00
10_BARC...	dsc	In	0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
10_BARC...	dsc	Out	0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
10_BARC...	ge-0/0/0	In	1000	0.008	0.008	0.008	0.007	0.008	0.007	0.008	0.007
10_BARC...	ge-0/0/0	Out	1000	0.016	0.016	0.016	0.015	0.016	0.015	0.016	0.016
10_BARC...	ge-0/0/0.0	In	1000	0.008	0.008	0.008	0.007	0.008	0.007	0.008	0.007
10_BARC...	ge-0/0/0.0	Out	1000	0.013	0.013	0.013	0.013	0.013	0.013	0.013	0.013
10_BARC...	ge-0/0/1	In	1000	0.261	0.261	0.261	0.261	0.261	0.261	0.261	0.261
10_BARC...	ge-0/0/1	Out	1000	0.272	0.272	0.272	0.272	0.272	0.272	0.272	0.272
10_BARC...	ge-0/0/1....	In	0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
10_BARC...	ge-0/0/1....	Out	0	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
10_BARC...	ge-0/0/1....	In	100	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
10_BARC...	ge-0/0/1....	Out	100	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
10_BARC...	ge-0/0/1....	In	1000	0.261	0.261	0.260	0.261	0.261	0.261	0.261	0.261
10_BARC...	ge-0/0/1....	Out	1000	0.265	0.265	0.264	0.265	0.265	0.265	0.265	0.265
10_BARC...	ge-0/0/2	In	1000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
10_BARC...	ge-0/0/2	Out	1000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

Related Documentation

- Live Traffic on page 140
- Aggregated Traffic Reports on page 147
- Monitoring Real-Time Traffic and Device Performance on page 152

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 8

Admin

- Admin on page 193

Admin

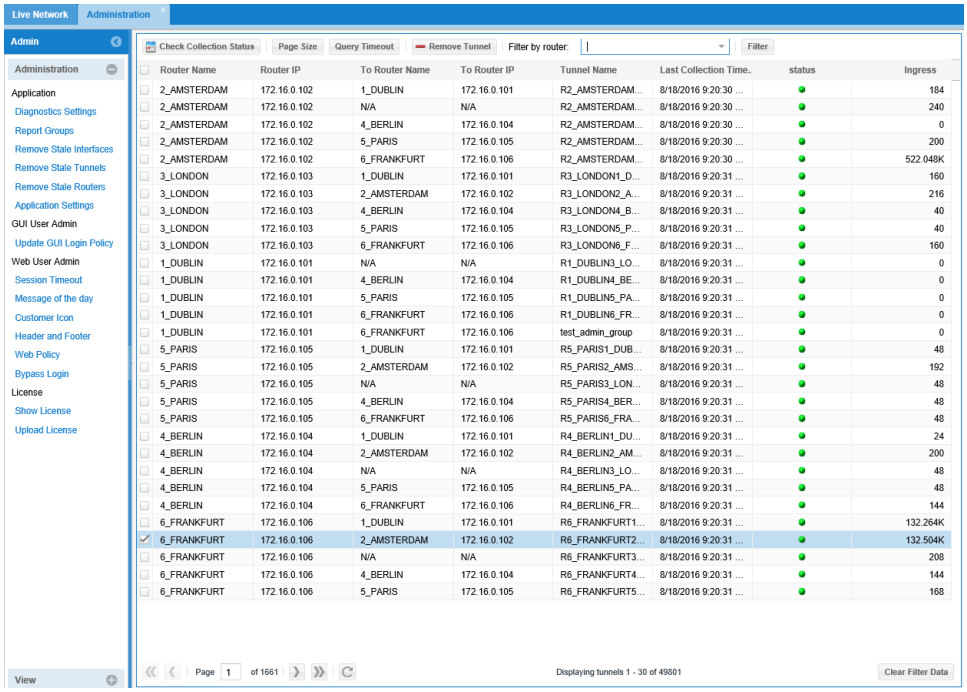
- Understanding the Admin Menu on page 193
- Duplicating or Renaming an Existing Report Group on page 194
- Updating the GUI Login Policy on page 195
- Displaying Current Licenses on page 196
- Uploading a License on page 196
- Viewing Vendor Icons on page 197
- Viewing the User Activity Log on page 197

Understanding the Admin Menu

The Admin menu contains administrative settings for the Web, Web applications, Web user accounts, and monitoring activities on the server. Web settings include session timeout, message of the day, and Web policies. Web applications include the diagnostic tools, ping parameters, and traceroute parameters. Web user accounts include user access, groups, and password reset. Server monitoring includes viewing logs, login history, memory, CPU, and IP/MPLSView system processes.

When you select the Admin menu, the Administration window is displayed. Among the sub-options under Application, you can remove stale interfaces, stale tunnels, and stale routers from your topology. For example, Figure 154 on page 194 illustrates how to use the Adminstration window to remove a stale tunnel.

Figure 154: Administration Window for Removing Stale Tunnels



Router Name	Router IP	To Router Name	To Router IP	Tunnel Name	Last Collection Time.	status	Ingress
2_AMSTERDAM	172.16.0.102	1_DUBLIN	172.16.0.101	R2_AMSTERDAM...	8/18/2016 9:20:30 ...		184
2_AMSTERDAM	172.16.0.102	N/A	N/A	R2_AMSTERDAM...	8/18/2016 9:20:30 ...		240
2_AMSTERDAM	172.16.0.102	4_BERLIN	172.16.0.104	R2_AMSTERDAM...	8/18/2016 9:20:30 ...		0
2_AMSTERDAM	172.16.0.102	5_PARIS	172.16.0.105	R2_AMSTERDAM...	8/18/2016 9:20:30 ...		200
2_AMSTERDAM	172.16.0.102	6_FRANKFURT	172.16.0.106	R2_AMSTERDAM...	8/18/2016 9:20:30 ...		522.048K
3_LONDON	172.16.0.103	1_DUBLIN	172.16.0.101	R3_LONDON1_D...	8/18/2016 9:20:31 ...		160
3_LONDON	172.16.0.103	2_AMSTERDAM	172.16.0.102	R3_LONDON2_A...	8/18/2016 9:20:31 ...		216
3_LONDON	172.16.0.103	4_BERLIN	172.16.0.104	R3_LONDON4_B...	8/18/2016 9:20:31 ...		40
3_LONDON	172.16.0.103	5_PARIS	172.16.0.105	R3_LONDON5_P...	8/18/2016 9:20:31 ...		40
3_LONDON	172.16.0.103	6_FRANKFURT	172.16.0.106	R3_LONDON6_F...	8/18/2016 9:20:31 ...		160
1_DUBLIN	172.16.0.101	N/A	N/A	R1_DUBLIN3_LO...	8/18/2016 9:20:31 ...		0
1_DUBLIN	172.16.0.101	4_BERLIN	172.16.0.104	R1_DUBLIN4_BE...	8/18/2016 9:20:31 ...		0
1_DUBLIN	172.16.0.101	5_PARIS	172.16.0.105	R1_DUBLIN5_PA...	8/18/2016 9:20:31 ...		0
1_DUBLIN	172.16.0.101	6_FRANKFURT	172.16.0.106	R1_DUBLIN6_FR...	8/18/2016 9:20:31 ...		0
1_DUBLIN	172.16.0.101	6_FRANKFURT	172.16.0.106	test_admin_group	8/18/2016 9:20:31 ...		0
5_PARIS	172.16.0.105	1_DUBLIN	172.16.0.101	R5_PARIS1_DUB...	8/18/2016 9:20:31 ...		48
5_PARIS	172.16.0.105	2_AMSTERDAM	172.16.0.102	R5_PARIS2_AMS...	8/18/2016 9:20:31 ...		192
5_PARIS	172.16.0.105	N/A	N/A	R5_PARIS3_LON...	8/18/2016 9:20:31 ...		48
5_PARIS	172.16.0.105	4_BERLIN	172.16.0.104	R5_PARIS4_BER...	8/18/2016 9:20:31 ...		48
5_PARIS	172.16.0.105	6_FRANKFURT	172.16.0.106	R5_PARIS6_FRA...	8/18/2016 9:20:31 ...		48
4_BERLIN	172.16.0.104	1_DUBLIN	172.16.0.101	R4_BERLIN1_DU...	8/18/2016 9:20:31 ...		24
4_BERLIN	172.16.0.104	2_AMSTERDAM	172.16.0.102	R4_BERLIN2_AM...	8/18/2016 9:20:31 ...		200
4_BERLIN	172.16.0.104	N/A	N/A	R4_BERLIN3_LO...	8/18/2016 9:20:31 ...		48
4_BERLIN	172.16.0.104	5_PARIS	172.16.0.105	R4_BERLIN5_PA...	8/18/2016 9:20:31 ...		48
4_BERLIN	172.16.0.104	6_FRANKFURT	172.16.0.106	R4_BERLIN6_FR...	8/18/2016 9:20:31 ...		144
6_FRANKFURT	172.16.0.106	1_DUBLIN	172.16.0.101	R6_FRANKFURT1...	8/18/2016 9:20:31 ...		132.264K
6_FRANKFURT	172.16.0.106	2_AMSTERDAM	172.16.0.102	R6_FRANKFURT2...	8/18/2016 9:20:31 ...		132.504K
6_FRANKFURT	172.16.0.106	N/A	N/A	R6_FRANKFURT3...	8/18/2016 9:20:31 ...		208
6_FRANKFURT	172.16.0.106	4_BERLIN	172.16.0.104	R6_FRANKFURT4...	8/18/2016 9:20:31 ...		144
6_FRANKFURT	172.16.0.106	5_PARIS	172.16.0.105	R6_FRANKFURT5...	8/18/2016 9:20:31 ...		168

You can also use the Administration window to duplicate or rename an existing report group.

Duplicating or Renaming an Existing Report Group

To duplicate or rename an existing report group:

1. Select **Admin**, and in the Admin pane, select **Application** > **Report Groups**.

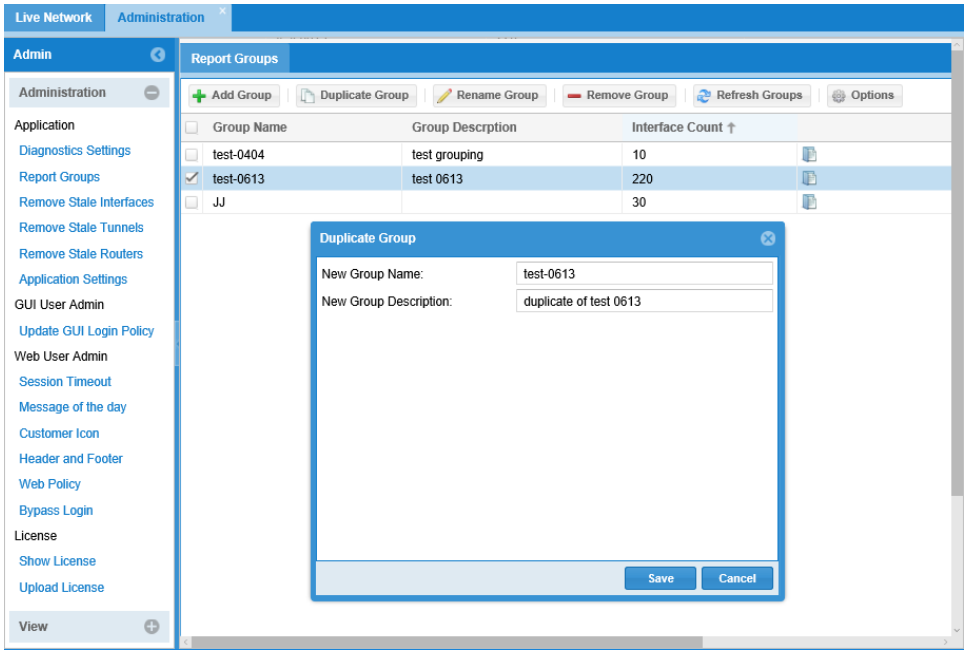
2. In the Report Groups pane, select the group name that you want to duplicate or rename.

3. Perform one of the following actions:

   - To create a duplicate report group, click **Duplicate Group** and complete the fields in the Duplicate Group dialog box, as shown in Figure 155 on page 195.

Copyright © 2018, Juniper Networks, Inc.

Figure 155: Administration Window for Creating a Duplicate Report Group



- To rename a report group, click **Rename Group** and complete the fields in the Rename Group dialog box. The Duplicate Group dialog box and the Rename Group dialog box have identical fields.

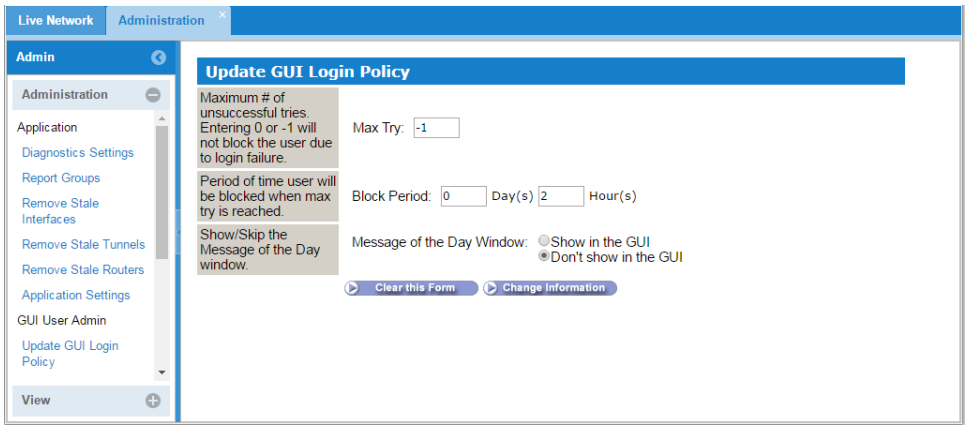
Updating the GUI Login Policy

To update the GUI login policy:

1. Select **Admin**, and in the Admin pane, select **GUI User Admin > Update GUI Login Policy**.

   The Update GUI Login Policy window is displayed.

Figure 156: Administration Window for Updating the GUI Login Policy



2. Modify the fields, following the descriptions in the main pane, and select the access control, if needed. Figure 156 on page 195 shows the fields and descriptions.

3. Click **Change Information** to apply the changes.

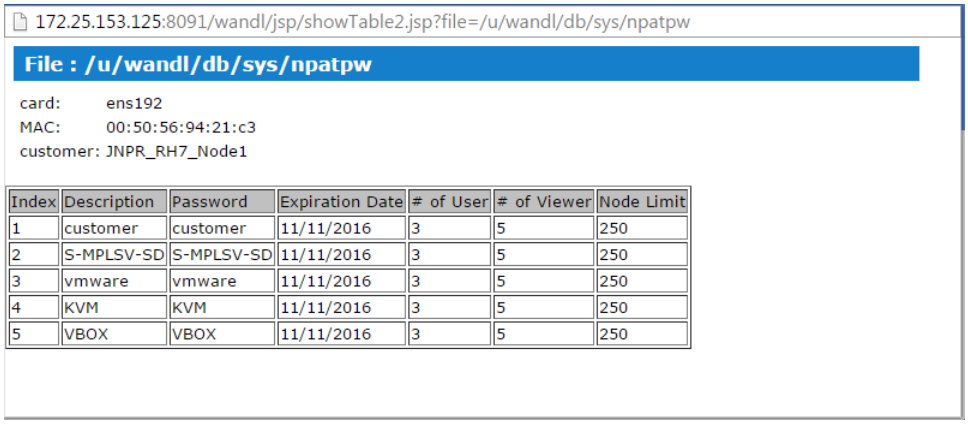
Displaying Current Licenses

To display current licenses:

1. Select **Admin** and in the Admin pane select **License > Show License**.

   The License File window is displayed, as shown in Figure 157 on page 196.

Figure 157: Display Licenses



Index	Description	Password	Expiration Date	# of User	# of Viewer	Node Limit
1	customer	customer	11/11/2016	3	5	250
2	S-MPLSV-SD	S-MPLSV-SD	11/11/2016	3	5	250
3	vmware	vmware	11/11/2016	3	5	250
4	KVM	KVM	11/11/2016	3	5	250
5	VBOX	VBOX	11/11/2016	3	5	250

This window shows the description, password, expiration date, number of users and viewers allowed using the license, as well as the node limit.

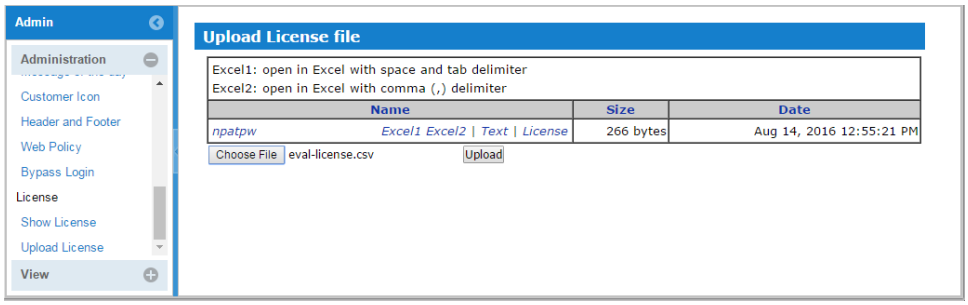
Uploading a License

To upload a license:

1. Select **Admin**, and in the Admin pane, select **License > Upload License**.

   The Upload Licence file window is displayed. Figure 158 on page 196 shows the Upload License file window.

Figure 158: Upload License File



Copyright © 2018, Juniper Networks, Inc.

2. Click **Choose File** to locate the license file, then click **Upload**.

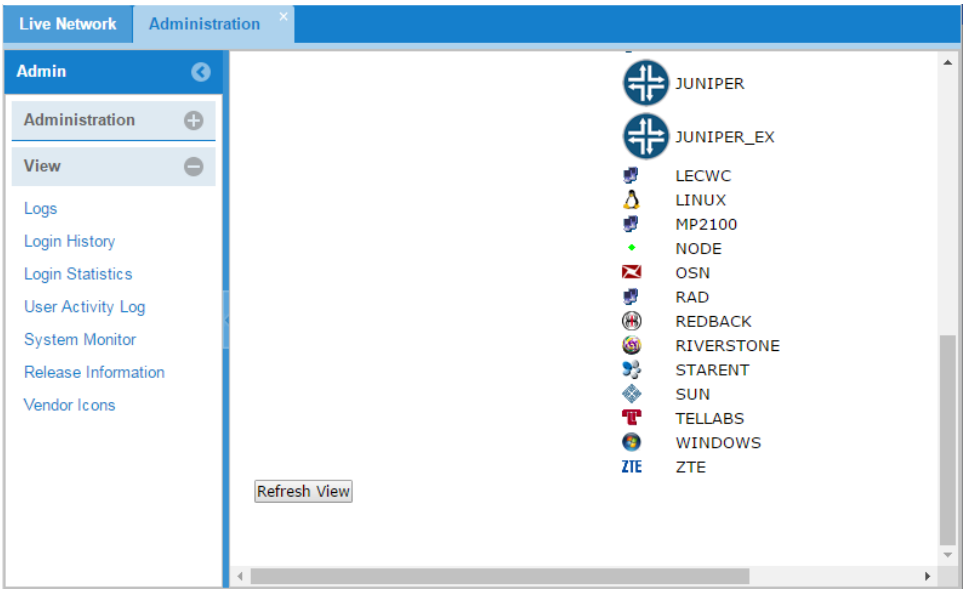
Viewing Vendor Icons

To view the vendor icons used in IP/MPLSView:

1. Select **Admin**, and in the Admin pane, select **View > Vendor Icons**.

   The Vendor Icons window is displayed, as shown in Figure 159 on page 197.

Figure 159: Vendor Icons



2. Click **Refresh View** to refresh the list.

Viewing the User Activity Log

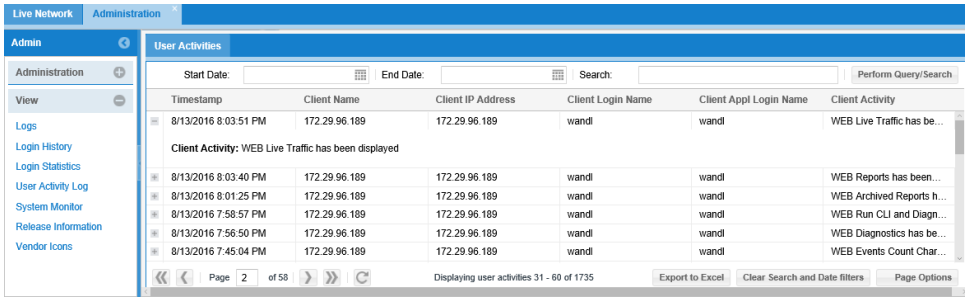
To view the user activity log:

1. Select **Admin**, and in the Admin pane, select **View > User Activity Log**.

   The User Activities window is displayed.

2. Double-click the timestamp entry to display the user activity. Figure 160 on page 198 shows an example of user activity.

Figure 160: Viewing the User Activity Log



3. To modify the dates, select a start date and end date, or search for a specific date and click **Perform Query Search**.

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 9

Tools

- Task Manager on page 199
- MIB Browser on page 210
- Device Profiles on page 218
- User Administration on page 230
- Using the File Browser on page 233

Task Manager

- Understanding Task Manager on page 199
- Creating a New Task in Task Manager on page 200
- Managing Existing Tasks on page 204
- Performance Management Tasks Using Task Manager and Apache Spark Clusters on page 205
- Running a Task Using Spark Clusters on page 207

Understanding Task Manager

The Task Manager is a fundamental component of IP/MPLSView that you use to create, schedule, run, and manage data collection and reporting tasks for your live network.

To access Task Manager, select **Tools > Task Manager** from the IP/MPLS main menu. Task Manager enables you to perform the following tasks:

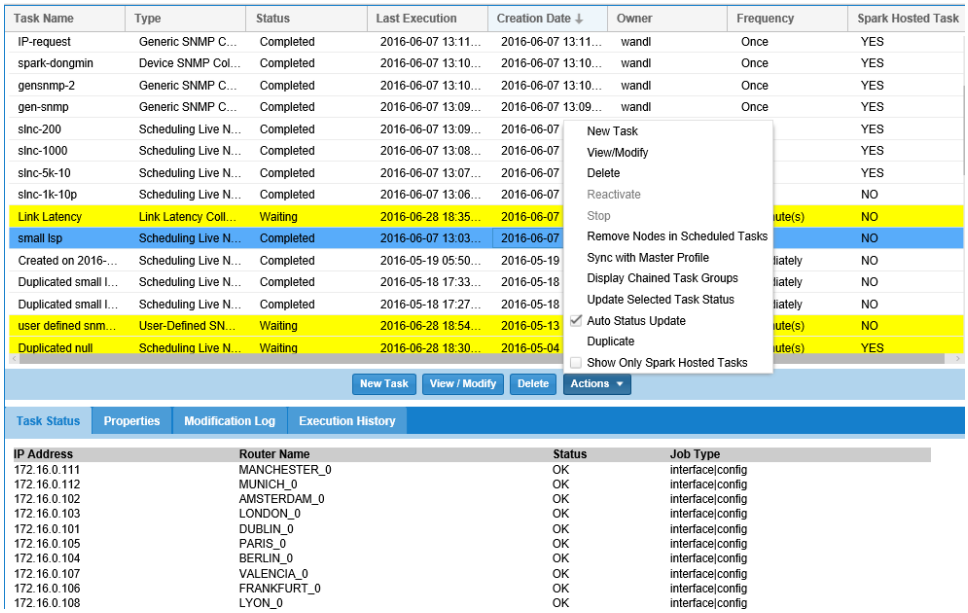
- Create, modify, delete, duplicate, and schedule network data collection tasks.
- Stop a task that is in progress.
- Search a list of tasks by name or by type of task.
- Chain together a sequence of similar tasks by scheduling a particular task to run immediately after another task.
- Chain tasks as part of a Scheduling Live Network Collection operation.
- Remove nodes in selected tasks.
- Run a Network Performance Data Report task.

Copyright © 2018, Juniper Networks, Inc.

- Run all SAM tasks (SAM Collection, SAM Interface Traffic Collection, and SAM LSP Statistics Collection).
- Assign a collection task to run on a distributed Task Manager server, distributed remote collection server, or an Apache Spark Cluster.

Figure 161 on page 200 shows an example of theTask Manager window, with the Actions drop-down menu expanded.

Figure 161: Task Manager



See Also

- Management and Monitoring Guide for IP/MPLSView
- Device Profiles on page 218
- *Task Manager*

Creating a New Task in Task Manager

To create a new task in Task Manager:

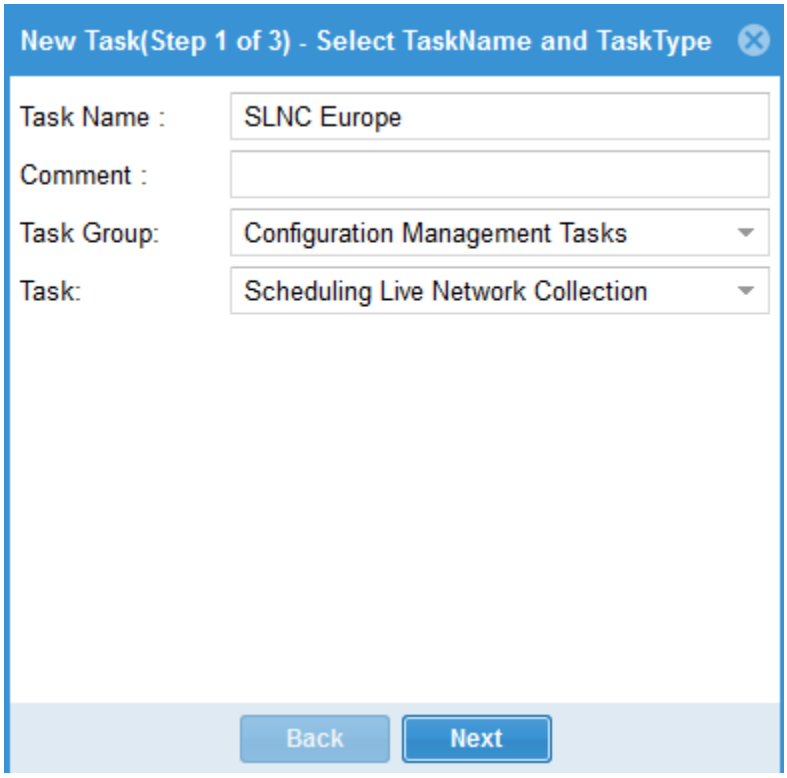
1. Click **New Task**, or select **Actions > New Task**.

2. Select the task, and specify a task name and optional comment.

   To select the task from a smaller list of related tasks, select the type of task in the Task Group field and then select the task.

Copyright © 2018, Juniper Networks, Inc.

Figure 162: Creating a New Task

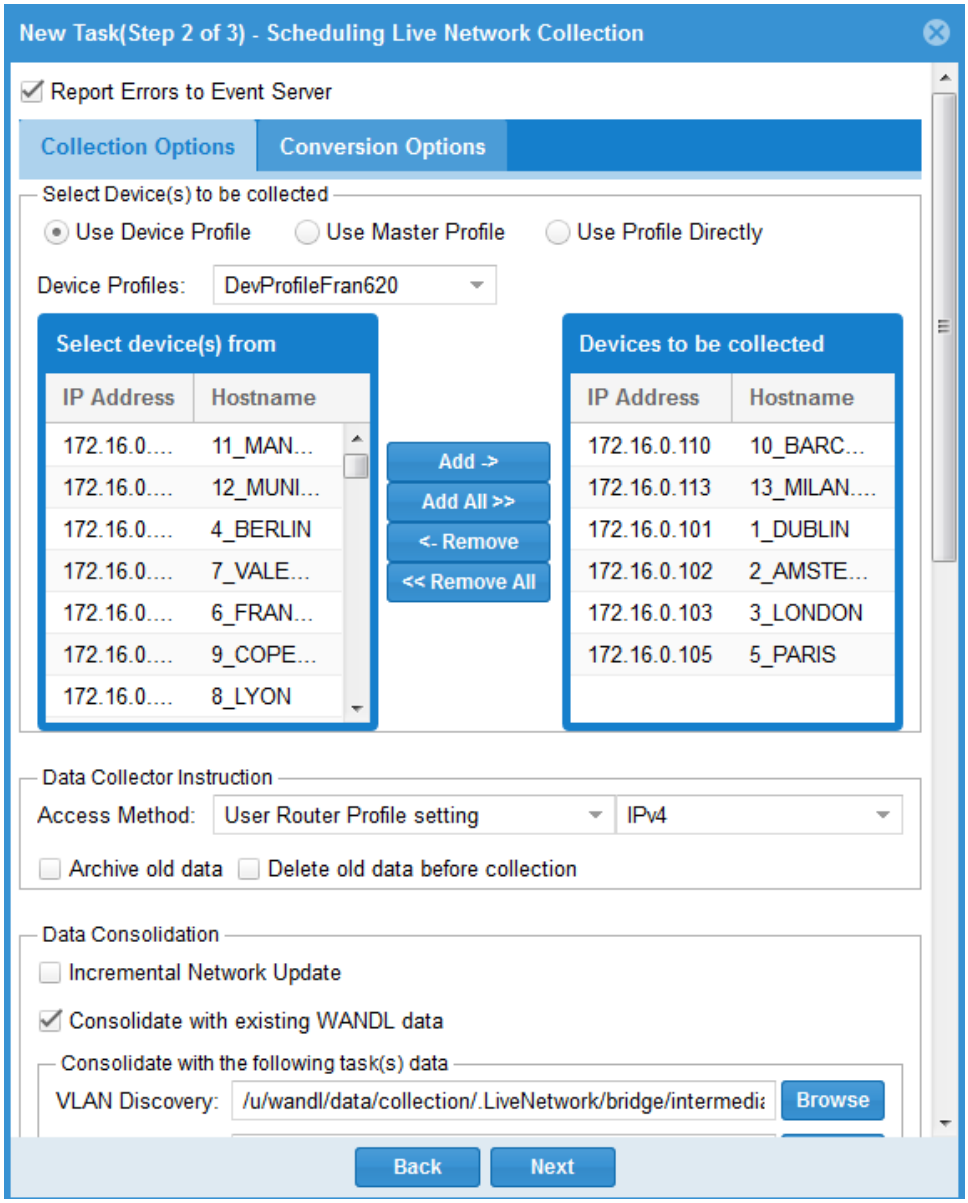


3. Click **Next**.

4. Specify the devices in the live network from which to collect data.

   You can choose some or all of the devices configured in a device profile, or you can use the master profile.

Figure 163: Selecting the Devices for Collection



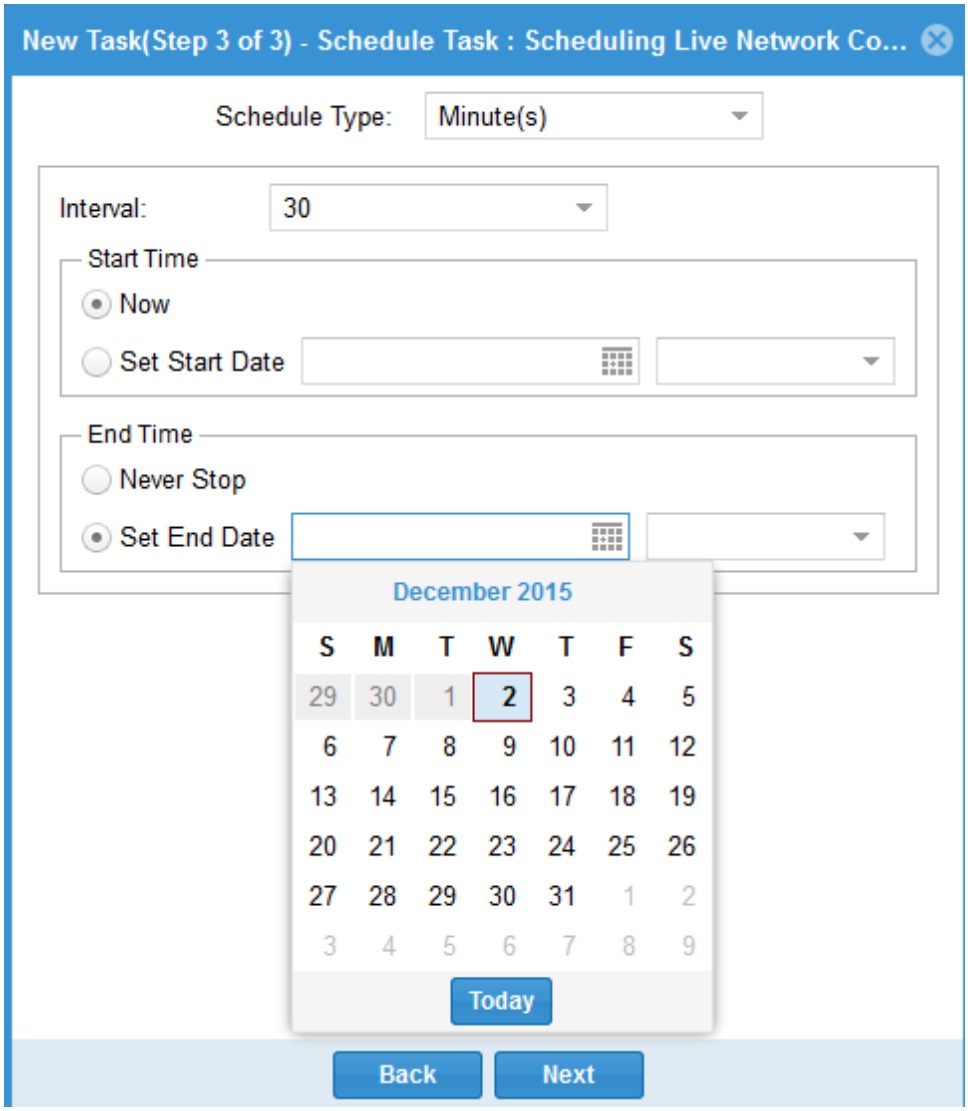
5. Configure the required collection options and consolidation options.

6. Click **Next**.

7. Configure scheduling parameters for the new task.

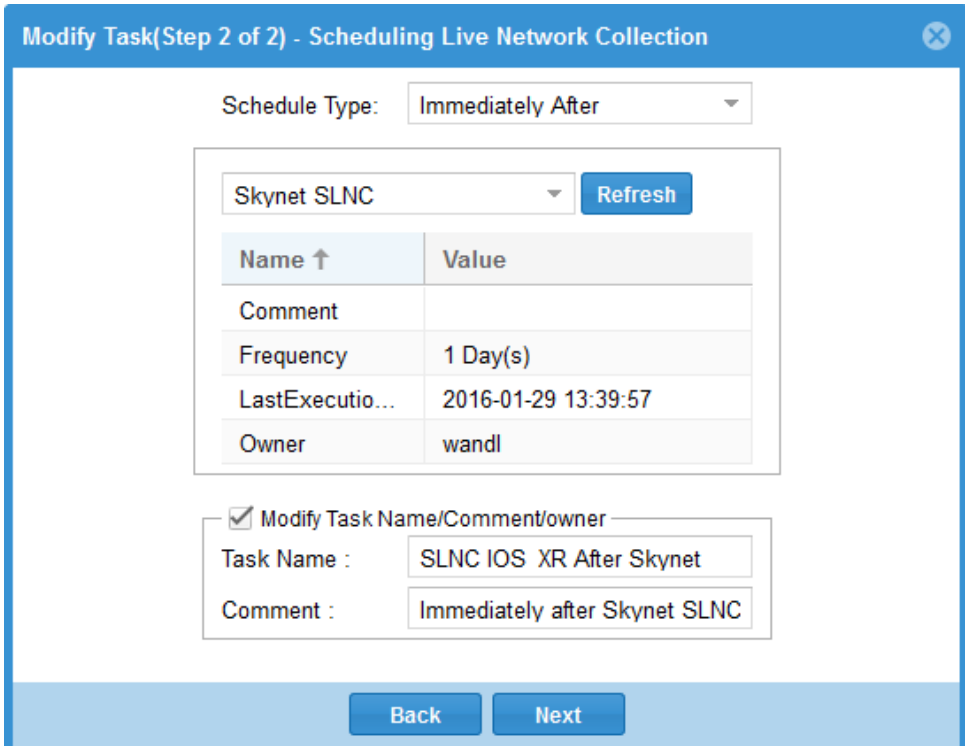
Copyright © 2018, Juniper Networks, Inc.

Figure 164: Scheduling the Task



8. To chain this Scheduling Live Network Collection task to another task, select **Immediately After** from the Schedule Type drop-down menu, and select the preceding task to which you want to chain this collection task. Optionally, you can select **Modify TaskName/Comment/Owner** to specify a different task name and comment for the chained task. Figure 165 on page 204 shows an example of how to chain a Scheduling Live Network Collection task.

Figure 165: Chained Scheduling Live Network Collection Task



9. Click **Next** to create the new task and display it in the Task Manager window.

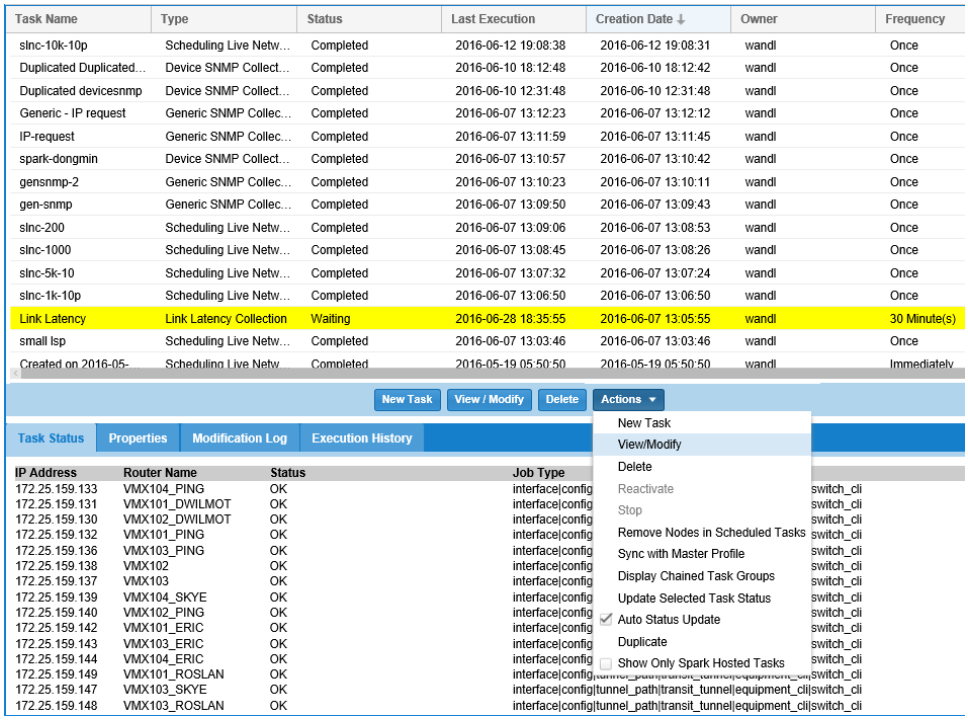
Managing Existing Tasks

To manage an existing task in Task Manager, select the task name in the upper pane and click the appropriate button, or right-click the task name and select the desired task from either the **Actions** drop-down menu or the task drop-down menu. You can access the same set of tasks from the Actions drop-down menu and the task drop-down menu.

- To view or modify task properties, click or select **View/Modify**.
- To delete a task, click or select **Delete**.
- To perform other tasks such as stopping a running task, removing devices in a scheduled task, updating the task status, and duplicating a task, select the desired task from either the **Actions** drop-down menu as shown in Figure 166 on page 205 or the task drop-down menu.

Copyright © 2018, Juniper Networks, Inc.

Figure 166: Managing an Existing Task



Performance Management Tasks Using Task Manager and Apache Spark Clusters

Apache Spark is a fast engine for big data processing using clusters. You can run the Performance Management Tasks using Task Manager and Spark clusters. The performance Management Tasks are:

Advanced Ping Collection Task—Collect latency and jitter between interfaces.

Device Ping Collection Task—Collect latency and loss percentage between devices.

Device SLA Collection Task—Collect SLA information from the devices.

Device SNMP Collection Task—Collect CPU usage, CPU temperature, memory, and system uptime from the device.

LSP Ping Collection Task—Collect tunnel LSP latency and jitter.

Link Latency Collection Task—Collect latency and jitter of the link.

Server Performance Data Collection Task—Similar to the Device SNMP Collection Task but for the servers.

User CLI Collection Task—Collect any CLI.

User-defined SNMP Collection Task—Collect any SNMP MIBs.

How to Prepare the Data

The following items need to be configured before running a task using Apache Spark:

- The Spark master must be running on the Application Server.
- SNMP has access to the devices/servers from the Application Server and Spark slaves.
- Log in access is available to the devices/servers for CLI collections from the Application Server and Spark slaves.
- Devices/servers must be reachable from the Application Server and Spark slaves.
- Proper license is copied to the Spark slaves.
- The SSH connection from master to slave does not require a password.

The Task Manager Server is running as a part of the Application Server. To execute the task in the Spark Cluster, select the Spark Cluster option in the last step of the task submission. This option is only available for the Spark Cluster enabled tasks. In the Task Manager window, the Spark Hosted Task column identifies the tasks running in the Spark Cluster. The Spark Hosted Task column is displayed in Figure 161 on page 200.

 Copyright © 2018, Juniper Networks, Inc.

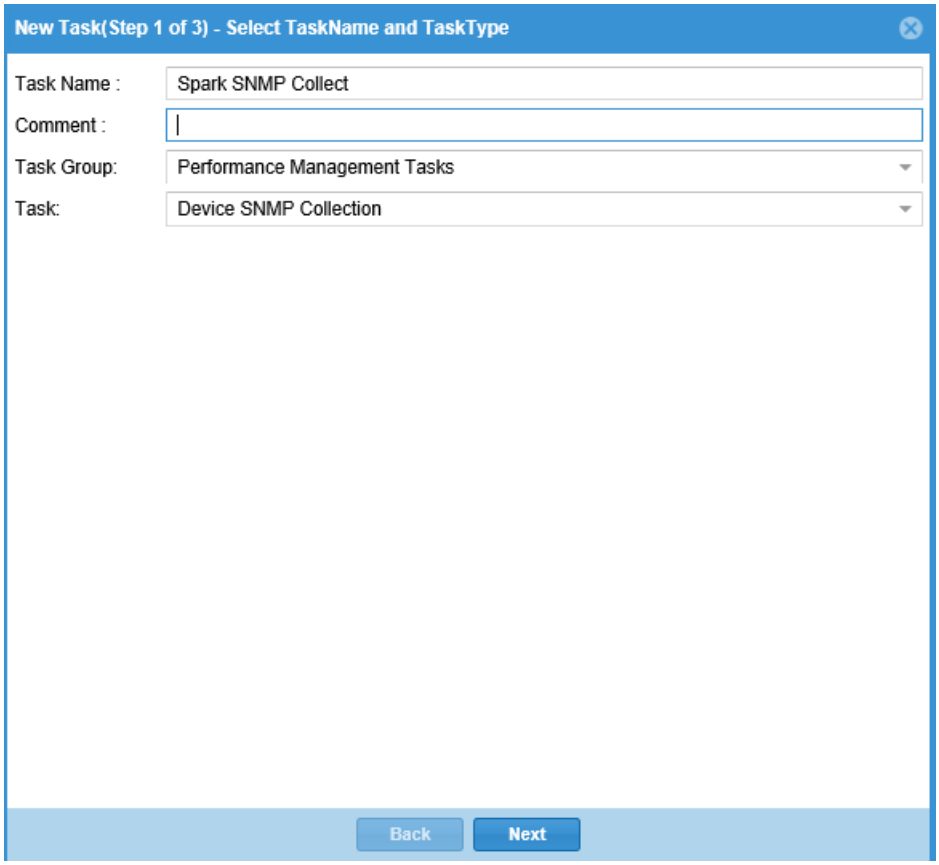
Running a Task Using Spark Clusters

To run a task using Spark Clusters:

1. Select **Tools > Task Manager**, then click **New Task**.

   The New Task (Step 1 of 3) - Select TaskName and TaskType window is displayed, as shown in Figure 167 on page 207.

Figure 167: New Task - Select Task Name and Task



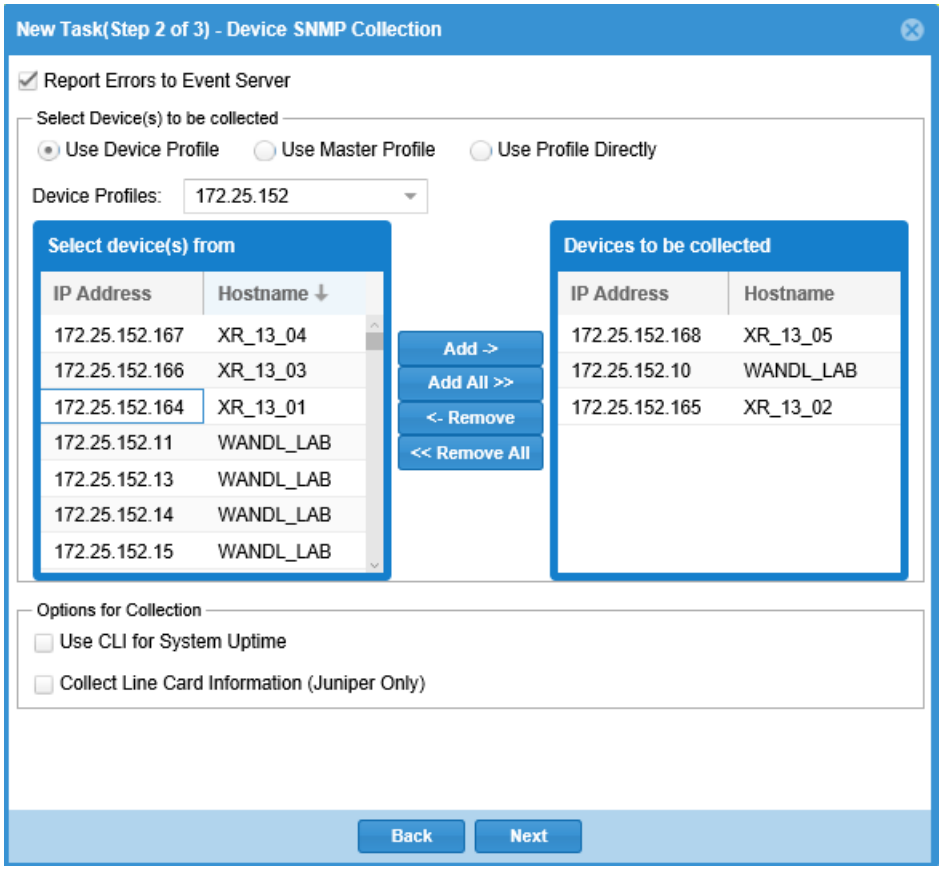
2. Select the task and specify a task name and optional comment.

   To select the task from a smaller list of related tasks, select the type of task from the Task Group list. Then select the task from the Task list.

3. Click **Next**.

   The New Task (Step 2 of 3) - Schedule Task: Device SNMP Collection window is displayed, as shown in Figure 168 on page 208

Figure 168: New Task - Select Devices and Options for Collection



4. Specify the devices in the live network from which to collect data.

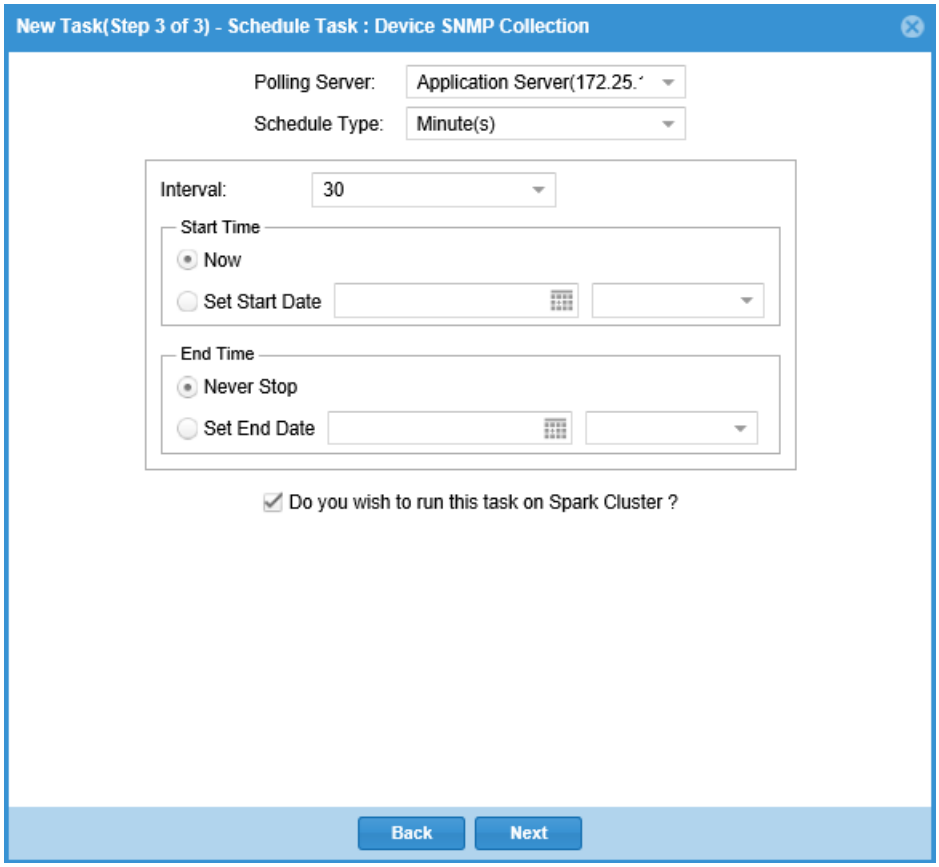
   You can choose some or all of the devices configured in a device profile, or you can use the master profile. You can also specify options for collection.

5. Click **Next**.

   The New Task (Step 3 of 3) - Schedule Task: Device SNMP Collection window is displayed, as shown in Figure 169 on page 209.

Copyright © 2018, Juniper Networks, Inc.

Figure 169: New Task - Schedule Task and Enable Spark

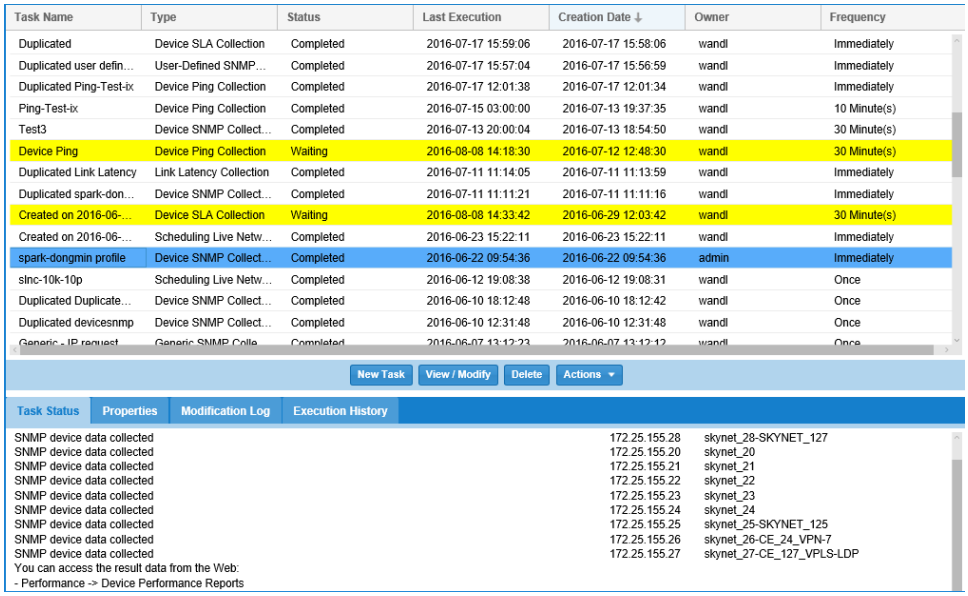


6. Configure the scheduling parameters for the new task.

7. Select **Do you wish to run this task on Spark Cluster?**, then click **Next**.

   The results are displayed in the Task Status tab, as shown in Figure 170 on page 210.

Figure 170: Task Status Results



Task Name	Type	Status	Last Execution	Creation Date ↓	Owner	Frequency
Duplicated	Device SLA Collection	Completed	2016-07-17 15:59:06	2016-07-17 15:58:06	wandl	Immediately
Duplicated user defin...	User-Defined SNMP...	Completed	2016-07-17 15:57:04	2016-07-17 15:56:59	wandl	Immediately
Duplicated Ping-Test-ix	Device Ping Collection	Completed	2016-07-17 12:01:38	2016-07-17 12:01:34	wandl	Immediately
Ping-Test-ix	Device Ping Collection	Completed	2016-07-15 03:00:00	2016-07-13 19:37:35	wandl	10 Minute(s)
Test3	Device SNMP Collect...	Completed	2016-07-13 20:00:04	2016-07-13 18:54:50	wandl	30 Minute(s)
Device Ping	Device Ping Collection	Waiting	2016-08-08 14:18:30	2016-07-12 12:48:30	wandl	30 Minute(s)
Duplicated Link Latency	Link Latency Collection	Completed	2016-07-11 11:14:05	2016-07-11 11:13:59	wandl	Immediately
Duplicated spark-don...	Device SNMP Collect...	Completed	2016-07-11 11:11:21	2016-07-11 11:11:16	wandl	Immediately
Created on 2016-06-...	Device SLA Collection	Waiting	2016-08-08 14:33:42	2016-06-29 12:03:42	wandl	30 Minute(s)
Created on 2016-06-...	Scheduling Live Netw...	Completed	2016-06-23 15:22:11	2016-06-23 15:22:11	wandl	Immediately
spark-dongmin profile	Device SNMP Collect...	Completed	2016-06-22 09:54:36	2016-06-22 09:54:36	admin	Immediately
slnc-10k-10p	Scheduling Live Netw...	Completed	2016-06-12 19:08:38	2016-06-12 19:08:31	wandl	Once
Duplicated Duplicate...	Device SNMP Collect...	Completed	2016-06-10 18:12:48	2016-06-10 18:12:42	wandl	Once
Duplicated devicesnmp	Device SNMP Collect...	Completed	2016-06-10 12:31:48	2016-06-10 12:31:48	wandl	Once
Generic - IP request	Generic SNMP Colle...	Completed	2016-06-07 13:12:23	2016-06-07 13:12:12	wandl	Once

NOTE: To view the Spark task logs, go to http://<application-server-ip>:18080.

Related Documentation

- Device Profiles on page 218

MIB Browser

- Understanding the MIB Browser on page 210
- Viewing MIB Information on page 211
- Loading and Unloading MIB Subtrees on page 211
- Querying SNMP MIB Information from Network Devices on page 212
- Filtering the MIB Tree Display by Trap Numbers on page 214
- Modifying SNMP Trap Configuration Files on page 215

Understanding the MIB Browser

The MIB Browser enables you to work with SNMP to perform the following tasks:

- View, load, and unload SNMP MIB information.
- Query SNMP MIB information from a network device.
- Filter the SNMP MIB tree display by trap numbers.
- Launch the SNMP Trap Editor to configure the SNMP traps to record.

Copyright © 2018, Juniper Networks, Inc.

In most cases, the preconfigured events that come with the Event Browser should be sufficient to meet your needs. In some situations however, you might want to create, modify, and delete the traps that are processed by the SNMP Trap server. To do so, you can launch the SNMP Trap Editor from the MIB Browser.

Viewing MIB Information

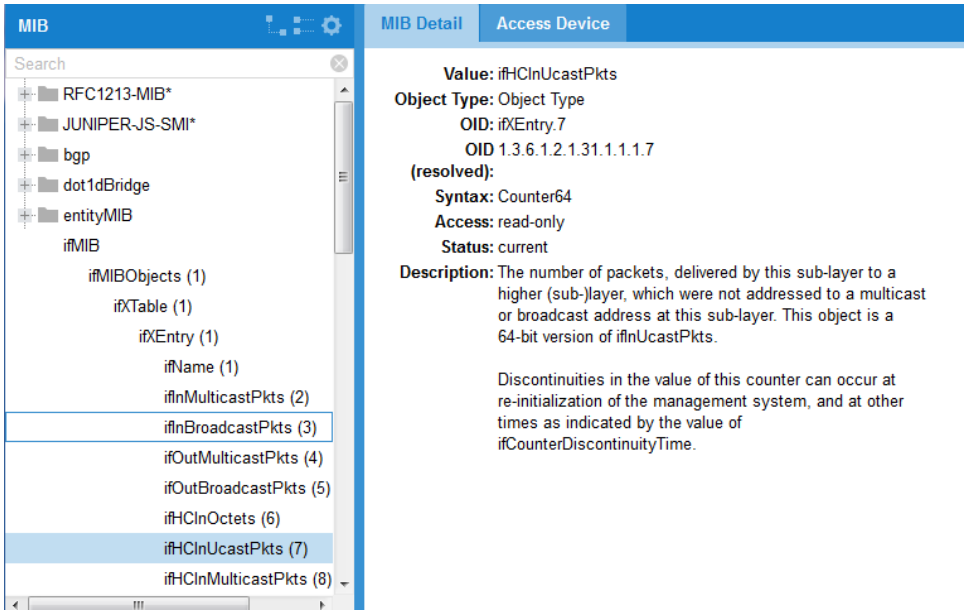
To view MIB information:

1. Select **Tools > MIB Browser**.

2. In the MIB pane, select the MIB object for which you want more information.

3. Select the **MIB Detail** tab to view a description of the selected MIB object.

Figure 171: MIB Browser with MIB Details



Loading and Unloading MIB Subtrees

To load and unload MIB subtrees:

1. Select **Tools > MIB Browser**.

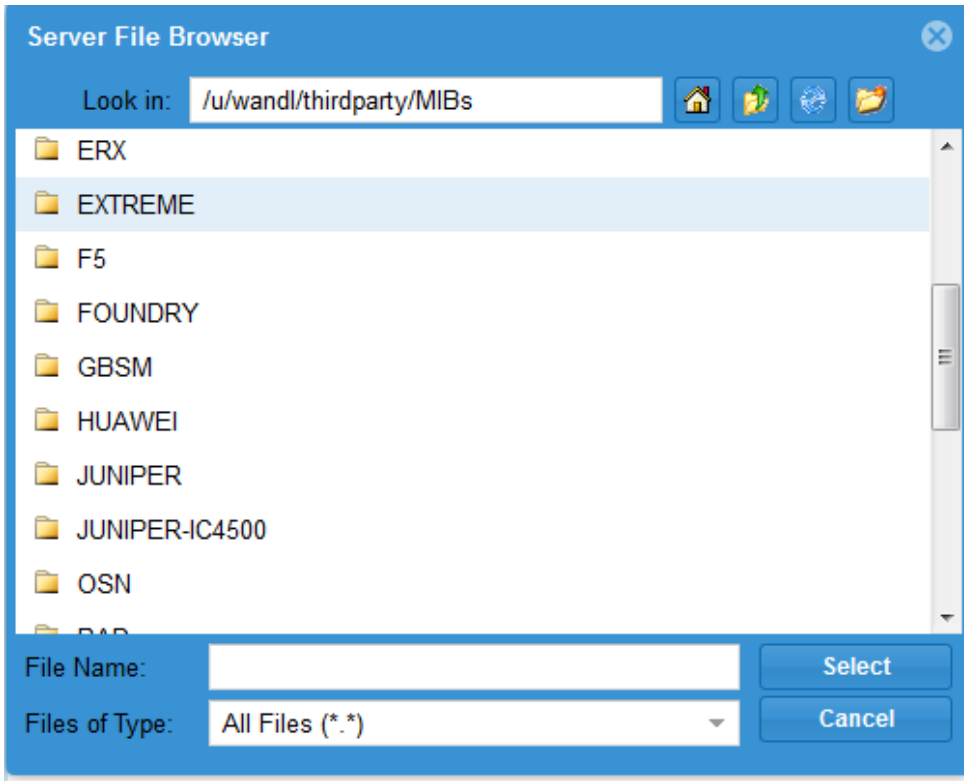
2. In the MIB pane, click the gear icon and select **Load MIB**.

Figure 172: Gear Icon in MIB Browser

3. Specify whether you want to load the new MIBs from the local client or the IP/MPLSView server, and browse to find the MIBs you want to load.

   If you load the MIBs from the server, **Browse** accesses the **/u/wandl/thirdparty/MIBs** directory by default, which is the repository for MIBs from Juniper Networks and other vendors.

Figure 173: Server File Browser



4. Click **Select** to load the desired MIBs.

5. To unload a specified MIB object, right-click the object in the left pane and select **Unload this MIB**.

Querying SNMP MIB Information from Network Devices

To query SNMP MIB information from network devices:

1. Select **Tools > MIB Browser**.

2. From the **Access Device** tab, specify the IP address in one of the following ways:

   - Click the magnifying glass icon in the Host/IP Address box. Select the device profile and associated network device that you want to query, and click **Select**.

Copyright © 2018, Juniper Networks, Inc.

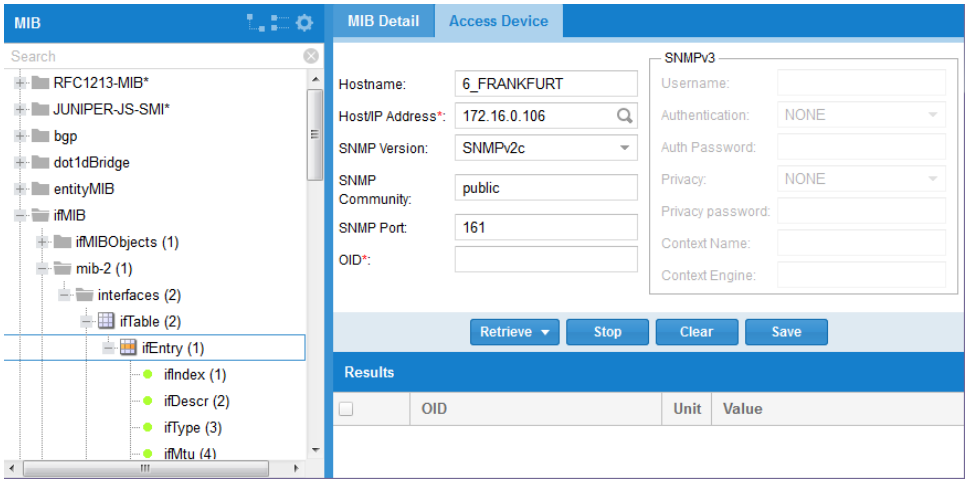
This action populates the Hostname, Host/IP Address, SNMP Community, and SNMP Port settings in the Access Device tab.

- Type a value in the Host/IP Address box.

3. Specify the SNMP Version (SNMPv1, SNMPv2c, or SNMPv3), and the SNMP Community string (default value is public).

   Choosing SNMPv3 displays additional authentication and password settings in the SNMPv3 group box.

Figure 174: MIB Browser Access Device Tab



4. In the MIB pane, click the MIB object for which you want to collect information.

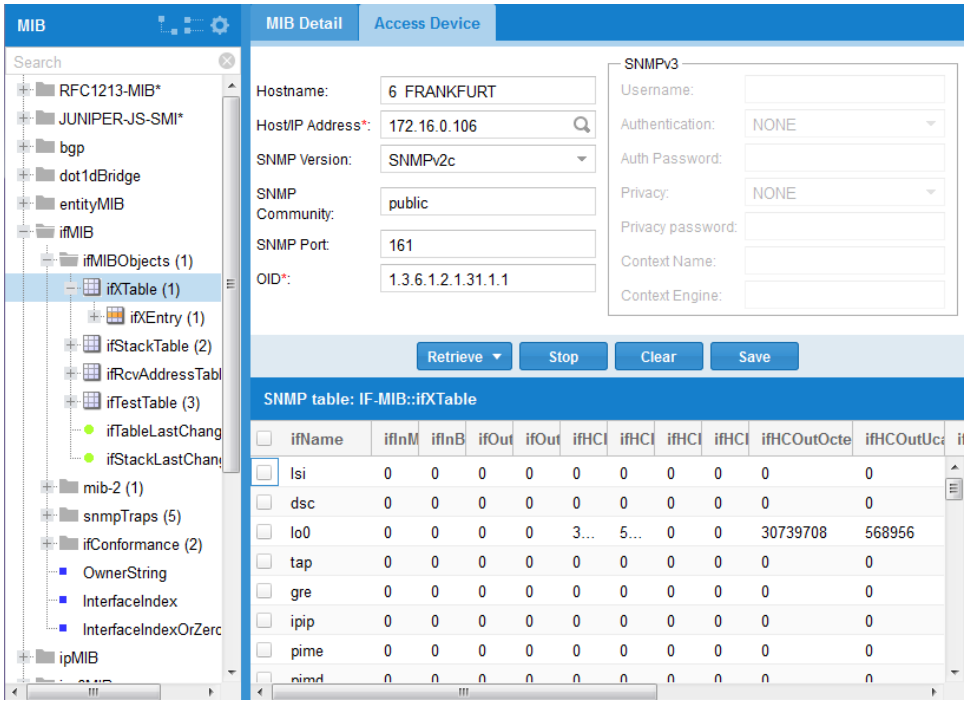
   This action populates the object identifier (OID) setting in the Access Device tab.

5. Retrieve data for the selected OID in one of the following ways:

   - To get data for the specified OID, select **Retrieve > Get**.
   - To step through the OIDs to get data for the next OID in the MIB, select **Retrieve > Get next** repeatedly.
   - To get data for all of the child OIDs of a selected parent OID, select **Retrieve > Get all**.

   Figure 175 on page 214 shows the results of retrieving all child OIDs under the ifXTable MIB object. The MIB Browser displays the results in a tabular format with columns for each field.

Figure 175: MIB Browser Retrieving All OIDs



Filtering the MIB Tree Display by Trap Numbers

To filter the MIB tree display by trap numbers:

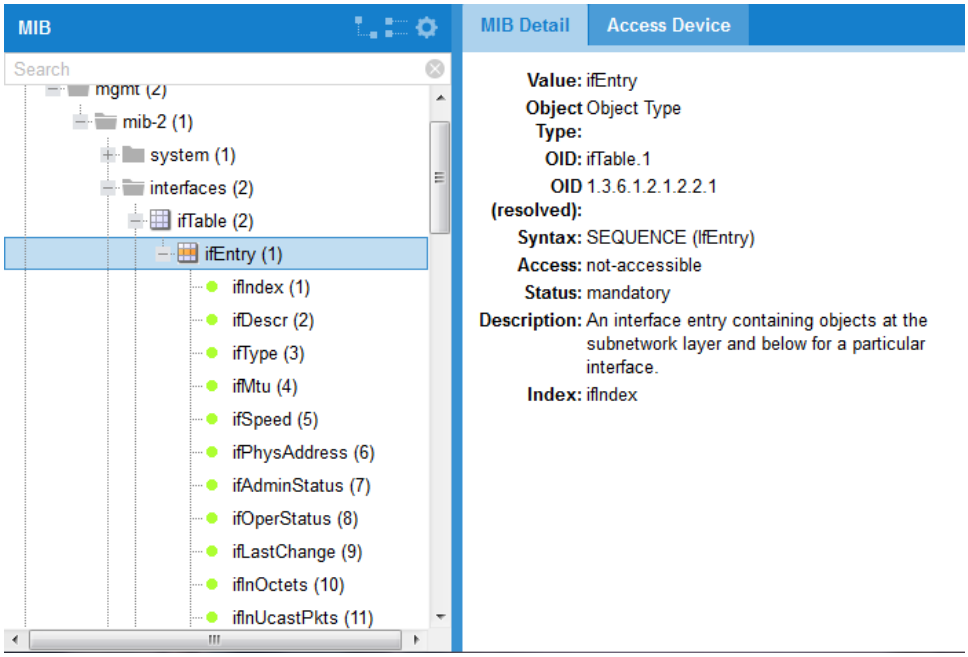
1. Select **Tools > MIB Browser**.

2. In the MIB pane, click the gear icon and select **Filter by trap**.

   Figure 176 on page 215 shows the MIB objects under ifEntry listed in ascending order by trap number.

Copyright © 2018, Juniper Networks, Inc.

Figure 176: MIB Browser Filtering by Trap Numbers



Modifying SNMP Trap Configuration Files

To modify SNMP trap configuration files:

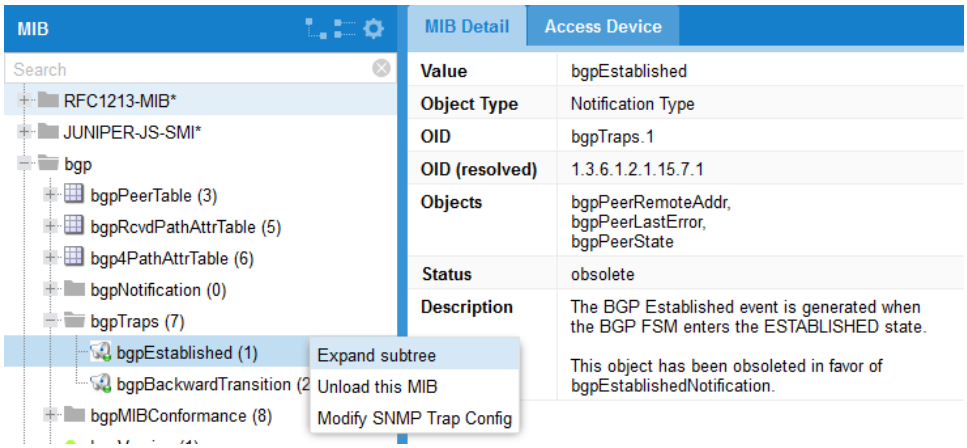
1. Select **Tools > MIB Browser**.

2. In the MIB pane, click the gear icon and select **Enable SNMP Config Editing**.

3. In the MIB pane, navigate to and select the trap you want to modify.

   Information about the properties of the selected trap is displayed in the MIB Detail tab.

Figure 177: Modify SNMP Trap Config for bgpEstablished



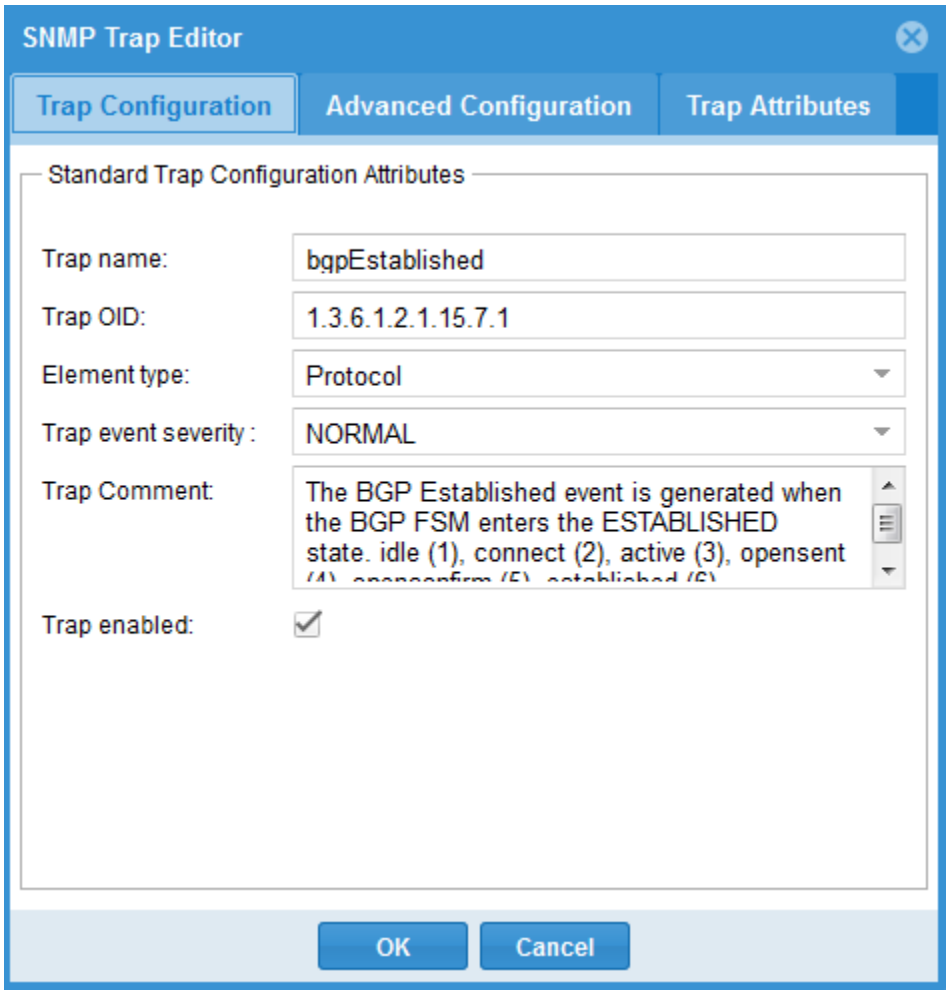
4. Right-click the trap you want to modify and select **Modify SNMP Trap Config**.

   This action launches the SNMP Trap Editor.

5. Select the **Trap Configuration** tab and modify the properties as needed.

   You can specify the trap name, trap OID, associated element type, severity, and a comment. You can also select or clear the **Trap enabled** check box to control whether or not the SNMP trap server can process the trap.

Figure 178: SNMP Trap Editor Trap Configuration Tab

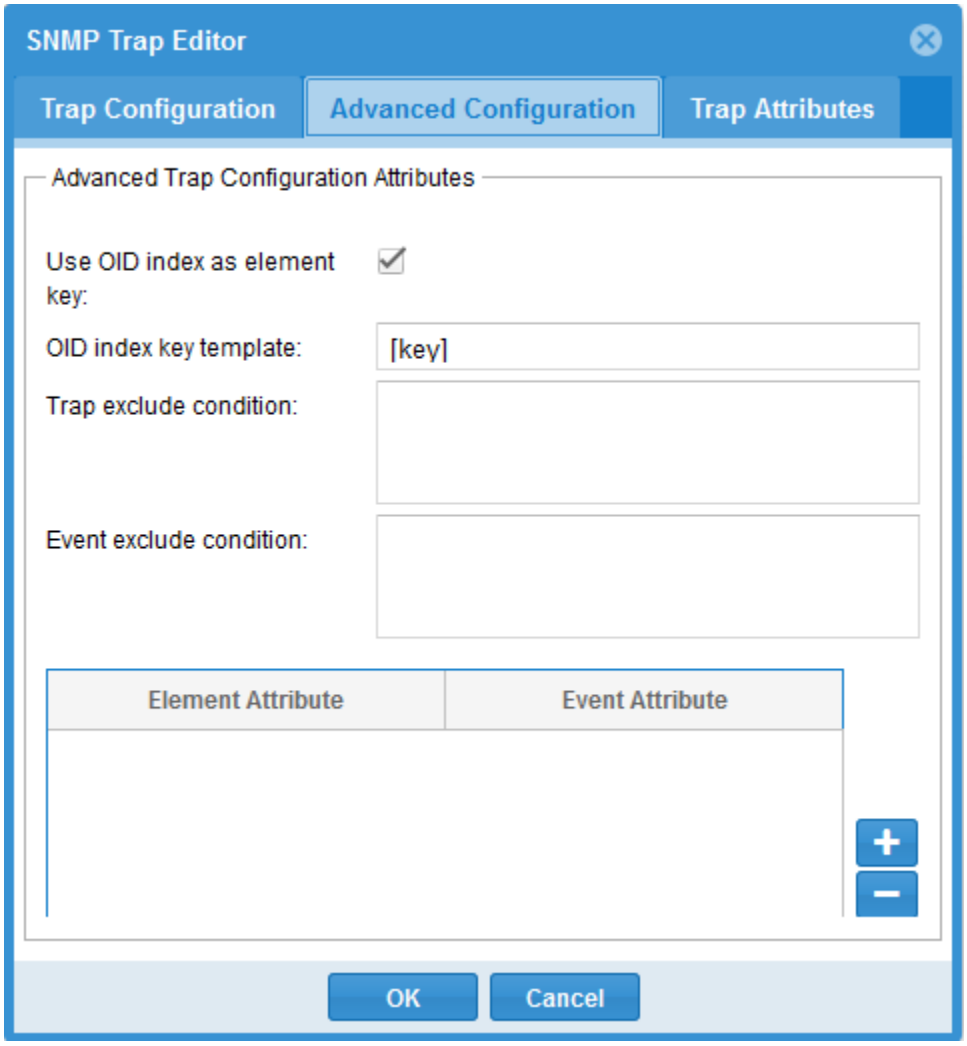


6. Select the **Advanced Configuration** tab and modify the properties as needed.

   Select the **Use OID as element key** check box to use the OID subidentifier as the key to associate the trap with the appropriate network element. You can then specify a value in the **OID index key template** field to map the subidentifier to the associated element.

Copyright © 2018, Juniper Networks, Inc.

Figure 179: SNMP Trap Editor Advanced Configuration Tab



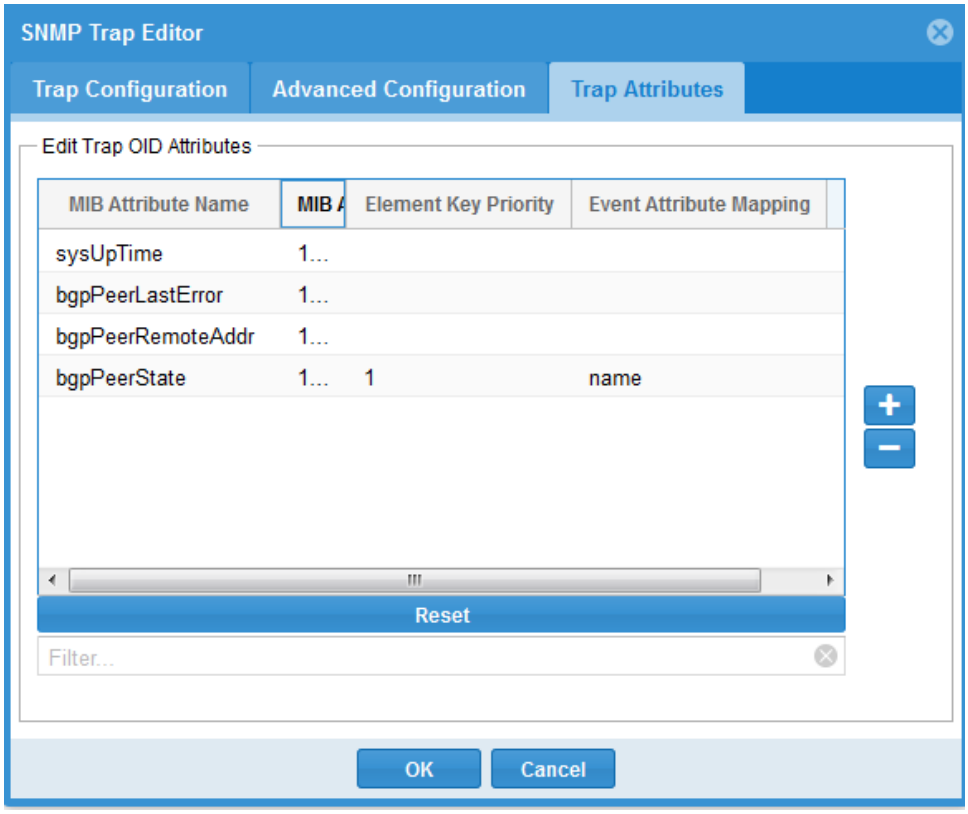
7. Select the **Trap Attributes** tab and modify the attributes as needed.

   The Edit Trap OID Attributes box lists the various MIB attribute OIDs associated with this trap and the corresponding MIB attribute name. To modify a particular MIB attribute, double-click the value you want to modify to make it editable.

   A nonzero value starting with 1 in the Element Key Priority column indicates that this OID is the key to identify the trap with its associated network element. For these key OIDs, the value in the Event Attribute Mapping column maps the value from the trap to the appropriate Event Browser column. For example, in Figure 180 on page 218, the bgpPeerState trap uses the keyword **name** as a mapping to the Event Browser.

   - To add a new MIB, click the plus (**+**).
   - To delete a MIB, select the row for that MIB and click the minus (**-**).
   - To automatically repair any previously entered OIDs that are incorrect, click **Reset**.

Figure 180: SNMP Trap Editor Trap Attributes Tab



Device Profiles

- Understanding Device Profiles on page 218
- Creating a New Device Profile on page 219
- Adding Devices to a Device Profile on page 220
- Modifying a Device Entry in a Profile on page 221
- Deleting an Entry in a Device Profile or a Device Profile on page 221
- Verifying Connectivity for One or More Devices in a Device Profile on page 222
- Populating a Device Profile on page 224
- Updating Device Profiles when Device Passwords are Changed on page 228
- Dual Routing Engine Support on page 228
- Inaccessible Nodes on page 229
- Syncing to the Master Profile on page 229

Understanding Device Profiles

To enable IP/MPLSView to connect to and collect data from devices in your network, you must configure one or more device profiles. A *device profile* is a list of devices (typically routers and switches) that specifies connection attributes including the device type, login

Copyright © 2018, Juniper Networks, Inc.

credentials, and IP addresses. You can define multiple device profiles, each containing as many devices as needed for your topology.

To access the Device Profiles window, select **Tools > Device Profiles** from the IP/MPLSView main menu. From the Device Profiles window, you can perform the following tasks:

- Create device entries and profiles.
- Modify device entries and profiles.
- Delete device entries and profiles.
- Verify connectivity for one or more devices in a device profile.

NOTE: To import a device profile into IP/MPLSView from an external source, such as a configuration file, you must access and use the Device Profile window from the Java client interface.

See Also

- Task Manager on page 199
- *Import Router Profile*

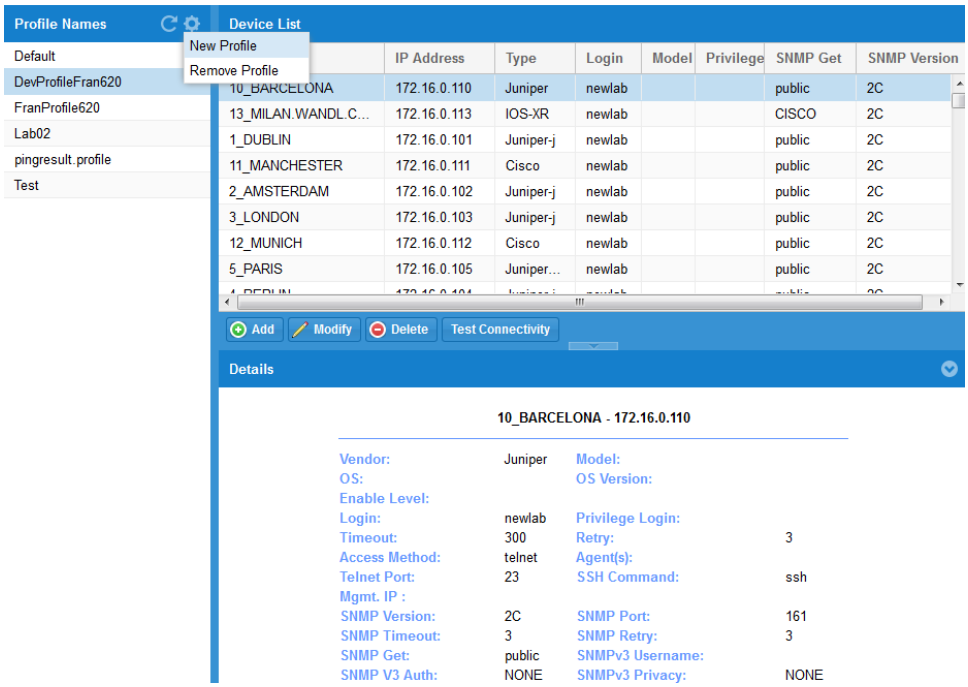
Creating a New Device Profile

To create a new device profile:

1. Select **Tools > Device Profiles**.

   The Device Profiles window is displayed. Figure 181 on page 220 shows the Device Profiles window.

Figure 181: Device Profiles Window



2. Click the gear icon at the top of the Profile Names pane and select **New Profile**.

3. Specify the profile name in the Add New Profile window, and click **OK**.

   The new profile is displayed in the Profile Names pane.

See Also

- Task Manager on page 199

Adding Devices to a Device Profile

To add devices to a device profile:

1. Select **Tools > Device Profiles**.

   The Device Profiles window is displayed.

2. Select the name of the device profile you want to populate, and click **Add**.

   The Add New Device window is displayed. (The Add New Device window is identical to the Modify Devices window shown in Figure 182 on page 221.)

3. Specify the access parameters and SNMP parameters for the new device, and click **Add**.

   The new device entry is displayed in the Device List pane for the selected profile.

Copyright © 2018, Juniper Networks, Inc.

For detailed descriptions of the parameters in the Add New Device window, see Table 30 on page 225.

Modifying a Device Entry in a Profile

To modify a device entry in a profile:

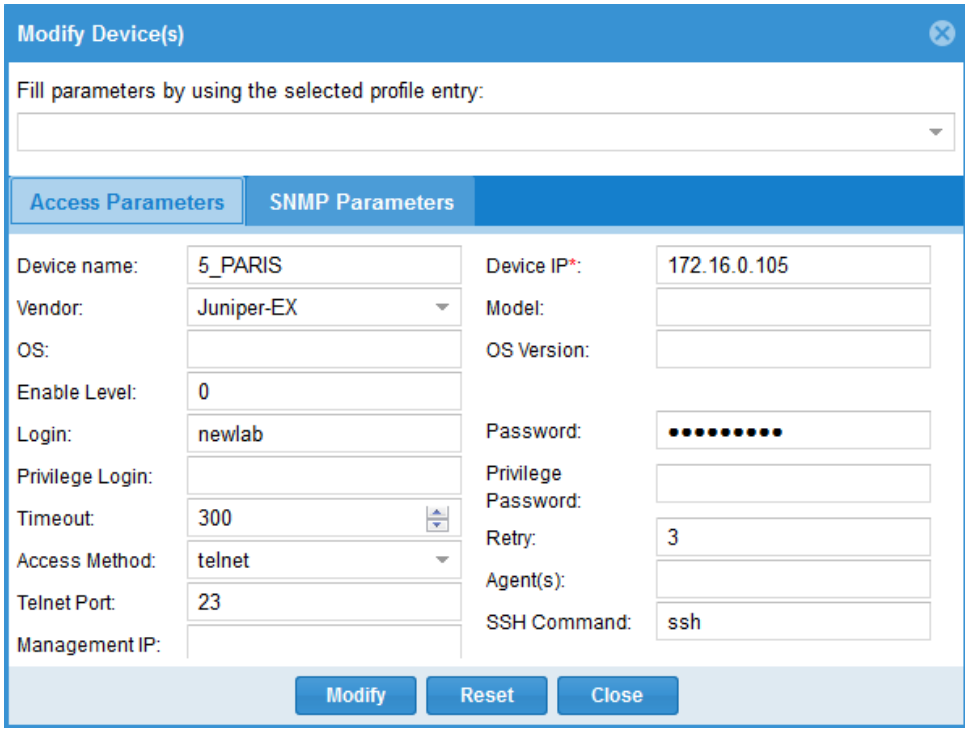
1. Select **Tools > Device Profiles**.

   The Device Profiles window is displayed.

2. Select the name of the device you want to modify, and click **Modify**.

   The Modify Devices window is displayed.

Figure 182: Modifying a Device Entry in a Profile



3. Update the parameters as needed for your device, and click **Modify**.

   For detailed descriptions of the parameters in the Modify Devices window, see Table 30 on page 225.

Deleting an Entry in a Device Profile or a Device Profile

To delete a device entry or a device profile:

1. Select **Tools > Device Profiles**.

   The Device Profiles window is displayed.

2. Select the profile name (in the Profile Names pane) or device name (in the Device List pane) that you want to delete.

   You can select multiple devices by holding down the Ctrl and Shift keys while selecting rows.

3. Click **Delete**.

Verifying Connectivity for One or More Devices in a Device Profile

To verify connectivity for one or more devices in a device profile:

1. Select **Tools > Device Profiles**.

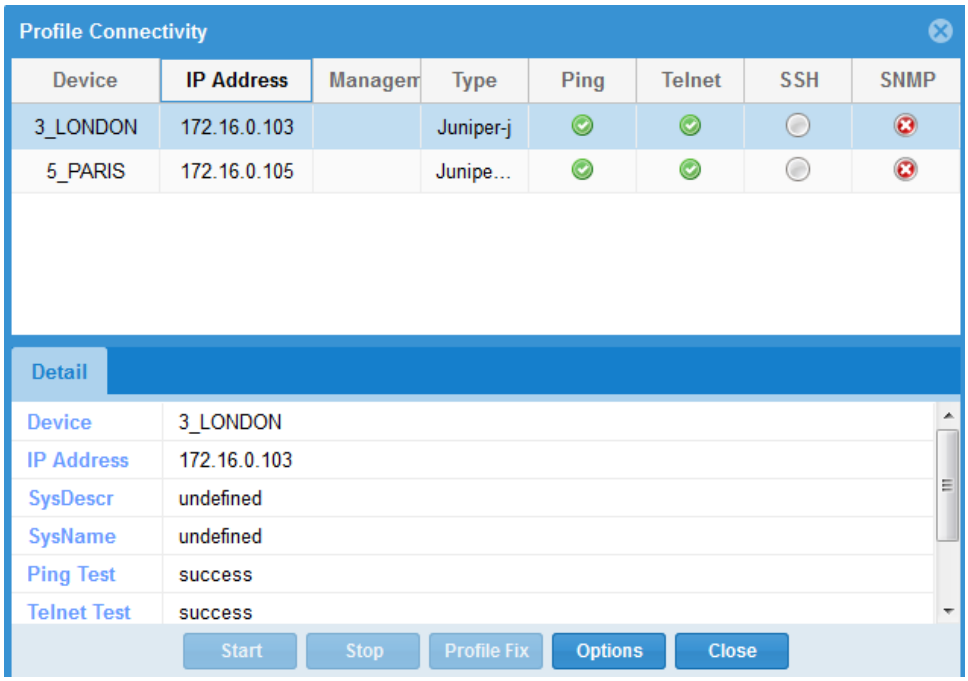
   The Device Profiles window is displayed.

2. In the Device List pane, select the names of one or more devices for which you want to verify connectivity.

3. Click **Test Connectivity**.

   The Profile Connectivity window is displayed. Figure 183 on page 222 shows the Profile Connectivity window.

Figure 183: Profile Connectivity Window



4. Click **Start** to begin the connectivity test using the default connectivity testing options.

   To stop the test before it completes, click **Stop**.

Copyright © 2018, Juniper Networks, Inc.

In the Profile Connectivity window:

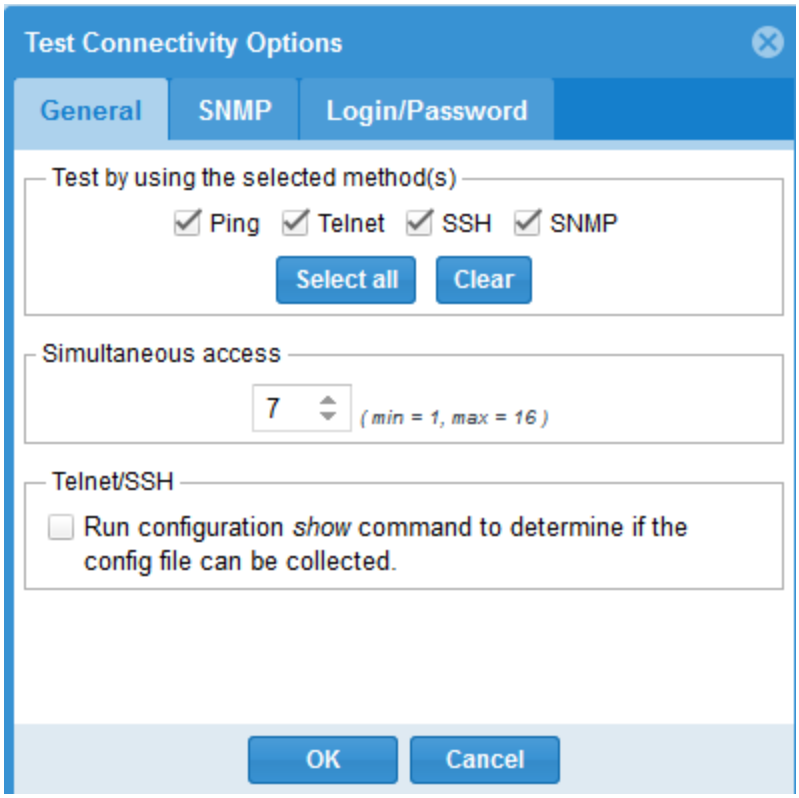
Green checkmark—Connectivity passed.

Gray circle—Not applicable (for example, if SSH is not specified in the router profile).

Hourglass—Processing.

Red circle with white X—Connectivity failed (for example, device is not reachable).

5. (Optional) To override the default connectivity testing options, click **Options**.
   - You can specify a subset of connectivity checks to perform by using the Ping, Telnet SSH, and SNMP protocols.
   - If the SNMP connectivity check fails with the SNMP settings given in the device profile, you can rerun the connectivity check with alternate SNMP community strings. In the SNMP tab of the Test Connectivity Options window, click **Browse** to upload a file containing a list of community strings, one per line. By default, it checks the same SNMP version as in the device profile. Select **Check both v1 and v2c versions** if you want to check both SNMP version 1 and 2c for these alternative strings. The check goes through each community string one by one, until it finds the correct community string. After the check is done, you can fix the profile with the correct community string (Step 6).



6. To correct errors with the current profile that the software can fix, **Profile Fix** is enabled. For example, the device hostname might not match the hostname entered into the device profile or the community string might be incorrect, but the correct one might be found following the steps mentioned in Populating a Device Profile.

7. (Optional) Save the results of the connectivity check onto your PC by clicking the **Save** icon at the lower left. You can then open the file using Excel.

Populating a Device Profile

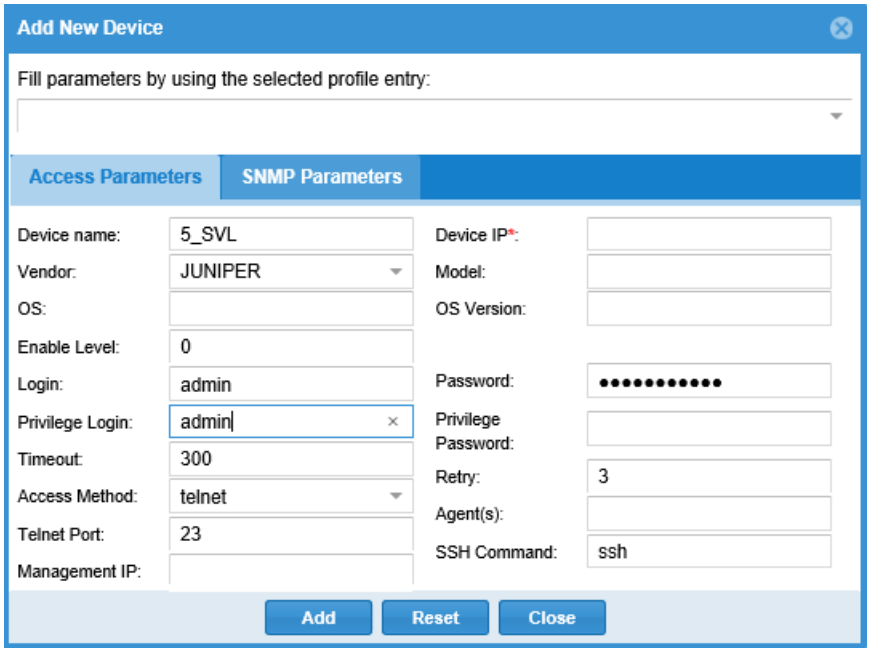
Determine how you want to logically group your network devices to facilitate config file organization and information entry. You can put them all in the same device profile or separate them into separate device profiles. Later you can select devices from one or multiple groups for collection purposes.

To use the Autodiscovery option to discover your network from a subset of all the routers, as described in Network Discovery Overview, you only need to include in your device profile the *seed routers* from which you want IP/MPLSView to start the discovery process. For an OSPF or ISIS network, you can discover an entire area with a seed router based on the OSPF or ISIS database, if router IP addresses are reachable by the management server. If routers can only be reached by management IP addresses, then this method will not work. In a typical out-of-band network, you can use an IP address range to discover the network. For autodiscovery using OSPF, enter one device in each OSPF area in order to collect configurations for all the devices in that area. When you perform the autodiscovery, the software creates a new profile that contains the original devices plus newly discovered devices.

To add entries to your device profile, select the device profile In the left pane of the Device Profiles window to display its contents in the upper right pane. Then, click **Add**. The Add New Device window with the access parameters is displayed, as shown in Figure 184 on page 225.

 Copyright © 2018, Juniper Networks, Inc.

Figure 184: Add New Device Access Parameters Window



The access parameters are described in Table 30 on page 225.

Table 30: Access Parameters in Add New Device Window

Parameter	Description
Device Name	Name of the network device, which should be identical to the hostname. During configuration collection, the software uses this name as part of the name of the collected configuration file. The configuration filename uses the format *ip.name*.cfg. If the device name is left blank, the configuration filename uses the format *ip*.cfg.
Device IP	IP address of the network device.
Vendor	Name of the hardware vendor for the device. Possible values include, but are not limited to: Generic, Cisco, Juniper, ERX, Foundry, Riverstone, CRS, and New. If you select Generic as the vendor, the software attempts to guess the vendor by issuing the **show version** CLI command. For traffic collection purposes, you must specify this field explicitly by choosing a value other than Generic. NOTE: You can also update the Vendor list by adding a new vendor in the Hardware Vendor/Type Manager, provided that you add the related commands in the **/u/wandl/db/command** directory. See *Editing Show Commands for Data Collection* for additional information.
Model	Model number of the network device.
OS	Type of operating system installed on the device.
OS Version	Version number of the operating system build installed on the network device.
Enable Level	Default = 0; reserved for future use. (Some devices may require a privilege password with a different enable level.)

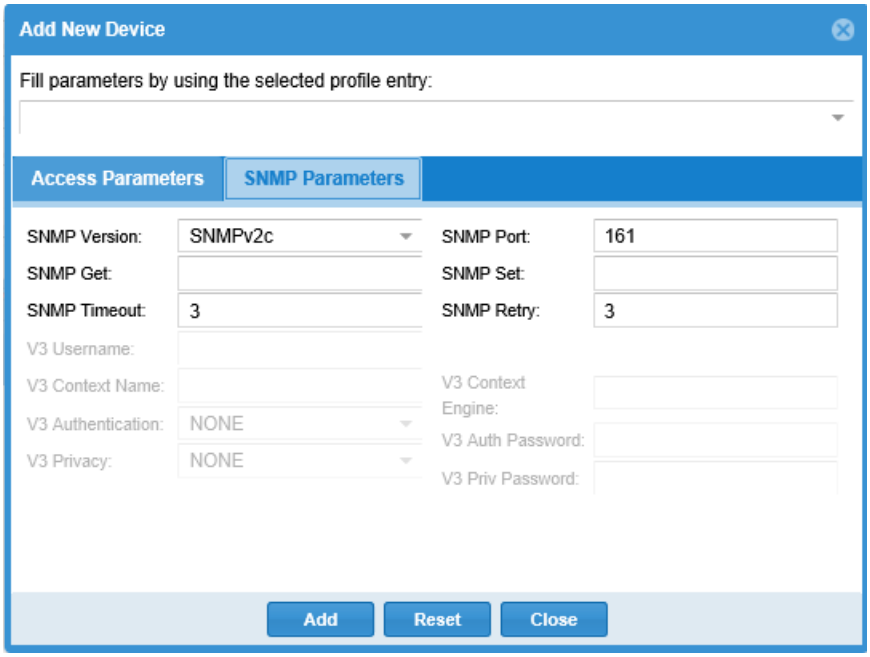
Table 30: Access Parameters in Add New Device Window (continued)

Parameter	Description
Login / Password	Login ID and password for the network device.
Privilege Login / Privilege Password	Login ID and password for situations that require a higher-security login. Use a login that has the appropriate privileges for the vendor-specific **show** commands listed in *Editing Show Commands for Data Collection*.
Timeout	Timeout value for telnet access method. The default value is 300 seconds.
Retry	Number of retries for telnet. The default number of retries is 3.
Access Method	Method used to access the network device. Possible values include: • telnet—(Default) Use only telnet access. • ssh—Use only ssh access. • telnet | ssh—Try telnet access first, and then try ssh access if telnet access fails. • ssh | telnet—Try ssh access first, and then try telnet access if ssh access fails.
Agent(s)	A space-delimited list of one or more intermediate servers that act as gateways to the device. The servers should either have the same login and password as the device, or there should be another entry in the device profile for the intermediate servers to indicate their login and password information. When scheduling a task to collect data for a device through an intermediate server, you must add the intermediate servers to the list of devices to be collected if the intermediate server and the devices have different login and password information.
Telnet Port	Port number for telnet access. The default telnet port number is 23.
SSH Command	The full path of the command and options used for ssh; for example, **/usr/bin/ssh -1 -p 8888**.
Management IP	The management IP address, which is used first to connect to the device, if available. If this connection fails, the software instead uses the IP address of the device.

Click the **SNMP Parameters** tab to enter further details for polling the device via SNMP. Some of the fields for SNMP V3 are grayed out by default and can be enabled by selecting **V3** in the SNMP Version selection box. The Add New Device and Modify Device windows have the same SNMP parameter fields. Figure 185 on page 227 shows the SNMP parameters.

 Copyright © 2018, Juniper Networks, Inc.

Figure 185: Add New Device SNMP Parameters Window



The SNMP parameters are described in Table 31 on page 227.

Table 31: SNMP Parameters in Add New Device Window

Parameter	Description
SNMP Version	V1, V2, V2C, or V3.
SNMP Port	Default = 161.
SNMP Get	SNMP get community string. The GET community can be optionally encrypted by selecting the encryption icon to the right of this field. NOTE: After you encrypt this field, it cannot be reversed from the Web interface to show the associated text.
SNMP Set	SNMP set community string; reserved for future use.
SNMP Timeout	Default = 3 seconds.
SNMP Retry	Default = 3 retries.
V3 User Name	Username.
V3 Context Name	Context name.
V3 Context Engine	Hexadecimal string representing the Context Engine ID.
V3 Authentication	Authentication type. For example, MD5, SHA-1, NONE.

Copyright © 2018, Juniper Networks, Inc.

Table 31: SNMP Parameters in Add New Device Window (continued)

Parameter	Description
V3 Auth Password	Associated authentication key, used to sign the message.
V3 Privacy	Privacy type, for example, CBC-DES, NONE.
V3 Priv Password	Associated privacy key used to encrypt the message's data portion.

After completing the SNMP parameters, click **Add**. Your new entry is displayed in the Device Profiles window. The New Device Profile Entry window remains on the screen, allowing you to quickly create another entry. Modify the necessary fields, including Router Name and IP Address, and click **Add** when you are finished. When you complete adding all entries to your device profile, click **Cancel** to close the New Device Profile Entry window.

See Also

- *Network Discovery Overview*

Updating Device Profiles when Device Passwords are Changed

You must update the corresponding device profiles every time a device password (or SNMP community string) on a device is changed in order to enable successful collection(s) to continue. To do so, select the affected entries in the device profile and perform a multiple modification, as described in Modifying Entries in a Router Profile on page 22.

Tasks using the device profile are updated automatically only if **Use Profile Directly** was selected. If **Use Profile Directly** is not selected, the tasks are then created to use a copy of the device profile, and need to be updated when the profile is updated.

Pre-existing device settings in Traffic Collection Manager are not automatically updated by changes to the device Profiles window, and should be re-done in addition to the Device Profiles window. See *Performance Management: Traffic Collection Overview* for more details on traffic collection settings.

Test the new device profile as described in Verifying Connectivity for One or More Devices in a Device Profile.

Dual Routing Engine Support

Some devices have more than one Routing Engine. In this case, only one Routing Engine is operational at any given point in time. Depending upon which Routing Engine is active, the hostname and management IP address can be different. In this case, for the traffic collection to recognize that two hostnames belong to the same device, this information may need to be provided as an additional input to IP/MPLSView.

In the case of Juniper master and backup Routing Engines, if the default Routing Engine naming conventions are used, beginning or ending with "re0" or "re1", then no special configuration is needed. For such a device, IP/MPLSView stores the hostname as the part in common between the two Routing Engines, that is, with the re0 and re1 removed, along with any separating characters adjacent to re0 and re1 (for example, ".", "_", or "-").

Copyright © 2018, Juniper Networks, Inc.

For other naming conventions for dual Routing Engines, it is necessary to create a special alias file to indicate which Routing Engine hostnames belong to the same router. The format of this file is as follows:

<AliasName> <RoutingEngine0's Hostname> <Routing Engine1's Hostname>

If this alias file is specified in the Conversion Options of the Scheduling Live Network Collection Task, then the routers in the topology display are displayed with the name <AliasName> if the hostname of the collected router matches with either <RoutingEngine0's Hostname> or <Routing Engine1's Hostname>. The original hostname can still be seen in the hostname field of the **Network > Elements > Nodes** view, which can be added as a column to the table via the right-click menu.

In this case, the Router Profile for the device with the dual Routing Engines should contain the AliasName in the Router Name field. The primary IP address can be set to the loopback IP address of the device, assuming that it is the same for both Routing Engines. Alternatively, if there is no common loopback IP address, then the primary and secondary addresses can be set to the master and backup Routing Engines' management IP addresses. In case the primary address fails, then the secondary address is used.

Inaccessible Nodes

For nodes that are inaccessible, an IP/MPLSView format config file can be provided. Include this file in the **/u/wandl/data/collection/. LiveNetwork/config** directory to be picked up by the Scheduling Live Network Collection task. The format of the file is as follows:

```
HOSTNAME=<nodeName>
HWTYPE=<hardwareType>
IP=<NodeAddress>
INTERFACE=<interfaceName> IP=<interfaceAddress>
```

For example, you could configure a device with HWTYPE=CISCO and INTERFACE=Serial1/1.

Syncing to the Master Profile

After scheduling tasks with device profiles, the master profile (**/u/wandl/data/.TaskManager/profile/.diag**) contains the last valid login for each device that is connected.

To copy settings from a current profile to the master profile:

1. Select **Tools > Device Profiles**.

   The Device Profiles window is displayed.

2. Select the profile name that you want to copy settings from the current profile to the master profile (.diag), and click **Sync to Master Profile**.

Related Documentation

- Task Manager on page 199

User Administration

- Understanding User Administration on page 230
- Creating User Groups and Assigning Permissions on page 231
- Adding, Modifying, or Deleting Users on page 231
- Defining Regions and Assigning Devices to Regions on page 232

Understanding User Administration

The User Administration window enables you to perform the following tasks to create and manage the user accounts and user group accounts that access the IP/MPLSView software:

- Create, modify, and delete users and user groups.
- Assign users to user groups.
- Assign permissions to view or modify features and functions at the user group level.
- Define regions and assign devices to regions.
- Work with Web VPN groups.

You can access the User Administration window from **Tools** > **User Admin** in the IP/MPLSView main menu.

Copyright © 2018, Juniper Networks, Inc.

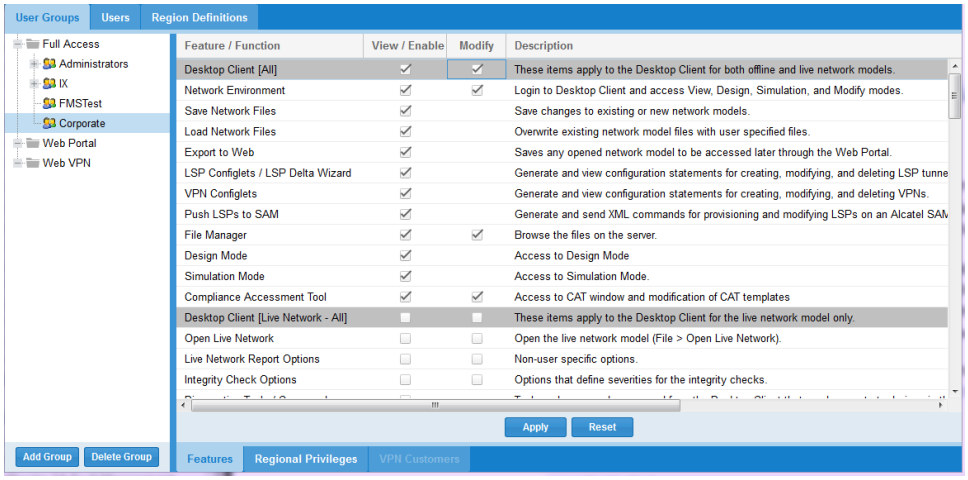
Creating User Groups and Assigning Permissions

To create user groups and assign permissions:

1. Select **Tools > User Admin** from the IP/MPLSView main menu.

   The User Groups tab is displayed by default. Figure 186 on page 231 shows the User Groups tab.

Figure 186: User Administration User Groups



2. Select the type of group you want to create (Full Access, Web Portal, or Web VPN), and click **Add Group**.

3. Specify a name for the new group.

4. Assign a set of privileges to the new user group by selecting one or more features and functions that the group can access.

Adding, Modifying, or Deleting Users

To add, modify, or delete users:

1. Select **Tools > User Admin** from the IP/MPLSView main menu.

   The User Groups tab is displayed by default. Figure 186 on page 231 shows the User Groups tab.

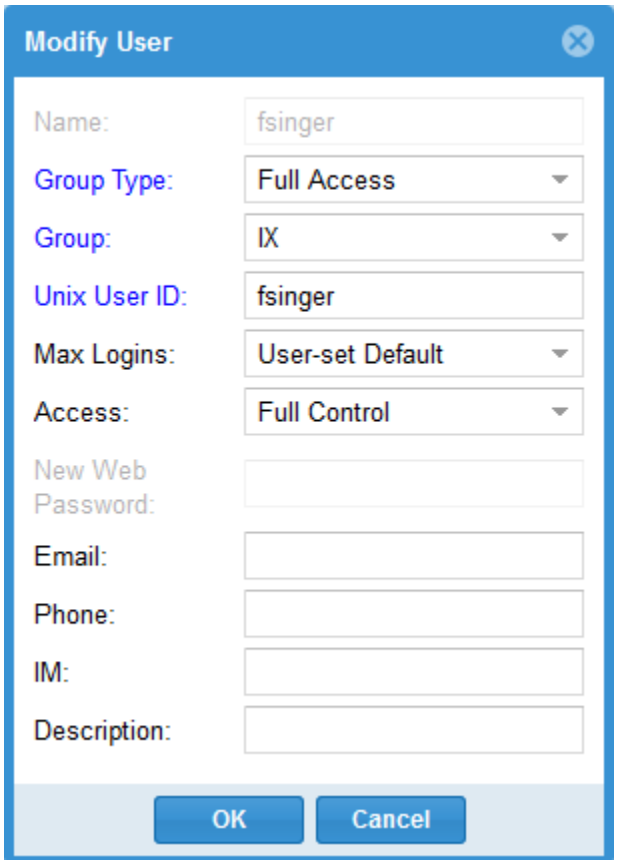
2. Select the **Users** tab.

3. Perform one of the following actions:

   - To add a new user, click **Add** and complete the specified fields in the Add User window.

- To modify an existing user, select the user name, click **Modify**, and update the fields in the Modify User window. Figure 187 on page 232 shows the Modify User window.

Figure 187: User Administration Modify User



- To delete an existing user, select the username and click **Delete**.

Defining Regions and Assigning Devices to Regions

To define regions and assign devices to regions:

1. Select **Tools > User Admin** from the IP/MPLSView main menu.

   The User Groups tab is displayed by default. Figure 186 on page 231 shows the User Groups tab.

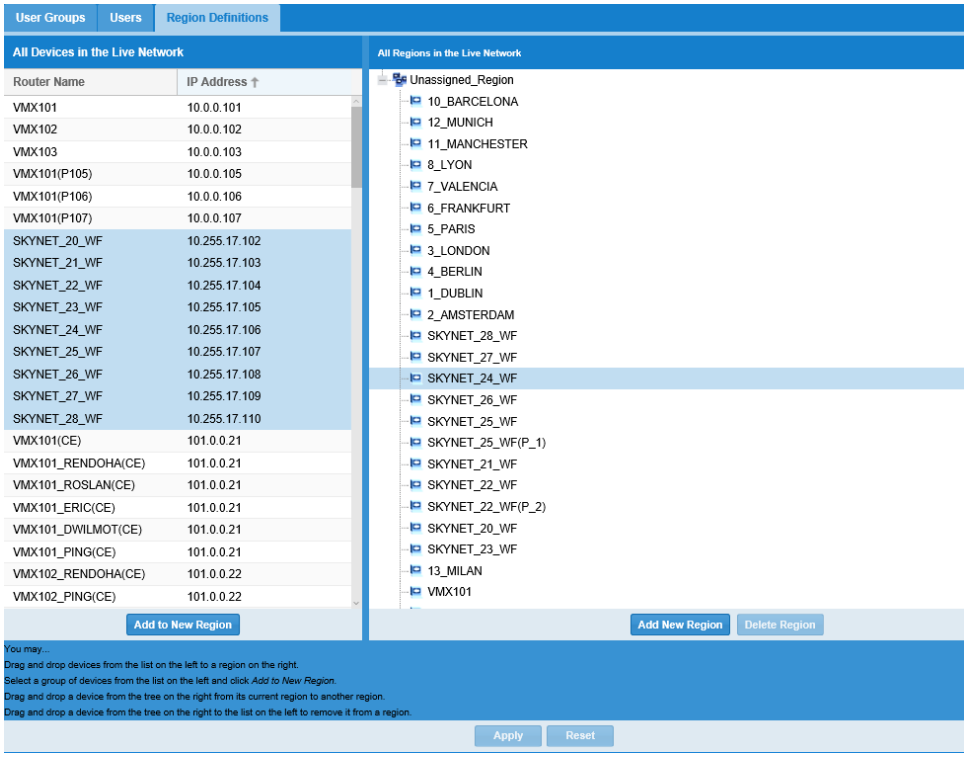
2. Select the **Region Definitions** tab.

3. Select **Add New Region** in the right pane, and specify the name of the region.

4. Select one or more network devices in the left pane and drag the devices to the name of the newly added region in the right pane.

Copyright © 2018, Juniper Networks, Inc.

Figure 188: User Administration Region Definitions



Using the File Browser

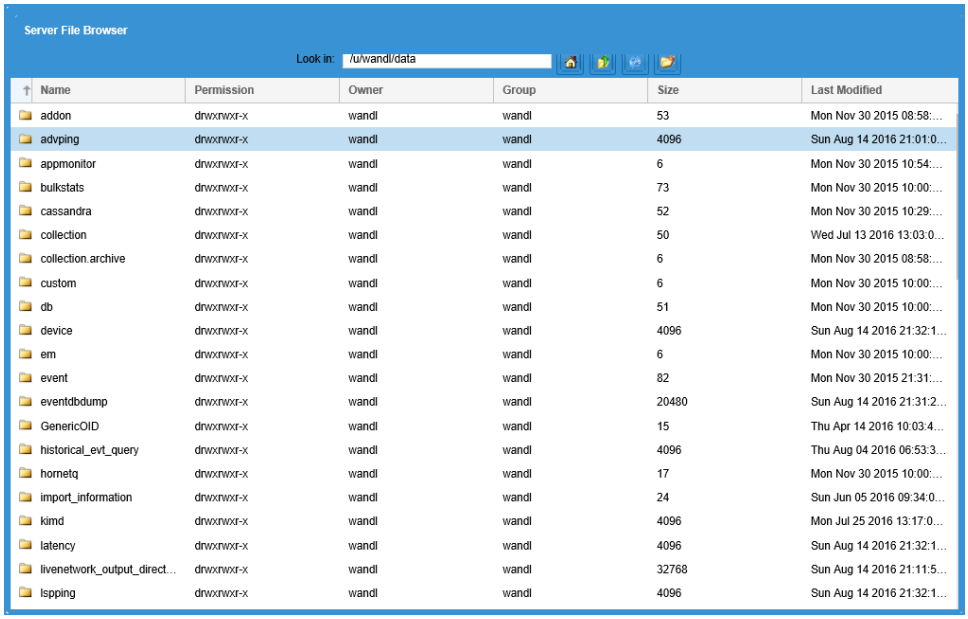
Use the File Browser to Download or view files in IP/MPLSView. Depending on your browser settings, you can view the file in .txt, .csv, .xml,. json, and other available formats.

To view files using the file browser:

1. Select **Tools > File Browser**.

   The Server File Browser window is displayed. Figure 189 on page 234 shows the Server File Browser.

Figure 189: Server File Browser



Name	Permission	Owner	Group	Size	Last Modified
addon	drwxrwxr-x	wandl	wandl	53	Mon Nov 30 2015 08:58:...
advping	drwxrwxr-x	wandl	wandl	4096	Sun Aug 14 2016 21:01:0...
appmonitor	drwxrwxr-x	wandl	wandl	6	Mon Nov 30 2015 10:54:...
bulkstats	drwxrwxr-x	wandl	wandl	73	Mon Nov 30 2015 10:00:...
cassandra	drwxrwxr-x	wandl	wandl	52	Mon Nov 30 2015 10:29:...
collection	drwxrwxr-x	wandl	wandl	50	Wed Jul 13 2016 13:03:0...
collection.archive	drwxrwxr-x	wandl	wandl	6	Mon Nov 30 2015 08:58:...
custom	drwxrwxr-x	wandl	wandl	6	Mon Nov 30 2015 10:00:...
db	drwxrwxr-x	wandl	wandl	51	Mon Nov 30 2015 10:00:...
device	drwxrwxr-x	wandl	wandl	4096	Sun Aug 14 2016 21:32:1...
em	drwxrwxr-x	wandl	wandl	6	Mon Nov 30 2015 10:00:...
event	drwxrwxr-x	wandl	wandl	82	Mon Nov 30 2015 21:31:...
eventdbdump	drwxrwxr-x	wandl	wandl	20480	Sun Aug 14 2016 21:31:2...
GenericOID	drwxrwxr-x	wandl	wandl	15	Thu Apr 14 2016 10:03:4...
historical_evt_query	drwxrwxr-x	wandl	wandl	4096	Thu Aug 04 2016 06:53:3...
hornetq	drwxrwxr-x	wandl	wandl	17	Mon Nov 30 2015 10:00:...
import_information	drwxrwxr-x	wandl	wandl	24	Sun Jun 05 2016 09:34:0...
kimd	drwxrwxr-x	wandl	wandl	4096	Mon Jul 25 2016 13:17:0...
latency	drwxrwxr-x	wandl	wandl	4096	Sun Aug 14 2016 21:32:1...
livenetwork_output_direct...	drwxrwxr-x	wandl	wandl	32768	Sun Aug 14 2016 21:11:5...
lspping	drwxrwxr-x	wandl	wandl	4096	Sun Aug 14 2016 21:32:1...

2. Navigate to the folder and file that you want to download or view.

Copyright © 2018, Juniper Networks, Inc.

CHAPTER 10

Generating and Viewing Reports

- Network Reports on page 235
- User Collected Data Report on page 236
- Shared Reports on page 243
- Shared Docs on page 244
- Report Filters on page 244

Network Reports

The Network Reports page contains a list of network specification (also known as *spec*) projects with their corresponding reports from Report Manager and an image of the Topology layout. To generate this Web report for a specification project, select **File > Export to Web**. You can also generate the Web report on a scheduled interval by selecting **Task Manager > Web Report**. Generating new reports does not overwrite old reports, and each report set is timestamped. The Web administrator can remove these Web reports as needed.

Node Discovery Report

The Node Discovery Report displays the names of devices (nodes) added to or removed from the network after completion of a Scheduling Live Data Collection task or Network Config Data Collection task. To generate the Node Discovery report, IP/MPLSView compares the device differences between the previous network and the current network, and lists any devices that have been added or removed. Viewing the Node Discovery Report enables you to identify and verify any additions, deletions, or changes to the devices in your network.

You can access the Node Discovery Report from either the Web interface or Java client interface in IP/MPLSView. The Web version of the Node Discovery Report provides the same features as the Java client version, with only minor variations in the appearance of the GUI.

To view the Node Discovery Report from the IP/MPLSView Web interface:

1. Log in to the IP/MPLSView Java client interface and open the live network.

2. Select **File > Export to Web**.

The software displays a message window stating that the Web reports are successfully saved.

3. Click **OK** in the message window.

4. Log in to the IP/MPLSView Web interface.

5. Select **Reports > Network Reports > Live Network**.

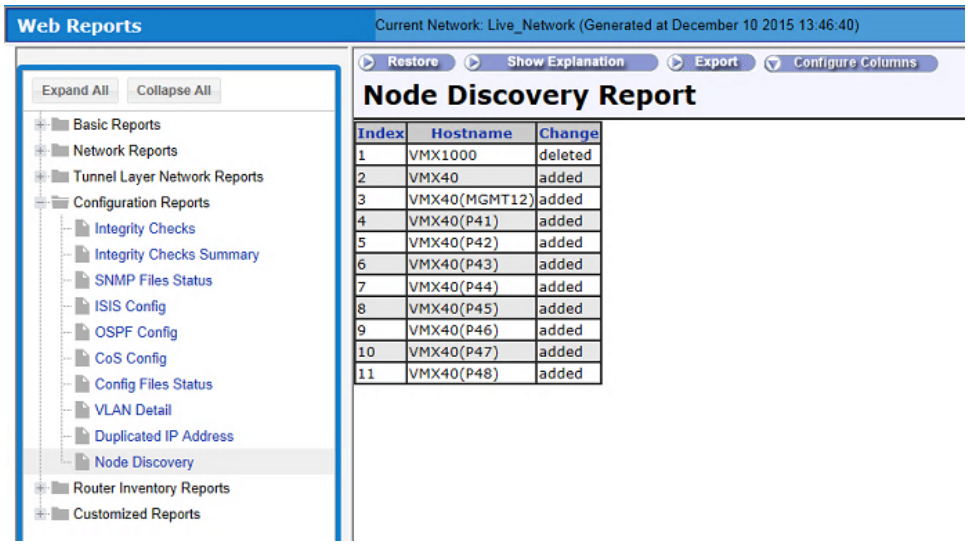
   The Generated Network Data window is displayed.

6. In the Generated Date column, select a date and time that includes a link to configuration reports in the Available Web Reports column.

7. Click **Web Reports**.

8. Select **Configuration Reports > Node Discovery** to display the Node Discovery Report.

Figure 190: Node Discovery Report (Web Version)



Related Documentation

- Shared Reports on page 243

User Collected Data Report

The User Collected Data Report can be generated automatically through the Task Manager, User-Defined SNMP Collection task, as explained in User-Defined SNMP Collection.

Alternatively, the admin user can create IP/MPLSView reports based on other user collected data, as long as it is processed into IP/MPLSView report directory structure.

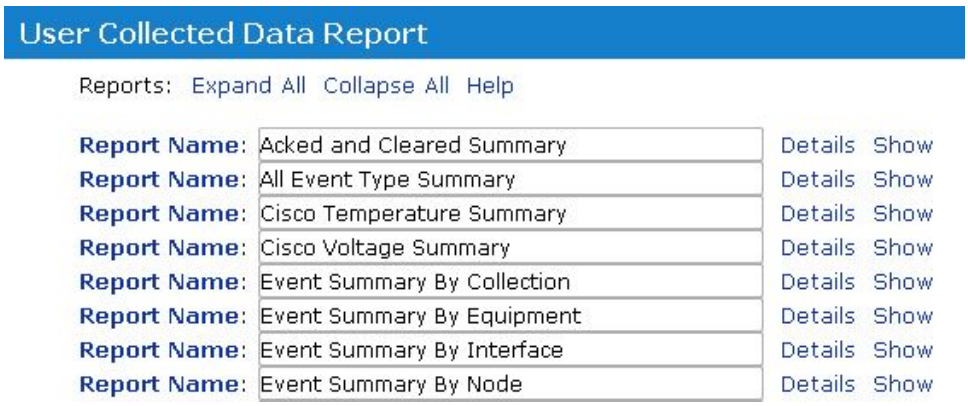
Copyright © 2018, Juniper Networks, Inc.

For information on this report directory structure, see Adding a User Collected Data Report.

NOTE: **This feature requires a license. Please contact your Juniper representative for more details on this feature.**

After collecting successive intervals via the User-Defined SNMP Collection task, the generated Web report can be viewed from **Reports > User Collected Data Report**. The Report Name configured in the task should be displayed in the list of available reports.

Figure 191: User Collected Data Report



Select **Details** to see the configuration options that were used to generate this report. Figure 192 on page 237 shows an example of the report details and configuration options.

Figure 192: Report Details

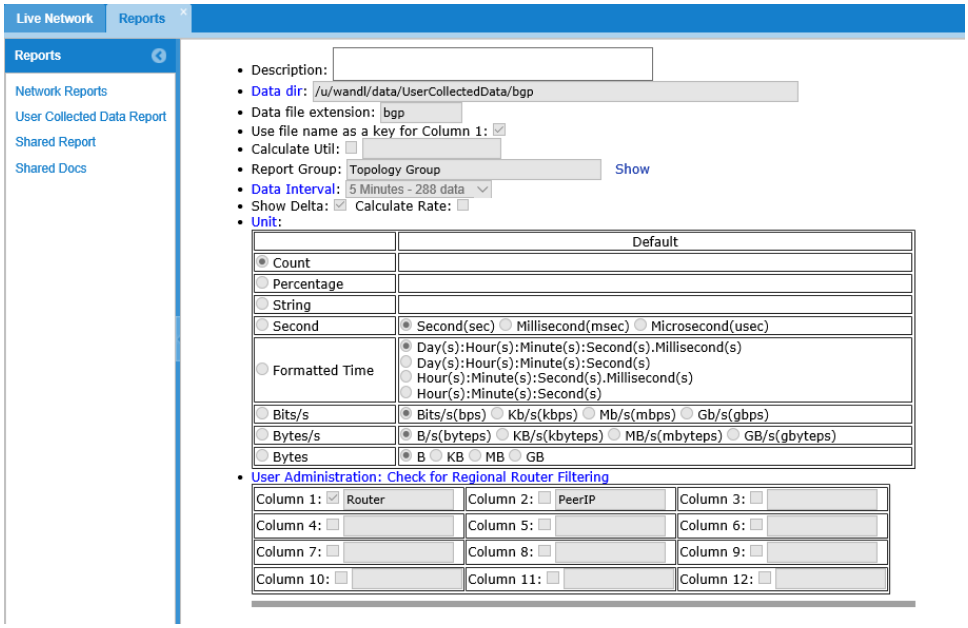


Table 32 on page 238 describes the settings that are used to configure each report.

Table 32: User Collected Data Report Settings

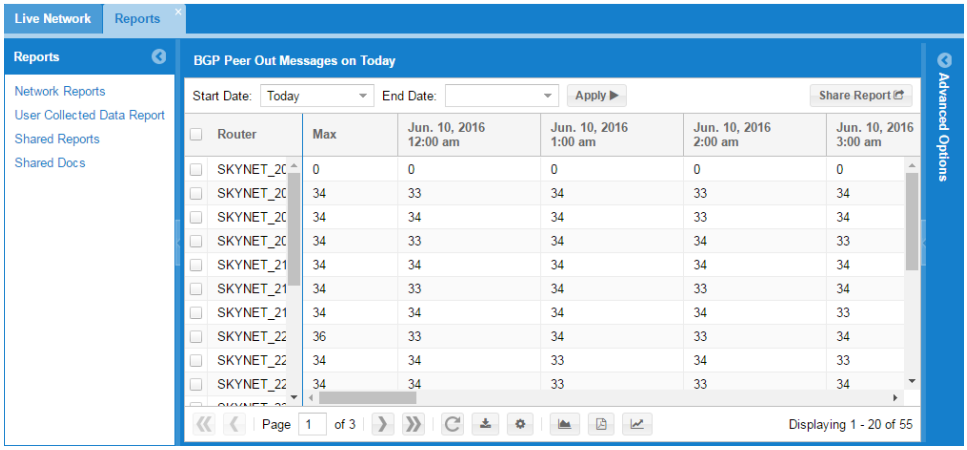
Item	Description
Report Name	Title of the report. This is required.
Data dir	The path of the report. Use only the **/reportname** path. This is required.
Data file extension	Specifies to use only the files with a matching extension name entered. If no extension name is entered, then all files are used. Example, if the report directory contains traffic.cisco and traffic.juniper files, the data file extension entered is juniper, then only traffic.juniper will be used in the report.
Use file name as key for Column 1	Sets the filename as the keyword for Column 1. The first keyword in the data file then becomes Column 2, the second keyword Column 3 and so forth. One example of using this option can be when filenames are organized by router name.
Calculate Util	Uses the util integer in the file and calculates Util% using the formula 100/util. The field entry is to name the ColumnUtil.
Data Interval	Sets the time interval between the sequence of data values.
Show Delta	Displays the difference in data values by subtracting the previous value. If the difference is negative or if there is no previous value, no value is displayed. This option is primarily used when the data value is based on a counter that increments such as traffic values reported by a router.
Calculate Rate	Divides the data value by the unit of measure chosen in the bytes per second option.
Unit	Sets the unit of measure for the data values.
User Administration	Check for Regional Router Filtering applies regional views to the marked Column number, and viewers of the report will only be able to see the data row if they belong to that region. Regional groups are organized by router names, so only a Column number using the router name as the keyword can be applied. Regional groups and user assignments are set up in the User Administration module.
Column field	An entry to set the Column header name.

Viewing Reports

Select **Show** to see the actual report itself. From this page, you can select the date range, the task collection time interval, the Aggregate method (Max, Avg, Sum, 80th, 90th, 95th, or 99th percentile), and the Unit. Click **Apply** after changing the filter criteria. Charts can be created by clicking the **PDF Charts** icon or the **Trending** icon. Figure 193 on page 239 shows a sample User Collected Data Report.

 Copyright © 2018, Juniper Networks, Inc.

Figure 193: Sample User Collected Data Report



This section describes how to view the reports.

- **Apply** refreshes and displays the report based on the configured report settings.
- **Start Date/End Date** is the date range to display.
- **Display data points every** is the time interval to display.
- **Aggregate Method** uses the calculation described in Aggregate Method section.
- **Unit** is the unit to display.
- **Column Filter** filters the display by Column header.
- **Sort By** sorts the display by Column header.
- **PDF Charts** displays row data as charts. You must select at least one row. You can select all rows near the Column header.
- **Line, Column** are chart types.
- **Chart** icon displays a chart for the row.
- **Trending** displays trending report for the row.

Aggregate Method

Aggregate Method is a report display option that returns new data values depending on which aggregate method is chosen. Table 33 on page 239 is used as an example in this section. The time interval of this data set is 1 hour.

Table 33: Aggregate Method Report Results

Base Data	Method	1:00	2:00	3:00	4:00
widgets	N/A	6	4	9	5

For aggregation to work, it requires aggregating the time interval of your data collection. This is done by changing the “Display data points every” option. If the Base Data is aggregated from 1 hour to 2 hours, the new time interval changes to 2 hours and the table

changes. 1:00 and 2:00 are aggregated as 1:00, and 3:00 and 4:00 are aggregated as 3:00.

Table 34: Aggregate Method Report Two-Hour Results

Aggregate Data	Method	1:00	3:00
widgets	select	data	data

The data value for widgets depends on which Aggregate Method is chosen. When data is aggregated, its calculation is based on the new time interval:

- Minimum displays the lowest value in the aggregate time.
- Maximum displays the highest value in the aggregate time.
- Average displays the average value in the aggregate time.
- Sum displays the sum value in the aggregate time.

The new data values for each method are shown in Table 35 on page 240.

Table 35: Aggregate Method Report New-Value Results

Aggregate Data	Method	1:00	3:00
widgets	Minimum	4	5
widgets	Maximum	6	9
widgets	Average	5	7
widgets	Sum	10	14

Data values using aggregate method Y percentile:

- 80% displays 80th percentile using formula average x 0.85 x sd
- 90% displays 90th percentile using formula average x 1.282 x sd
- 95% displays 95th percentile using formula average x 1.645 x sd
- 99% displays 99th percentile using formula average x 2.32 x sd

The new data values using Y percentile and aggregating from 1 hour to 4 hours are shown in Table 36 on page 240.

Table 36: Aggregate Method Report Y Percentile Results

Aggregate Data	Method	1:00
widgets	80%	7.836
widgets	90%	8.769

Copyright © 2018, Juniper Networks, Inc.

Table 36: Aggregate Method Report Y Percentile Results (continued)

Aggregate Data	Method	1:00
widgets	95%	9
widgets	99%	9

Report Directory Structure

The report generally consists of keywords followed by a sequence of values with a definable time interval between those values. One example of a report using this format are traffic reports. The keywords are routers, the values represent traffic data, and the time interval can be defined as hourly. To use this report feature, the requirements are having proper format for the report directory structure and data files on the application server.

Each path corresponds to one day of data. If multiple days are needed for the reports, multiple paths must be created. The directory structure uses the following format:

/reportname/YYMMDD

- *reportname* is a string and helps identifies the report subject.
- *YYMMDD* is year, month, day. All six digits must be entered.
- To share the reports with all users, create the directory structure path in **/u/wandl/data/report/**.
- To restrict the reports from other users, create the directory structure path in the user's home directory **/export/home/username**.

Sample directory structure shared with all users for traffic reports from January 20, 2011 to January 22, 2011:

```
/u/wandl/data/report/traffic/110120
/u/wandl/data/report/traffic/110121
/u/wandl/data/report/traffic/110122
```

File Format

Each file corresponds to one day of data. If multiple days of data are needed for the reports, each file must be placed in the appropriate path using the directory structure format. The filename can be any string and extension that's valid in Unix. The file contents use the following format per line:

keyword1^*keyword2* ^^^ *util*value*util*

- *keyword1* is a string and identifies the data in Column 1. This is required.
- ^ is used to separate keywords.
- *keyword2* is a string and identifies the data in Column 2. Up to nine keywords are supported. (Optional)

- ^^^ is used after the last keyword to indicate the start of the value sequence. This is required.

  NOTE: The ^^^ separator is space,carrot,carrot,carrot,space (^^^).

- *util* is an integer that modifies the report's Util% calculation using the formula 100/util. If you do not need the Util% calculation in the report, there is an option to ignore util in Settings.

  NOTE: The first integer after the ^^^ separator is always considered the util even if Util% calculation is ignored in the Settings. If you do not need Util% calculation, it's recommended to enter 0 for the util before starting the value sequence.

- *value* is an integer and identifies the data in the row. Values are separated by a space. Up to 288 values are supported per row. Additional values after 288 are ignored. The first value entry corresponds to timestamp 00:00 or 12:00am. The time interval between each value is set in Settings.

Table 37 on page 242 corresponds the number of data points to time intervals. If your row has more data points than the interval selected, the additional data points are ignored. If your row has less data points than the interval selected, there will be time intervals with no data.

Table 37: Data Points to Time Intervals

Time Interval	Data Points
5 minutes	288
10 minutes	144
15 minutes	96
20 minutes	72
30 minutes	48
1 hour	24
2 hours	12
3 hours	8
4 hours	6
6 hours	4

Copyright © 2018, Juniper Networks, Inc.

Table 37: Data Points to Time Intervals (continued)

Time Interval	Data Points
8 hours	3
12 hours	2
24 hours	1

Sample file format containing 2 keywords, 0 util, and 8 values:

```
BRTN^VT ^^^ 0 299 250 160 300 499 99 600 430
SMKN^NV ^^^ 0 180 50 499 250 610 450 320 420
LBTC^WA ^^^ 0 459 299 410 326 410 199 200 315
```

Directory and File

Place your data files into each directory: */reportname/YYMMDD/filename*

- Each path corresponds to one unique day. Thus the file contents should be organized as data only for that day.
- Multiple files can be placed in the same *YYMMDD* directory. The report will use all the keywords in all the files and sort them alphabetically in Column1. One example of using multiple files can be traffic data collected and organized by vendor such as traffic.cisco and traffic.juniper.
- Consecutive days are not required for the directory structure.
- The report will display the date range for the directories created.

Related Documentation

- Shared Reports on page 243

Shared Reports

The Shared Reports feature allows users to save, share, and manage certain traffic reports. Saving a report remembers the filter options of the report such as the date range, units, and routers or interfaces selected. The report can be saved as private or public for sharing. To share a report, click the **Share Report** button (see Figure 194 on page 244). The Shared Reports page is accessed under the Reports menu (see Figure 195 on page 244).

Figure 194: Share Report Button

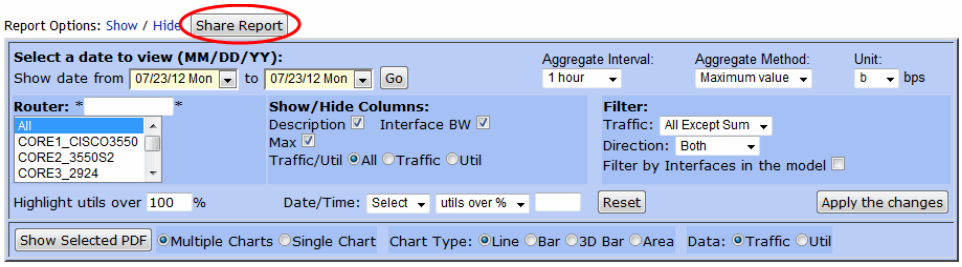
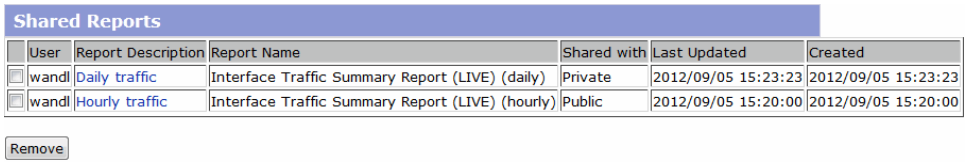


Figure 195: Shared Reports Page



Shared Reports

	User	Report Description	Report Name	Shared with	Last Updated	Created
	wandl	Daily traffic	Interface Traffic Summary Report (LIVE) (daily)	Private	2012/09/05 15:23:23	2012/09/05 15:23:23
	wandl	Hourly traffic	Interface Traffic Summary Report (LIVE) (hourly)	Public	2012/09/05 15:20:00	2012/09/05 15:20:00

Remove

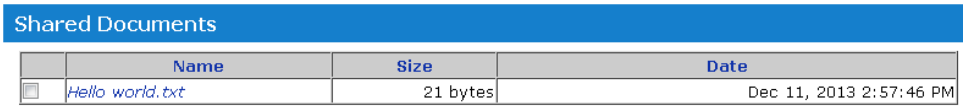
Related Documentation

- Network Reports on page 235

Shared Docs

This page functions as a central place to share documents and files to all Web users. Only the Web administrator can upload or delete files. To download a document, click on the filename and you will be prompted to save or open the file. You can also sort the files by name, size, or date by clicking on the respective column headers. See Figure 196 on page 244.

Figure 196: Shared Documents



Shared Documents

	Name	Size	Date
	Hello world.txt	21 bytes	Dec 11, 2013 2:57:46 PM

Related Documentation

- Network Reports on page 235

Report Filters

- Filtering by Device or Interface on page 244
- Filtering for Group Sum Value on page 246

Filtering by Device or Interface

Using the Column Filter, you can filter what is displayed in the report, such as filtering to display a specific router or interface in the report. The Column Filter is available in traffic, device, and network performance reports.

Copyright © 2018, Juniper Networks, Inc.

To use filtering in a traffic summary report:

1. Select **Performance > Live Traffic.**

   The Live Traffic window is displayed.

2. In the Traffic Type pane, select **Interface > Interface - Summary**.

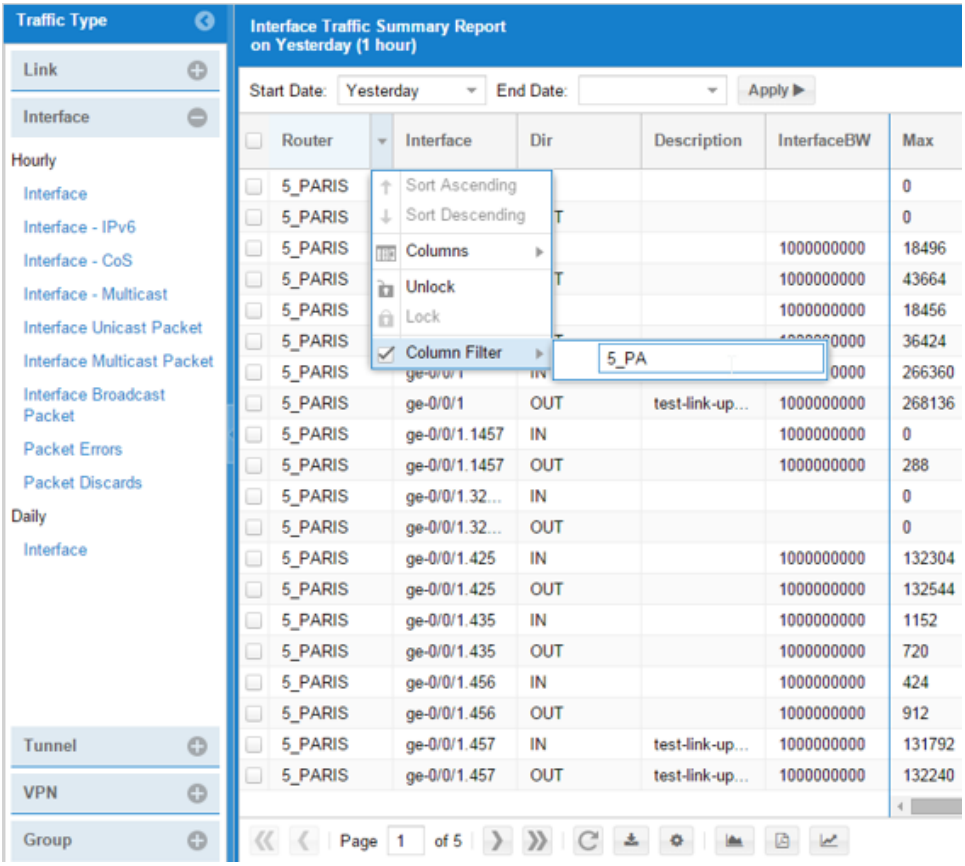
   The Interface Traffic Summary Report window is displayed.

3. From the drop-down lists, select the Start Date and End Date, then click **Apply**.

4. In the Router column drop-down list, select **Column Filter** and enter full or partial router name to filter, and press Enter.

   The Interface Traffic Summary Report window displays only routers that match the filter text. Figure 197 on page 245 displays filtering by router name.

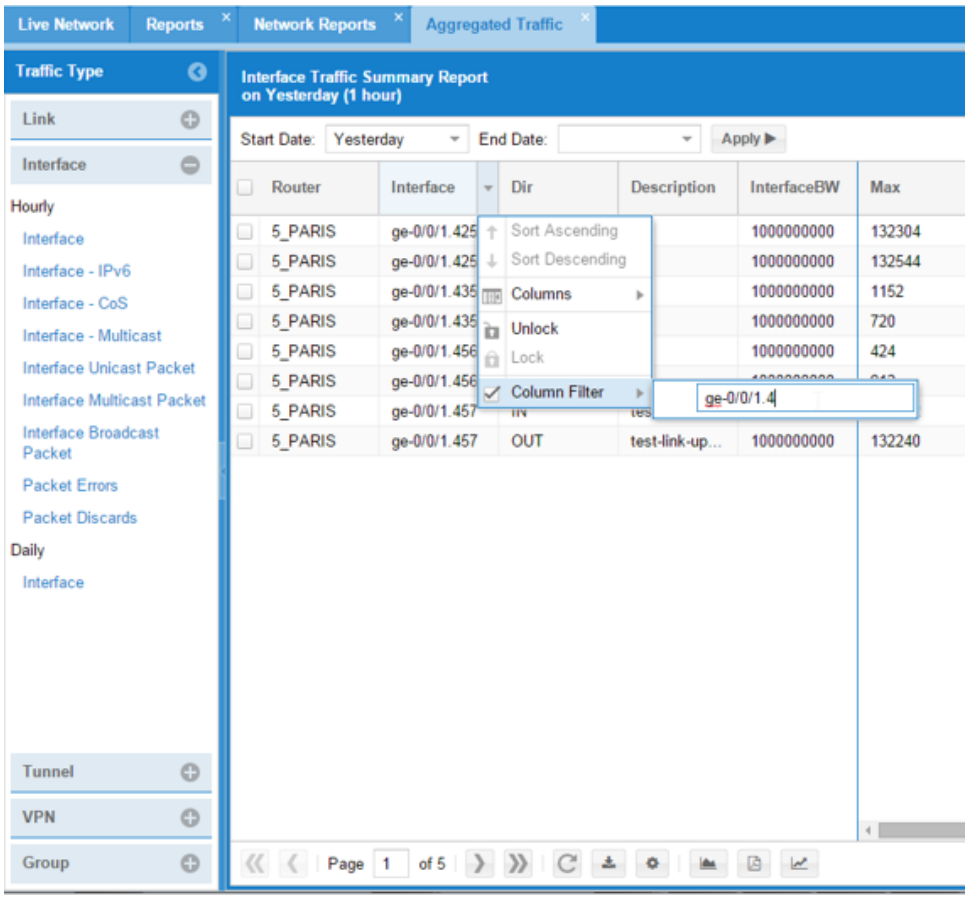
Figure 197: Filter by Device



5. (Optional) In the Interface column drop-down list, select Column Filter and enter the interface to filter, and press Enter.

The Traffic Summary Report window displays only interfaces that match the filter text. Figure 198 on page 246 displays filtering by interface.

Figure 198: Filter by Interface



Filtering for Group Sum Value

The sum displays the total group value for each defined group. Groups are defined in Admin > Report Groups. Groups are sorted in Advanced Options.

To display group sum value in a User Collected Data Report:

1. Select **Reports**.

   The Network reports window displays.

2. In the Reports pane, select **User Collected Data Report**.

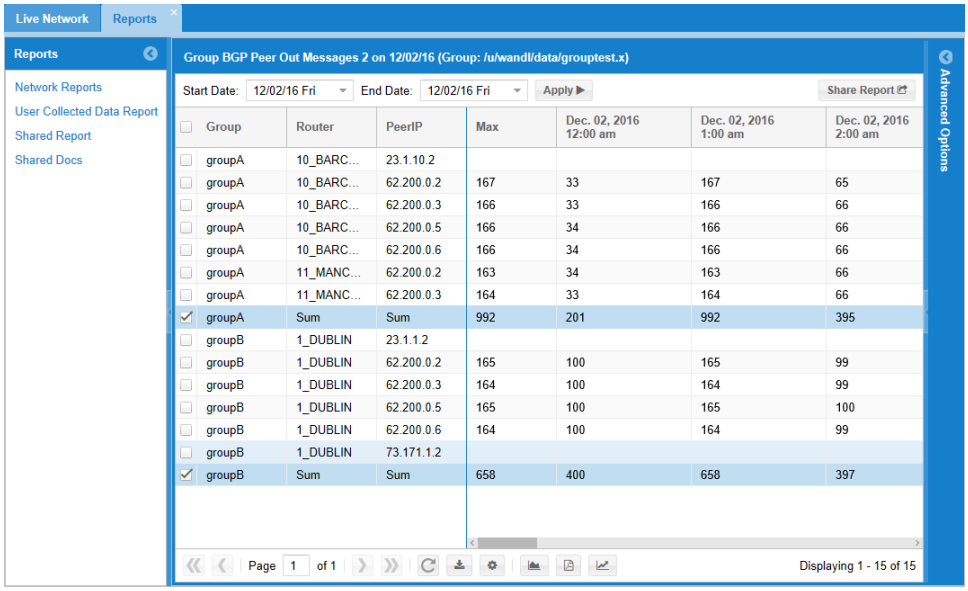
   The User Collected Data Report list is displayed.

3. Select **Show** to view a listed report.

   Figure 199 on page 247 displays the sum group values for each group of routers.

Copyright © 2018, Juniper Networks, Inc.

Figure 199: Group Sum Value



Group	Router	PeerIP	Max	Dec. 02, 2016 12:00 am	Dec. 02, 2016 1:00 am	Dec. 02, 2016 2:00 am
groupA	10_BARC...	23.1.10.2				
groupA	10_BARC...	62.200.0.2	167	33	167	65
groupA	10_BARC...	62.200.0.3	166	33	166	66
groupA	10_BARC...	62.200.0.5	166	34	166	66
groupA	10_BARC...	62.200.0.6	166	34	166	66
groupA	11_MANC...	62.200.0.2	163	34	163	66
groupA	11_MANC...	62.200.0.3	164	33	164	66
groupA	Sum	Sum	992	201	992	395
groupB	1_DUBLIN	23.1.1.2				
groupB	1_DUBLIN	62.200.0.2	165	100	165	99
groupB	1_DUBLIN	62.200.0.3	164	100	164	99
groupB	1_DUBLIN	62.200.0.5	165	100	165	100
groupB	1_DUBLIN	62.200.0.6	164	100	164	99
groupB	1_DUBLIN	73.171.1.2				
groupB	Sum	Sum	658	400	658	397

Related Documentation

- User Collected Data Report on page 236

Copyright © 2018, Juniper Networks, Inc.